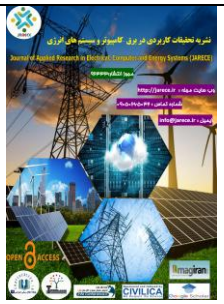
Vol. 3, No. 9, Apr-Jun 2025, (48-65)

Journal of Applied Research in Electrical, Computer and Energy Systems (JARECE)

نشریه تحقیقات کاربردی در برق ، کامپیوتر و سیستم های انرژی

دوره ۳، شماره ۹، بهار ۱۴۰۴ (۶۵-۴۸)

journal homepage: https://jarece.ir/



بررسی کاربرد روش رمزنگاری منحنی بیضوی در تامین امنیت شبکه های حسگر بیسیم

محمد هادی نیا

Mohammad.hadinia1@gmail.com

فوق لیسانس مهندسی فناوری اطلاعات گرایش امنیت اطلاعات ، دانشگاه بین المللی امام رضا (علیه السلام)

چکیده

شبکه های حس گر بی سیم یکی از فناوریهای مهم و تاثیرگذار است که امروزه استفاده از آن در بخش های مختلف جامعه بشری در حال افزایش است . یک شبکه حس گر بی سیم متشکل از تعداد زیادی گرههای حس گری است که در یک محیط به طور گسترده پخش شده و به جمع آوری اطلاعات از محیط می پردازند. شبکه حسگر بی سیم (WSN) در حال تبدیل شدن به یک تکنولوژی قابل توجه برای یک طیف گسترده ای از برنامه های کاربردی . پیشرفت های اخیر در WSN تحقق را تسهیل کرده است. شبکه های حس گر بی سیم به دلیل تنوع در علوم مختلف، دچار چالش های فراوانی بر حسب کاربرد شده اند. با توجه به رشد سریع شبکه‌های حسگر بی‌سیم (WSN) در جهان امروزی ، این شبکه‌ها در تمام شاخه‌های علوم و مهندسی وارد شده‌اند و به دلیل همین کاربردهای وسیع شبکه های حسگر بیسیم ، این شبکه ها بیشتر در معرض تهدیدها و حملات امنیتی هستند. لازم است با در نظر گرفتن ویژگی‌های منحصر به فرد حس‌گرها، یک طرح کلیدی موثر برای مدیریت شبکه‌های حسگر بی‌سیم ارائه شود که بتواند این شبکه ها را در مقابل کلیه حملات و تهدیدات در امان بگذارد و امنیت را برقرار سازد . در این مقاله با کمک رمز نگاری منحنی بیضوی (ECC) ، یک روش امنیتی اصلاح‌شده برای محافظت از شبکه-های حس‌گر بی‌سیم ارائه شده‌است. این طرح با بهره‌گیری از مزیت ECC ، بر اساس تبدیل متن ساده به مقادیر کد ASCII و مبتنی بر عملیات دوتایی به کار رفته در رمزنگاری عمل می‌کند که می‌تواند پیچیدگی محاسباتی را تا حد زیادی کاهش بدهد و امنیت مورد نیاز شبکه های حسگر بیسیم را تامین کند .

واژه‌های کلیدی: امنیت شبکه‌ها،حس‌گر بی‌سیم، رمزنگاری منحنی بیضوی.

۱. مقدمه

پیشرفت های تکنولوژیکی فعلی در سنسورها ، مدارهای یکپارچه با کارایی برق و ارتباطات بی سیم ، امکان توسعه گره های سنسور فیزیولوژیکی مینیاتوری ، سبک وزن ، کم هزینه و هوشمند را فراهم کرده است . این گره ها قادر به حس کردن ، پردازش،و ارتباط یک یا چند نشانه حیاتی می باشند. علاوه بر این ، آنها می توانند در شبکه های منطقه شخصی بی سیم (WPANs) یا شبکه های حسگر بدن (WBSNs) برای نظارت بر سلامت بی سیم استفاده شوند.بسیاری از مطالعات انجام شده و / یا در حال انجام است تا WBSN های انعطاف پذیر ، قابل اعتماد ، امن ، در آنی و کارآمد برای برنامه های کاربردی مراقبت های سلامتی را توسعه دهد. برای کنترل و نظارت موثر بر وضعیت بیمار و همچنین کاهش هزینه انژیی و نگهداری انجام شده است ، IEEE ۸۰۲ .۱۵.۴ ZigBee / aاستاندارد ارتباطی برای ارتباطات بی سیم کم مصرف ، به عنوان یک تکنولوژی جدید و کارآمد در سیستم های نظارت بر سلامت . این مقاله ارائه بررسی مدل و تجزیه و تحلیل و طراحی برای سیستم های نظارت بر سلامت WSN است(رضا تاتی،۱۴۰۳). شبکه های حس گر بی سیم یکی از فناوریهای مهم و تاثیرگذار است که امروزه استفاده از آن در بخش های مختلف جامعه بشری در حال افزایش است . یک شبکه حس گر بی سیم متشکل از تعداد زیادی گرههای حس گری است که در یک محیط به طور گسترده پخش شده و به جمع آوری اطلاعات از محیط می پردازند. این شبکه ها، کاربردهای متنوعی در زمینه هایی چون کشاورزی، حمل و نقل ، صنعت ، ترافیک ، امنیت و پزشکی و غیره دارند. در زمینه پزشکی و سامانه های مراقبت های بهداشتی هوشمند، شبکه های حس گر بی سیم می توانند در به کارگیری تجهیزات پزشکی هوشمند، برای نظارت و مراقبت از بیماران در سنین مختلف و در زمان و مکانهای متفاوت مورد استفاده قرار گیرند. این امر می تواند کمبود شدید کارکنان مراقبت از سلامت را بطور قابل توجهی بهبود دهد. به کارگیری این فناوری در حوزه مراقبت های بهداشتی هوشمند، باعث در دسترس بودن بیشتر و ارتقای خدمات قابل ارائه توسط موسسات خدمات بهداشت و درمان خواهد شد. در نتیجه هزینه های مراقبت بهداشتی در ارائه این خدمات در کلیه سامانه های مراقبت های بهداشتی موجود کاهش پیدا کرده و موجب افزایش بهرهوری سازمانی خواهد شد. امروزه تلفیق این شبکه ها با فناوری در حال توسعه اینترنت اشیاء، کاربرد های چشمگیر، متنوع و مفیدی خواهد داشت که در قالب بخش های دیگری از خدمات و تجهیزات پزشکی می تواند بسیار کارگشا و اثربخش باشد(رمضان تیموری یانسری و همکاران،۱۴۰۲). اخیرا شبکه های حسگر بی سیم مورد استفاده گسترده ای در زمینه های گوناگون از جمله مراقبت های بهداشتی، نظارت در محیط زیست و میدان های جنگ، خانه های هوشمند، حوادث طبیعی و غیر طبیعی و دسترسی به مناطق صعب العبور قرار گرفته اند. این شبکه ها به قوانین مدیریت انرژی برای بهره وری استفاده از منابع محدود باطری برای افزایش طول عمر شبکه نیاز دارند(وحید کبودی و همکاران،۱۳۹۶). شبکه‌های حسگر بی‌سیم شامل تعداد زیادی ازحسگرهای کوچک بوده که برای جمع‌آوری و تشخیص رویدادها به کار می‌شوند. مهم‌ترین محدودیت این شبکه‌ها انرژی بود و یکی از روش‌های مؤثر در کاهش انرژی و افزایش طول عمر شبکه، الگوریتم هاگ انتقال داده خوشه بندی است . در این الگوریتم حال تعدادی از گره‌ها تشکیل یک [ده و یکی از این‌ها به عنوان سرخوش داده‌های سائل گره‌های هم خوشه‌ای را جمع‌آوری کرده در ایستگاه پای می‌فرستد. نحوه انتخاب سرخوش ها و تشکیل خوشه ها خود می‌تواند یک چالش جدی باشد. انتخاب سر خوشه‌های با انرژی پایین‌تر و یا دورتر به ایستگاه پایه می‌تواند منجر به تخلیه انرژی که رها شود(بهزاد مصلحی،۱۳۹۱). شبکه‌های حس‌گر بی‌سیم (WSN) از صدها ابزار مکانیکی ساده به نام گره‌های حس‌گر تشکیل شده‌اند. این حس‌گرها دارایی‌های محدودی دارند. به عنوان مثال دارای توان اندک و حافظه کم هستند. حس‌گرها به صورت دلخواه به فضاهای باز با شرایط دشوار فرستاده می‌شوند تا انواع اطلاعات درباره وزن، دما، رطوبت، میزان سر و صدا و مانند آنها را جمع‌آوری کنند. حس‌گرهای شبکه‌های بی‌سیم می‌توانند از طریق کانال‌های رادیویی با هم ارتباط برقرار کرده و اطلاعات را به یک گره هدایت که به عنوان گره سینک (ایستگاه پایه) شناخته می‌شود انتقال دهند. WSN ها ویژگی‌های لازم برای پوشش حوزه‌های استفاده متنوع مانند بیمه اجتماعی، نظامی، بلایای طبیعی و غیره را دارا هستند (Alkadhmawee and Lu, 2016) و (Pawgasame, 2016). بیشترین کاربرد WSN ها در برنامه‌های کاربردی نظامی است که با اطلاعات بسیار حساسی سر و کار دارند(Kumar et al, 2017) و (Nagender et al, 2017). مدیریت

کلیدها پیش نیاز اصلی برای حفظ ارتباط بین شبکه های حسگر بیسیم است (Zhang and Varadharajan , 2010). مـدیریت کلیدها شامل سن، چرخش و استقرارکلیدها درون گره‌هاست و باید گره‌ها را با رد کردن یا به روز رسانی کردن ، گسـترش داده و یا حذف کند (Kumara et al, 2018).

رمزنگاری متقارن و غیر متقارن برای تحقق امنیت (تایید اعتبار، صحت و محافظت) شبکه‌های حس‌گر بی‌سیم به کار برده می‌شوند. در رمزنگاری متقارن، تمام گره‌ها (فرستنده یا گیرنده) دارای کلید رمزی مشابهی هستند که برای رمزنگاری و رمزگشایی اطلاعات منتقل شده در سیستم مورد استفاده قرار می‌گیرند(Ayman and ali, 2014). در رمز نگاری غیر متقارن، هر گره فرستنده یا گیرنده دارای یک کلید عمومی، که تمام گره‌های سیستم آن را می شناسند، و یک کلید رمزی خصوصی است. رمزنگاری متقارن محاسبات کمتری نیاز داشته و انرژی کمتری نیز نسبت به رمزنگاری غیر متقارن مصرف می-کند(Jasim et al, 2015) و (Aluvala et al, 2016). در این مقاله به بررسی کاربرد روش رمزنگاری منحنی بیضوی در تامین امنیت شبکه های حسگر بیسیم پرداخته شد.

۲-پیشینه

سامان شورابی ثانی و همکاران در سال ۱۳۹۵ به مطالعه ای تحت عنوان مانیتورینگ سلامت سازه های بتنی با استفاده از شبکه های حسگر بی سیم پرداختند در این پژوهش یک سیستم نظارت بر سلامت سازه های بتنی با استفاده از شبکه های حس گر بی سیم معرفی و پیاده سازی می گردد. هدف اصلی در این پژوهش ارائه ی یک سیستم برای اندازه گیری دو پارامتر دما و رطوبت در داخل سازه های بتنی- بویژه در مواقع بتن ریزی با حجم زیاد- با کمترین هزینه طراحی و پیاده سازی و کمترین هزینه ونیاز به عملیات نگهداری و تعمیرات و با بیشترین طول عمر مفید در هنگام قرارگیری در داخل یا مجاورت بتن و عوامل مخرب مشابه در سازه ها ی بتنی است. عمده تمرکز این پژوهش بر دوره های اولیه ی شکل گیری و تشکیل یافتن بتن است. در این پژوهش برای نیل به هدف مذکور چهار تکنولوژی مختلف مورد ارزیابی عملی قرار می گیرد. اولین روش عبارت است از استفاده از ترمیستور با ضریب حرارتی منفی و IRIS mote در قالب توپولوژی شبکه ی IEEE ۸۰۲.۱۵.۴. نتایج نشان می دهد که اندازه گیری این سنسور در حدود ۵ C^{o} بین مقادیر واقعی و مقادیر اندازه گیری شده از خود انحراف معیار استاندارد بروز می دهد. روش دوم از یک سنسور ۱۵SHT (دما و رطوبت) به همراه میکروکنترلر ۴۶۸۰F۱۶PIC و یا برد آردینهو استفاده می کند. روش سوم شامل استفاده از سنسور S۲۱SHT (دما و رطوبت) به همراه برد کاربردی ۲۵۰۰-RF۴۳۰eZ با پردازنده ی ۴۳۰MSP می باشد. در این حالت قرائت مقادیر دما در طول ۱۶ ساعت اولیه به خوبی انجام می گیرد در حالی که مقادیر رطوبت برای ۲۴ ساعت اول آزمایش به خوبی اندازه گیری و ثبت گردیدند. با وجود این که مقادیر اندازه گیری شده برای سنسورهای ۱۵SHT و S۲۱SHT مطابقت خوبی دارند، هر دو سنسور بعد از گذشت مدت زمان مشخصی از کار ایستادند که نشان دهنده ی رابطه ی معکوس بین طول عمر سنسور و شدت قلیایی بودن محیط بتن است و بطور ضمنی لزوم ایجاد پوشش برای سنسور های مذکور را برای کاربرد در داخل بتن متذکر می شود. در روش چهارم از هر دو سنسور ۱۵SHT و S۲۱SHT بصورت محافظت شده برای مانیتورینگ درازمدت استفاده گردید. از آن جا که در مورد اخیر دو سنسور ۱۵SHT و S۲۱SHT با وجودتحت تاثیر قرار گرفتن بواسطه ی محیط قلیایی بتن، موفق به اندازه گیری به مدت نزدیک به دو ماه گردیدند، امکان نظارت بلادرنگ و پیوسته با کمک سنسورهای ویژه در قالب شبکه های حس گر بی سیم با حداقل قیمت تمام شده محقق می گردد(سامان شورابی ثانی و همکاران،۱۳۹۵).

سعید سراج و سلمان فاتحی پیکانی در سال ۱۳۹۶ به مطالعه ای تحت عنوان معرفی شبکه های چند شیبی و الگوریتم های برگشتی هوشمند به منظور کنترل ترافیک درتقاطع ها پرداختند هدف از ارایه ی تحقیق حاضر معرفی مدل های کنترل ترافیک در شبکه سنسور های وایرلس چند شیبی با توجه به الگوریتم های مختلف نظیر الگوریتم پویا برگشتی با در نظر گیری مدت زمان تاخیر برگشتی دینامیکی، مسایل اقتصادی ودست یابی به ماکزیمم توان عملیاتی و کنترل کیفیت برای کنترل ترافیک شبکه های ترافیک شهری می باشد. روش ارایه شده در تحقیق حاضر استفاده از الگوریتم حرکتی چرخشی پویا با در

نظر گیری سیستم ترافیک رایج در شبکه ی ترافیکی در تقاطع ها می باشد. انجام این تحقیق ها منجر به تحولی بزرگ در آینده ای نزدیک برای همگرایی حسگرها ،ارتباطات سریعتر و وسایل ارتباطی خواهد شد لذا جهت توسعه ی هرچه بیشتر نیاز به انتخاب صحیح، زمان واقعی داده های عبوریمی باشد که خود وابسته به مختصات جغرافیایی ، سرعت ، مسیر حرکت ، شتاب و موانع می باشد، جهت بررسی رعایتحق عبور ماشین ها به پاکت هایی تعبیه شده اند که در تقاطع ها در حرکت می باشند و با مدل های کامپیوتری به براوردحق الویت در حرکت مطابق با نیاز وسیله عبوری داده خواهد شد و با برنامه ریزی صحیح و هوشمند کمترین تلفات وبیشترین ایمنی به منظور حق عدالت در حرکت مشخص خواهد شد(سعید سراج و سلمان فاتحی پیکانی،۱۳۹۶).

مجید بقائی نژاد و همکاران در سال ۱۳۹۴ به مطالعه ای تحت عنوان سیستم نوین ارزان قیمت نظارت بر سلامت سازه پل در قسمت عرشه با استفاده از شبکه های حس گر بی سیم مبتنی بر اندازه گیریدما و رطوبت پرداختند در این پژوهش یک نمونه پل مدل کوچک شده از پل های رایج امروزی با ابعاد متوسط (طول ۰۵ متر ’ارتفاع ۰۵ متر ’تعداد پایه ۲) مورد بررسی قرار گرفته و دو گره حس گر با قابلیت اندازه گیری دما و رطوبت دردو سمت قسمت عرشه آن نصب می گردد.اطلاعات جمع آوری شده توسط سیستم شامل مقادیر دما و رطوبت در نرم افزار بر پایه ی LABVIEW دریافت و تحلیل و در یک دیتا بیس مدون ذخیره سازی می شوند.قیمت بسیار پایین، افزایش راندمان بهره برداری از پل وکاهش هزینه های نگهداری و تعمیرات ،این سیستم SHM را به سیستمی پیشرفته و کاربردی مبدل می سازد. در تمامی موارد فوق داده ها و نتایج به تفصیل مورد بررسی قرار گرفته و میزان دقت و قابلیت اطمینان بخش های مختلف سیستم SHM مذکور مورد ارزیابی قرار می گیرد.نتایج نشان می دهد سیستم فوق صلاحیت استفاده در کاربرد SHM برای پل های با ابعاد متوسط تا بزرگ را دارد(مجید بقائی نژاد و همکاران،۱۳۹۴).

سامان شورابی ثانی و منا کلاته عربی در سال ۱۳۹۴ به مطالعه ای تحت عنوان مانیتورینگ سلامت سازه های بتنی با استفاده ازشبکه های حسگر بی سیم پرداختند در این پژوهش یک سیستم نظارت با کمک شبکه های حسگری بی سیم برای بررسی وضعیت سلامت ساختارها و سازه های عمرانی معرفی و پیاده سازی می گردد. هدف اصلی در این پژوهش اندازه گیری دو پارامتر دما و رطوبت در داخل سازه های بتنی است. این تحقیق بردوره های اولیه ی شکل گیری و تشکیل یافتن بتن متمرکز است. در این پژوهش برای نیل به هدف مذکور از چهار متد مختلف استفاده شده است. اولین متد عبارت است از استفاده از ترمیستور با ضریب حرارتی منفی وIRIS mote در غالب توپولوژی شبکه ی IEEE۸۰۲.۱۵.۴ . نتایج نشان می دهد که اندازه گیری این سنسور در حدود ۵C ° بین مقادیر واقعی و مقادیر اندازه گیری شده از خود انحراف معیار استاندارد بروز می دهد. روش دوم از یک سنسورSHT۱۵ دما و رطوبت(به همراه میکروکنترلر PIC۴۶۸۰F۱۶ و یا برد آردینهو استفاده می کند. روش سوم شامل استفاده از سنسور SHT۲۱S دما و رطوبت(به همراه برد کاربردی ۲۵۰۰-RF۴۳۰eZ با پردازنده ی MSP۴۳۰ می باشد. در این حالت قرائت مقادیر دما در طول ۱۱ ساعت اولیه به خوبی انجام گرفت در حالی که مقادیر رطوبت برای ۲ ساعت اول آزمایش به خوبی اندازه گیری و ثبت گردیدند. با وجود این که مقادیر اندازه گیری شده برای سنسورهای SHT۲۱S و SHT۱۵ مطابقت خوبی دارند، هر دو سنسور بعد از گذشت مدت زمان مشخصی از کار ایستادند که نشان دهنده ی رابطه ی مستقیم بین طول عمر سنسور و محیط الکلی موجود در داخل بتن است(سامان شورابی ثانی و منا کلاته عربی،۱۳۹۴).

سید مجید مزینانی و همکاران در سال ۱۳۹۲ به مطالعه ای تحت عنوان مسیریابی آگاه از طیف چند مسیری در شبکه های حس گر رادیو شناختگر با کاربرد شبکه های هوشمند پرداخت در این مقاله، یک الگوریتم مسیریابی آگاه از طیف چند مسیری در شبکه های حس گر رادیو شناختی در شبکه های هوشمند پیشنهاد شده است. پروتکل های مسیریابی موجود نمی توانند به صورت همزمان ویژگی های ترافیکی متفاوت موجود در شبکه های هوشمند را دنبالکنند. از این رو، یک طرح مسیریابی آگاه از طیف با بستر مخابراتی CRSN برای شبکه های هوشمند ارائه می دهیم، که می تواند تعادل ترافیک،ساختن مسیر و کنترل توان را در نظر بگیرد. یک مسیریابی چند مسیری می تواند از دایورسیتی مسیر برای کاهش تداخل در محیط شبکه

هایهوشمند بهره ببرد. روش بیز برای تخمین تعداد کاربران اولیه (PU ها) و کاربران ثانویه (SU ها) مجاور استفاده شده است. تحقیقات نشان می دهدکه طرح مسیریابی آگاه از طیف چند مسیری به صورت قابل توجهی می تواند تداخل را کم کند در نتیجه قابلیت اطمینان را بهبود بخشد(سید مجید مزینانی و همکاران،۱۳۹۲).

محمدرضا ذوقی و محمدحسین کهایی در سال ۱۳۸۷ به مطالعه ای تحت عنوان انتخاب حس گرهای فعال در شبکه های حس گر بی سیم بر اساس GDOP پرداختند در این مقاله موضوع انتخاب حسگرهای فعال برای رهگیری هدف در شبکه حسگر بی سیم بررسی می شود. با توجه به آرایش متراکم حسگرها و مسئله افزونگی اطلاعات نیازی به فعال بودن تمام حسگرها در هر لحظه نیست. در نتیجه به دنبال یافتن مجموعه ای از حسگرهای فعال هستیم تا اولاً مصرف انرژی شبکه کنترل گردد و ثانیاً خطای رهگیری نیز از حداکثر مجازی تجاوز ننماید. با توجه به همخوانی خطای واقعی با اندازه GDOP، ابتدا تابع هزینه ای با استفاده از این اندازه استخراج نموده و سپس برای حل این تابع هزینه روش جستجوی زیر بهینه ای پیشنهاد می نماییم. نتایج شبیه سازی الگوریتم مذکور با الگوریتم های دیگر نشان می دهد که دقت رهگیری قابل مقایسه با روش های جستجوی بهینه است در حالی که میزان محاسبات بسیار کمتر می باشد(محمدرضا ذوقی و محمدحسین کهایی،۱۳۸۷).

سیدمهدی سیادتیان و احمد فراهی در سال ۱۴۰۰ به مطالعه ای تحت عنوان مروری بر روشهای رمزنگاری پایگاه داده های ابری پرداختند در این تحقیق تلاش شده است با شناسایی روش های معمول رمزنگاری در حیطه پایگاه داده های ابری، ضمن استخراج مزایا و معایب هر یک از این روش ها، عوامل موثر در انتخاب یک روش رمزنگاری متناسب با نوع پایگاه داده ابری تبیین شوند. به این ترتیب نتایج این تحقیق هم می تواند به محققان این حوزه در فرآیند مطالعاتی کمک رساند و هم می تواند توسط افراد علاقمند به اجرای روش های رمزنگاری در پایگاه داده های ابری به کار رود(سیدمهدی سیادتیان و احمد فراهی،۱۴۰۰).

فاطمه رمضانی و علیرضا چمکوری در سال ۱۴۰۴ به مطالعه ای تحت عنوان بهبود امنیت داده در رایانش ابری عمومی با استفاده از یک معماری ترکیبی مبتنی ECC, AES پرداختند هدف از این پژوهش نیز ارائه روش کارآمد برای حفظ حریم خصوصی و امنیت دادهها در یک ابر عمومی با استفاده از ترکیب الگوریتمهای رمزنگاری است. از اینرو الگوریتمی ترکیبی با نام ECC - AES ارائه و در نرم افزار متلب پیاده سازی و مورد آزمایش قرار گرفت. دادههای مورد آزمایش شامل مجموعه دادههای تصویری، ۳۲۳، ۴۸۳ و ۶۳۰ بود و به منظور ارزیابی قدرت الگوریتم طول کلیدها نیز ۶۴، ۱۲۸، ۱۹۲ و ۲۵۶ انتخاب و الگوریتم ارائه شده با سایر الگوریتمها شامل Blowfish، AES و DES مقایسه شده است. نتایج به دست آمده نشان داد که الگوریتم ارائه شده در مقایسه با الگوریتمهای گذشته، سرعت بسیار بالا در رمزگذاری و رمزنگاری دارد(فاطمه رمضانی و علیرضا چمکوری،۱۴۰۴).

ایمان سلطانی و شیوا مختاری در سال ۱۳۹۸ به مطالعه ای الگوریتم رمزنگاری AES پرداختند در این مقاله ابتدا توضیح مختصری از روش رمزنگاری متقارن ونامتقارن گفته شده و کلیدهای رمزنگاری مورد بحث قرار گرفته و در ادامه الگوریتم رمزنگاری Rijndael که در حال حاضر بعنوان استاندارد رمزگاری پیشرفته یا به عبارت دیگر Advanced Encryption Standard)AES) شناخته می شود بررسی خواهد شد. در انتها نیز نقاط قوت ASE وتفاوت آن با رمزنگاری های دیگر و حملات صورت گرفته بر روی آن، مورد بحث قرار می گیرد(ایمان سلطانی و شیوا مختاری،۱۳۹۸).

جواد حمیدزاده و همکاران در سال ۱۳۹۴ به مطالعه ای تحت عنوان استفاده از منطق فازی در فرآیند رمزنگاری و رمزگشایی اطلاعات بر روی GPU پرداختند در این مقاله هدف به دست آوردن این حد آستانه با استفاده از منطق فازی در سیستم های مختلف می باشد. این سیستم فازی با در نظر گرفتن سه عامل کلیدی قدرت GPU نسبت به CPU، سرعت انقال اطلاعات به حافظه ی GPU و زمان انجام آماده سازی های اولیه برای انجام عملیات، حد آستانه مناسب را تخمین می زند.آزمایش ها نشان می دهد که انجام عملیات رمزنگاری به این روش بر روی GPU می تواند باعث افزایش کارایی اجرا تا هشت برابر نسبت به CPU شود(جواد حمیدزاده و همکاران،۱۳۹۴).

میثم بهروزیان در سال ۱۴۰۴ به مطالعه ای تحت عنوان چارچوب ترکیبی یادگیری فدرال و رمزنگاری منحنی بیضوی برای تشخیص ناهنجاری در شبکه های اینترنت اشیاء با تضمین حریم خصوصی و کارایی بهینه پرداخت در این مقاله، یک چارچوب ترکیبی مبتنی بر یادگیری فدرال (Federated Learning) و رمزنگاری مبتنی بر منحنی بیضوی (ECC) برای تشخیص ناهنجاری در شبکه های IoT ارائه می شود. در روش پیشنهادی، هر گره IoT با استفاده از یک شبکه عصبی پیچشی (CNN) به صورت محلی آموزش می بیند و گرادیان های محاسبه شده با استفاده از الگوریتم ECC رمزنگاری شده و به سرور مرکزی ارسال می شوند. سرور مرکزی بدون دسترسی به داده های خام، به کمک عملگرهای هوموروفیک مبتنی بر منحنی بیضوی، گرادیان های دریافتی را تجمیع و مدل جهانی را به روزرسانی می کند. برای اعتبارسنجی روش، از دو دیتاست عمومی TON_IoT و BoT-IoT استفاده شده است. نتایج شبیه سازی (روی ماشین محلی با پردازنده Intel i۷-۹۷۵۰H و ۱۶ گیگابایت رم) نشان می دهد که روش پیشنهادی به دقت متوسط ۹۲.۳٪ و مقدار Score۱F- برابر با ۰.۹۱ دست می یابد، در حالی که سربار زمانی رمزنگاری تنها ۱۲٪ افزایش می یابد. این ارقام نسبت به روش های متمرکز مرسوم، بهبود قابل ملاحظه ای در حفظ حریم خصوصی بدون کاهش دقت ایجاد می کنند(میثم بهروزیان،۱۴۰۴).

رضا شاعری نیا و همکاران در سال ۱۴۰۴ به مطالعه ای تحت عنوان ارائه یک طرح احراز هویت و توافق کلید ایمن و کارا مبتنی بر رمزنگاری منحنی بیضوی برای محیط های اینترنت اشیاء صنعتی پرداختند در این پژوهش، یک طرح تبادل کلید احراز هویت مبتنی بر رمزنگاری منحنی بیضوی (ECC) برای ارتباط امن بین دستگاه ها ارائه شده است. پروتکل پیشنهادی در چهار مرحله شامل راه اندازی، ثبت نام، احراز هویت و توافق کلید، و به روزرسانی کلید های خصوصی/عمومی انجام می پذیرد. تحلیل امنیتی نشان می دهد که طرح پیشنهادی در مقایسه با روش های موجود، ایمنی باالتری در برابر حمله های شخص میانی، جعل، نشت پارامتر مخفی و تسخیر کلید دارد. همچنین، بهینه سازی محاسباتی و کاهش تعداد عملیات رمزنگاری، آن را برای محیط های صنعتی با منابع محدود مناسب می سازد. این پژوهش گامی مهم در جهت تضمین اعتمادپذیری و امنیت دستگاه های IIoT است و راه را برای پیاده سازی سیستم های صنعتی مقاوم در برابر تهدیدات امنیتی هموار می کند(رضا شاعری نیا و همکاران،۱۴۰۴).

رضا شفارودی در سال ۱۴۰۳ به مطالعه ای تحت عنوان ساختارهای جبری در رمزنگاری پست کوانتومی پرداخت این پژوهش به بررسی جامع ساختارهای جبری که پایه و اساس رمزنگاری پست کوانتومی را تشکیل می دهند، می پردازد. مطالعه حاضر با تمرکز بر چهار خانواده اصلی رمزنگاری پست کوانتومی شامل رمزنگاری مبتنی بر شبکه، رمزنگاری مبتنی بر کد، رمزنگاری مبتنی بر چندجمله ای های چندمتغیره و رمزنگاری مبتنی بر ایزوژنی، ساختارهای جبری زیربنایی این سیستم ها را مورد تحلیل قرار می دهد. با استفاده از روش تحلیل محتوای کیفی و مرور نظام مند ادبیات موجود، این پژوهش چالش های ریاضی و الگوهای جبری را در طراحی و تحلیل امنیت الگوریتم های پست کوانتومی بررسی می کند. یافته های این مطالعه نشان می دهد که ساختارهای جبری پیچیده مانند شبکه های سخت، کدهای تصحیح خطا، چندجمله ای های چندمتغیره و گراف های ایزوژنی، نقش کلیدی در ایجاد الگوریتم های مقاوم در برابر حملات کوانتومی دارند. همچنین، چالش های موجود در استانداردسازی و پیاده سازی این الگوریتم ها مورد بحث قرار گرفته و مسیرهای آتی تحقیقات در این حوزه پیشنهاد شده است(رضا شفارودی،۱۴۰۴).

محمدعلی شریفی و همکاران در سال ۱۴۰۳ به مطالعه ای تحت عنوان بهبود الگوریتم های رمزنگاری با سیستم تراختنبرگ مطالعه ای درباره سرعت و امنیت پرداختند این تحقیق به بررسی کاربرد سیستم تراختنبرگ، یک روش برای محاسبات سریع ریاضی، در بهبود عملکرد الگوریتم های رمزنگاری، به ویژه در سیستم های رمزنگاری کلید عمومی مانند RSA و رمزنگاری

منحنی بیضوی (ECC) می پردازد. فرآیندهای رمزنگاری به شدت به عملیات محاسباتی سنگینی مانند ضرب اعداد بزرگ، حساب مدولار و توان رسانی مدولار وابسته هستند. این مطالعه بررسی می کند که آیا روش های بهینه سازی شده ضرب و تقسیم در سیستم تراختنبرگ می توانند در این محاسبات رمزنگاری ادغام شوند تا زمان های رمزگذاری و رمزگشایی را کاهش دهند، بدون اینکه امنیت به خطر بیفتد. تحلیل دقیقی روی چگونگی بهینه سازی ضرب در طول توان رسانی مدولار و بهبود کارایی محاسبه معکوس های مدولار با استفاده از تکنیک های تراختنبرگ انجام شد. نتایج تجربی نشان می دهد که به کارگیری این روش ها منجر به کاهش قابل توجهی در زمان محاسبات کلیدی رمزنگاری، به ویژه در الگوریتم RSA، شده است. ارزیابی های امنیتی نشان می دهد که با وجود بهبود در عملکرد، یکپارچگی ساختاری الگوریتم های رمزنگاری حفظ شده و هیچ گونه کاهش قابل ملاحظه ای در قدرت رمزنگاری مشاهده نمی شود(محمدعلی شریفی و همکاران،۱۴۰۳).

وهاب امبنی آذر و همکاران در سال ۱۴۰۲ به مطالعه ای تحت عنوان ارائه یک راهکار رمزنگاری سبک وزن به منظور تامین امنیت داده در اینترنت اشیا پرداختند در این مقاله یک راهکار رمزنگاری سبک وزن مبتنی بر رمزنگاری متقارن و نامتقارن جهت تامین امنیت داده در اینترنت اشیا ارائه شده است. در روش پیشنهادی در ابتدا داده اصلی توسط الگوریتم متقارن بلوفیش رمزنگاری می شود و سپس کلید آن¬ به کمک الگوریتم رمزنگاری خم¬های بیضوی ایمن¬سازی می شود تا در نتیجه بتوان در زمان کم و با امنیت بالا امنیت داده را در زیرساخت¬های مبتنی بر اینترنت اشیا تامین کرد. در انتها راهکار پیشنهادی، از طریق شبیه ساز Eclipse و با آزمایش بر روی حجم داده ۲۰ تا ۱۰۰۰ کلیوبایت مورد ارزیابی قرار داده شده است. نتایج حاصل از شبیه¬سازی نشان می¬د¬هد که روش پیشنهادی در مقایسه با سایر الگوریتم¬های رمزنگاری از نظر معیارهای ارزیابی هم چون زمان اجرا و توان عملیاتی رمزنگاری و رمزگشایی بهینه¬تر عمل می¬نماید. این نتایج؛ بیانگر آن است که راهکار پیشنهادی ضمن برقراری امنیت، کمترین تاثیر منفی را بر روی منابع پردازشی گره های IoT داشته است(وهاب امبنی آذر و همکارانف۱۴۰۲).

سجاد رضایی ادریانی و مهدیه سجادی در سال ۱۴۰۱ به مطالعه ای تحت عنوان رای گیری الکترونیکی بر اساس رمزنگاری همریخت در گروه خم بیضوی پرداختند در این مقاله، یک طرح انتخابات بر اساس رمزنگاری همریخت در گروه جمعی خم بیضوی بیان میشود که ویژگیهایی از جمله استحقاق، محرمانگی، بدون رسید بودن، عدم امکان اجبار و غیره را برآورده میسازد و بدلیل استفاده از گروه خم بیضوی، درکنار امنیت معادل، کارایی خوبی در مقایسه با طرح‌هایی که بر اساس مسئله‌ی تجزیه اعداد و مسئله‌ی لگاریتم گسسته هستند را ارائه میدهد(با کلید ۱۶۰بیتی خم بیضوی امنیت معادل کلید ۱۰۲۴ بیتی RSA دارد). هر چند انتخابات مبتنی بر رمزنگاری همریخت و مسالهی لگاریتم گسسته در طرح هوزتی آمده است ولی روش مستحکمتر ارائه شده با تغییرات لازم و همچنین با ارائهی یک امضای کور که متناسب با طرح رای گیری، سعی شده است که این روش نسبت به مباحث ارائه شده تا به امروز امنتر باشد(سجاد رضایی ادریانی و مهدیه سجادی،۱۴۰۱).

نرگس اسدنجفی و مهدی ملا مطلبی در سال ۱۳۹۹ به مطالعه ای تحت عنوان بهبود احراز هویت در خانه هوشمند مبتنی بر رمز یکبار مصرف و رمزنگاری منحنی بیضوی پرداختند در این مقاله، روشی برای بهبود احراز هویت افراد، مبتنی بر رمز یکبار مصرف با استفاده از کارت هوشمند و الگوریتم رمزنگاری منحنی بیضوی در سامانه خانه هوشمند، ارائه‌شده است. ارزیابی روش پیشنهادی توسط منطق بن و در محیط نرم-افزار آویسپا انجام شده است. نتایج ارزیابی-ها حاکی از بهبود احراز هویت متقابل بین کاربر و گره دروازه جهت مقابله با حملات متداول به خانه هوشمند، در مقایسه با روش‌های موجود است. به‌علاوه، روش پیشنهادی از حملات استراق سمع و حمله سرک-کشی جلوگیری می-نماید که اکثر روش‌های موجود، قادر به جلوگیری از آنها نیستند(نرگس اسدنجفی و مهدی ملا مطلبی،۱۳۹۹).

مریم عطایی نژاد و حمید براتی در سال ۱۳۹۸ به مطالعه ای تحت عنوان یک روش احرازهویت دوطرفه مبتنی بر رمزنگاری منحنی بیضوی در سیستم رادیوشناسه پرداختند در این مقاله یک پروتکل احرازهویت دوطرفه با استفاده از رمزنگاری منحنی بیضوی برای سیستمهای رادیو شناسه ارائه شده است که روشی کارآمد جهت شناسایی حملات مخرب میباشد. مزیت اصلی رمزنگاری منحنی بیضوی یک کلید با اندازه کوچکتر است؛ که این موضوع به معنی کاهش ذخیره سازی و انتقال مورد نیاز است، در نتیجه، یک سیستم منحنی بیضوی میتواند همان سطح از امنیت را که یک سیستم مبتنی بر RSA با ماژول های بزرگ و طول بلند کلید فراهم میکند را ایجاد کند، مزیت دیگر این نوع رمزنگاری عدم توانایی معکوس کردن فرآیندها می باشد به این معنی که وقتی کلید عمومی را که از کلیدخصوصی شما ساخته شده است را اعلام میکنید، با معکوس کردن فرآیند کلید خصوصی شما قابل محاسبه نیست(مریم عطایی نژاد و حمید براتی،۱۳۹۸).

پرویز کشاورزی و محبوبه جعفری در سال ۱۳۹۷ به مطالعه ای تحت عنوان افزایش سرعت پیاده سازی سخت افزاری در رمزنگاری منحنی بیضوی در میدان محدود اول پرداختند در این مقاله برای کاهش پیچیدگی محاسبات و هم چنین افزایش سرعت سیستم رمزنگاری منحنی بیضوی در میدان محدود اول، از روشی استفاده شده است که باعث افزایش سرعت در محاسبات و در نتیجه سرعت سیستم می گردد. در این روش پیشنهادی برای انجام عملیات معکوس پیمانه۱ که عملیات وقتگیر و پیچیده ای می باشد از روشی استفاده کردیم که بجای استفاده از الگوریتم های پیچیده، با استفاده از یک روش ساده و یک جدول پیشنهادی محاسبات معکوس پیمانه در یک کلاک پالس انجام می شود که باعث افزایش سرعت سیستم رمزنگاری منحنی بیضوی می گردد(پرویز کشاورزی و محبوبه جعفری،۱۳۹۷).

ایران حکمتیان در سال ۱۳۹۶ به مطالعه ای تحت عنوان طراحی یک سیستم بازیابی اطلاعات محرمانه مبتیی بر رمزنگاری می‌حنی بیضوی پرداخت در این مقاله یک سیستم بازیابی اطلاعات خصوصی مبتنی بر روش رمزنگاری منحنی بیضوی ارایه می شود که علاوه بر داشتن امنیت در سطح قابل قبول به دلیل برخی ویژگی های این روش از جمله طول کوتاه کلیدها و داده های رمزنگاری شده، میزان هزینه ارتباطی را در محیط های توزیع شده تا سطح قابل توجهی کاهش می دهد(ایران حکمتیان،۱۳۹۶).

حسین نیک خواه در سال ۱۳۹۷ به مطالعه ای تت عنوان افزایش امنیت و کاهش مصرف انرژی در شبکه حسگر بی سیم با استفاده از رمزنگاری منحنی بیضوی پرداخت این مقاله یک راه حل عملی برای احراز هویت همه پخشی چند کاربر و مبتنی بر رستگاری منحنی ایزدی در شبکه های حسگر رییس این پیشنهاد شده است. در مقایسه با کارهای مشابه و از جمله روش فن و همکارانش که جدیدترین آن ها است ، پیچیدگی زمانی مورد نیاز روش پیشنهادی در این مقاله به طور چشمگیری کاهش یافته است. علاوه بر این امنیت قابل اثبات را فراهم کرده و پیاده سازی ساده ای دارد. بنابراین روش پیشنهادی مناسب برای به کارگیری در شبکه های حسگر بایستی می باشد. روش پیشنهادی با تاکید بر ماهیت تولید و تایید امضای دیجیتال در بخش های جداگانه، باعث کاهش هزینه محاسبات می شود. انتهای این مقاله برای اثبات درستی عملکرد روش پیشنهادی با استفاده از زبان برنامه نویسی سی شارپ ، عملیات شبیه سازی روش پیشنهادی صورت گرفته و نتایج این شبیه ساز در قسمت نتیجه گیری مورد تحلیل و بررسی قرار خواهند گرفت(حسین نیک خواه،۱۳۹۷).

سارا همتی و شیوا تقی پورعیوضی در سال ۱۳۹۵ به مطالعه ای تحت عنوان بررسی انواع روش و الگوریتم های رمزنگاری پرداخت این مقاله انواع الگوریتم رمزنگاری مورد بررسی قرار گرفته است. طبقه بندی توابع و الگوریتم-های مورد استفاده در رمزنگاری بر اساس تعداد کلید به دو دسته کلی الگوریتم های رمزنگاری متقارن و نامتقارن تقسیم می شوند. نکته اساسی در طراحی الگوریتم های رمزنگاری انتخاب کلید مناسب می باشد. در هنگام استفاده از الگوریتم های رمزنگاری بایستی در نظر

داشت که سری ماندن پیام صرفاً به مخفی و محرمانه بودن کلید رمز وابسته است. بنابراین انتخاب کلید رمز در کنار الگوریتم مناسب بسیار ضروری می باشد. هدف این پژوهش انتخاب معیارهای مهم به منظور ایجاد یک سیستم امن می باشد. در این مقاله مزایا و معایب الگوریتم های مختلف رمزنگاری و روش پیاده سازی آنها بررسی می شود.معیارهای مهم به منظور انتخاب یک الگوریتم مناسب شامل زمان اجرای الگوریتم، پیچیدگی الگوریتم، مصرف انرژی کمتر، میزان امنیت الگوریتم و بهره وری می باشند(سارا همتی و شیوا تقی پورعیوضی،۱۳۹۵).

۳-چالش های شبکه های حسگر بیسیم

همان گونه که دیدیم علیرغم صورت به ظاهر جذابی که این دسته از شبکه‌ها دارند، اما به دلیل محدودیتهایی که در ساختار فیزیکی و نحوه ارتباطات برای آنها وجود دارد، پیاده سازی عملی آنها با مشکلاتی جدی مواجه است که در زیر آن ها را توضیح می دهیم.

۳-۱- تنگناهای سخت افزاری

هر گره ضمن این که باید کل اجزای لازم را داشته باشد باید به حد کافی کوچک، سبک و کم حجم نیز باشد. به عنوان مثال، در برخی کاربردها گره باید به کوچکی یک قوطی کبریت باشد و حتی گاهی حجم گره محدود به یک سانتی متر مکعب و یا کمتر است و از نظر وزن باید آن قدر سبک باشد که بتواند همراه باد در هوا معلق شود. در عین حال، هر گره باید توان مصرفی بسیار کم و قیمت تمام شده پایین داشته و با شرایط محیطی سازگار باشد.

۳-۲-توپولوژی

توپولوژی ذاتی شبکه حسگر، توپولوژی گراف است. به دلیل این که ارتباط گره‌ها بیسیم و به صورت پخش همگانی است و هر گره با چند گره دیگر که در محدوده برد آن قرار دارد ارتباط دارد، الگوریتم های کارآ در جمع آوری داده و کاربردهای ردگیری اشیاء شبکه را درخت پوشا در نظر می‌گیرند. چون ترافیک اصولاً به فرمی است که داده‌ها از چند گره به سمت یک گره حرکت می‌کنند، مدیریت توپولوژی باید با دقت انجام شود.

۳-۳-قابلیت اطمینان

هر گره ممکن است خراب شود و یا در اثر رویدادهای محیطی مثل تصادف یا انفجار به کلی نابود شود و یا در اثر تمام شدن منبع انرژی اش از کار بیفتد. منظور از تحمل پذیری یا قابلیت اطمینان این است که خرابی گره‌ها نباید عملکرد کلی شبکه را تحت تاثیر قرار دهد.

۳-۴-مقیاس پذیری

شبکه باید هم از نظر تعداد گره و هم از نظر میزان پراکندگی گره‌ها، مقیاس پذیر باشد. به عبارت دیگر، شبکه حسگر از طرفی باید بتواند با تعداد صدها، هزارها و حتی میلیون ها گره کار کند و از طرف دیگر، چگالی توزیع متفاوت گره‌ها را نیز پشتیبانی کند(Kofman et al ,2005).

۳-۵- قیمت تمام شده

از آنجایی که در این شبکه‌ها تعداد گره‌ها زیاد است، کاهش قیمت هر تک گره اهمیت زیادی دارد. تعداد گره‌ها گاهی تا میلیون ها عدد میرسد. در این صورت کاهش قیمت گره، حتی به مقدار کم تاثیر قابل توجهی در قیمت کل شبکه خواهد داشت.

۳-۶-شرایط محیطی

طیف وسیعی از کاربردهای شبکه‌های حسگر، مربوط به محیط هایی می‌شوند که انسان نمی‌تواند در آن حضور داشته باشد. مانند محیط های آلوده از نظر شیمیایی، میکروبی، هسته‌ای و یا مطالعات در کف اقیانوسها و فضا و یا محیط های نظامی به علت حضور دشمن و یا در جنگل و زیستگاه جانوران که حضور انسان باعث فرار آنها می‌شود. در هر مورد، شرایط محیطی نیز باید در طراحی گره‌ها در نظر گرفته شود. به عنوان مثال در دریا و محیط های مرطوب، گره حسگر در محفظه ای که رطوبت را منتقل نکند قرار می‌گیرد.

۳-۷-رسانه ارتباطی

در شبکه‌های حسگر، ارتباط گره‌ها به صورت بیسیم و از طریق رسانه رادیویی، مادون قرمز، یا رسانه‌های نوری دیگر صورت می‌گیرد. اغلب اوقات در این شبکه‌ها از ارتباط رادیویی استفاده می‌شود. البته ارتباط مادون قرمز، ارزانتر و ساختن آن آسانتر است ولی مهمترین عیب آن این است که فقط در خط مستقیم سیر میکند(Banerjee and Khuller, 2001).

۳-۸-توان مصرفی گره‌ها

گره‌های شبکه حسگر باید توان مصرفی کم داشته باشند. گاهی منبع تغذیه، یک باتری ۱/۲ ولتی با انرژی ۵/. آمپر-ساعت است که باید توان لازم برای مدت طولانی مثلاً ۹ ماه را تامین کند. در بسیاری از کاربردها، باتری گره قابل تعویض نیست. لذا عمر باتری عملاً عمر گره را مشخص میکند.

۳-۹- افزایش طول عمر شبکه

یکی از مشکلات اساسی در این شبکه‌ها این است که عمر شبکه‌های حسگر، نوعاً کوتاه است چون طول عمر گره‌ها به علت محدودیت انرژی منبع تغذیه کوتاه است. علاوه بر آن، گاهی موقعیت ویژه یک گره در شبکه، مشکل را تشدید میکند. به عنوان مثال در گره‌ای که در فاصله یک قدمی گره اصلی قرار دارد از یک طرف به دلیل بار کاری زیاد، خیلی زود انرژی خود را از دست می‌دهد و از طرف دیگر، از کار افتادن آن باعث قطع ارتباط گره اصلی با کل شبکه می‌شود و لذا کار شبکه مختل می‌گردد.

۳-۱۰- ارتباط بلادرنگ و هماهنگی

در برخی از کاربردها مانند سیستم تشخیص و جلوگیری از گسترش آتش‌سوزی یا سیستم پیش‌گیری از سرقت، سرعت پاسخگویی شبکه اهمیت زیادی دارد. برای تحقق بلادرنگ بودن انتقال اطلاعات، یک راه حل این است که برای بسته‌های ارسالی، یک ضرب العجل تعیین شود و در لایه کنترل دسترسی رسانه، بسته‌های با ضرب العجل کوتاهتر زودتر ارسال شوند. مدت ضرب العجل به کاربرد آن شبکه بستگی دارد.

۳-۱۱- عوامل پیش بینی نشده

یک شبکه حسگربیسیم، تابع تعداد زیادی از عدم قطعیت هاست. عوامل طبیعی غیرقابل پیش بینی مثل سیل، زلزله، مشکلات ناشی از ارتباط بیسیم و اختلالات رادیویی، امکان خرابی هر گره، کالیبره نبودن حسگرها، پویایی ساختار و مسیردهی شبکه، اضافه شدن گره‌های جدید و حذف گره‌های قدیمی، جابجایی گره‌ها به طور کنترل شده و یا در اثر عوامل طبیعی و غیره، همه و همه مثال هایی از وجود عدم قطعیت در این شبکه‌هاست.

۱۳-۱۲-امنیت

اساسی ترین چالش در شبکه های حسگر بیسیم موضوع امنیت است. امنیت در برخی کاربردها به خصوص در کاربردهای نظامی یک موضوع بحرانی است و به خاطر برخی ویژگی ها شبکه‌های حسگر در مقابل مداخلات آسیب پذیرترند. یک مورد، بیسیم بودن ارتباط شبکه است که کار دشمن را برای فعالیتهای ضد امنیتی و مداخلات آسانتر می‌سازد.

مورد دیگر استفاده از یک فرکانس واحد ارتباطی برای کل شبکه است که شبکه را در مقابل استراق سمع آسیب‌پذیر می‌کند. مورد بعدی ویژگی پویایی توپولوژی است که زمینه را برای پذیرش گره‌های دشمن فراهم می‌کند. این که پروتکلهای مربوط به مسیریابی، کنترل ترافیک و لایه کنترل دسترسی شبکه سعی دارند با هزینه و سربار کمتری کار کنند مشکلات امنیتی به وجود می‌آورد. به عنوان مثال برای شبکه‌های حسگر در مقیاس بزرگ برای کاهش تاخیر بسته‌هایی که در مسیر طولانی در طول شبکه حرکت می‌کنند یک راه حل خوب این است که اولویت مسیردهی به بسته‌های عبوری داده شود. همین روش باعث می‌شود حمله‌های سیل آسا موثرتر باشد. یکی از نقاط ضعف شبکه‌های حسگر کمبود منبع انرژی است و دشمن می‌تواند با قرار دادن یک گره مزاحم که مرتباً پیغامهای بیدار باش به صورت پخش همگانی و با انرژی زیاد تولید می‌کند باعث شود گره‌های همسایه بدون دلیل از حالت خواب خارج شوند. ادامه این روند باعث به هدر رفتن انرژی گره‌ها شده و عمر آنها را کوتاه می‌کند.

با توجه به محدودیتهای ذکر شده بایستی به دنبال راه حلهای ساده و کارا مبتنی بر طبیعت شبکه حسگر بود. مثلاً این که گره‌ها با چگالی بالا میتوانند توزیع شوند و هر گره دارای اطلاعات کمی است یا این که داده‌ها در یک مدت کوتاه معتبرند از این ویژگیها میتوان به عنوان یک نقطه قوت در رفع مشکلات امنیتی استفاده کرد. اساساً چالشهای زیادی در مقابل امنیت شبکه حسگر وجود دارد و مباحث تحقیقاتی مطرح در این زمینه گسترده و پیچیده است که ما برای حل این مشکل از الگوریتم رمزنگاری اصلاح شده منحنی بیضوی برای تامین و تضمین امنیت داده های ارسالی در محیط گره های شبکه حسگر بیسیم استفاده می کنیم.

۴-چهارچوب پیشنهادی

سناریو را به این ترتیب در نظر بگیرید که A و B امکان ارسال داده‌ها به یکدیگر را به یک شیوه امن دارند. آنها برای ارسال این داده‌ها نیاز به یک کلید خصوصی دارند. این کلید خصوصی یک عدد صحیح اول مثبت است که به صورت تصادفی در حین وقوع نشست انتخاب می‌شود. شعار اصلی این روش کاهش عملیات اضافی مورد نیاز است. کل عملیات در فلوچارت نشان داده شده تا افراد بتوانند مکانیزم این روش را به خوبی درک کنند. در این فلوچارت، جریان دقیق داده‌ها میان کاربران به خوبی نمایش داده شده‌است.

در شکل۱ الگوریتم رمزنگاری اصلاح شده منحنی بیضوی به کمک فلوچارت توضیح داده شده است و در شکل ۲ مدل چهار چوب سیستم‌های حس‌گر نمایش داده شده‌است.

Step 1: Key Scheduling

User A

- Choose the private key $n_A \in [1, p-1]$.
- Compute the public key $P_A = n_A . G$

User B

- Choose the private key $n_B \in [1, p-1]$.
- Compute the public key $P_B = nA . G$

The secret Key will be $K = n_A P_A = nB\ P_A = n_A n_B G$

Encryption

User A

- Convert each character of the message m to hexadecimal ASCII value of two digits $(h_1 h_2)_{16}$.
- Rewrite the value $(h_1 h_2)_{16}$ as $(h_1, h_2)_{16}$ then convert it to two decimal values $(d_1, d_2)_{10}$.
- Compute $P_{h1} = d_1 G\ //\ G$ is the base point.
- Compute $P_{h2} = d_2 G\ //\ G$ to represent the values d_1 and d_2 as points on E (F_B).
- Compute K= $n_A P_B\ //\ n_A$ the private key of user A and P_B the public key of user B

Decryption

User B

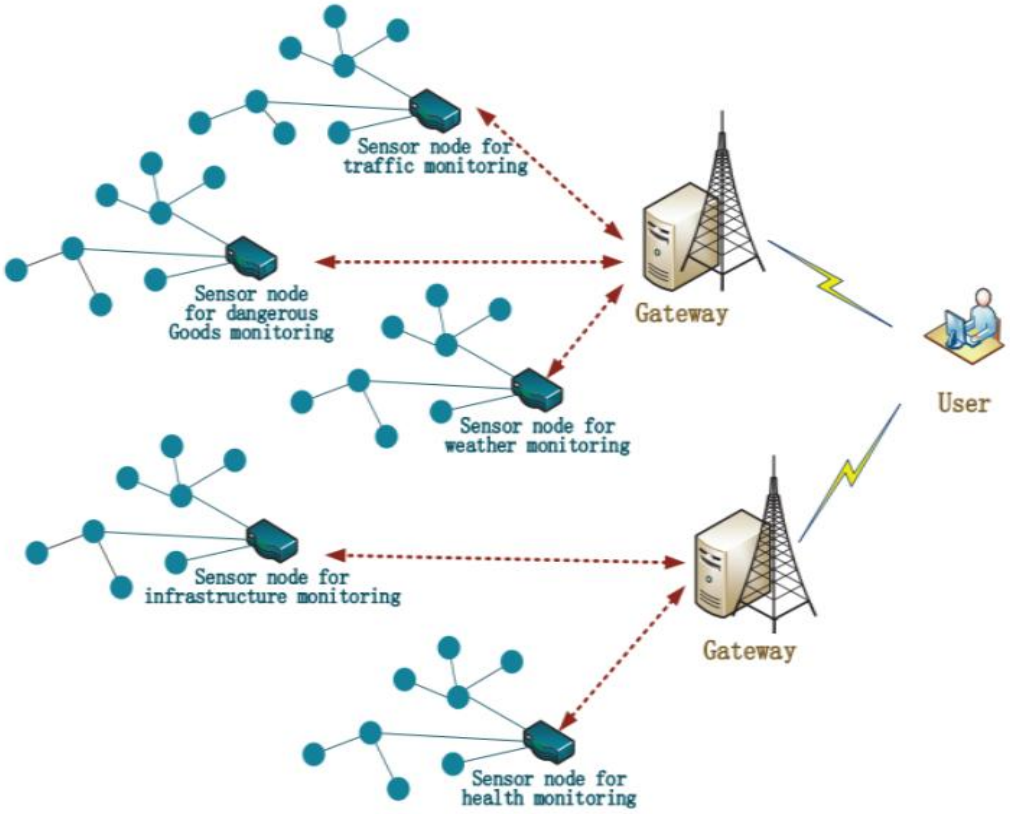
Compute K= $n_B P_A$

- Compute $P_{h1} = C_1 - K$
- Compute $P_{h2} = C_2 - K$

Extract d_1 from P_{h1}, // by solving the discrete logarithm problem $P_{h1} = d_1 G$.

- Extract d_2 from P_{h2}, // by solving the discrete logarithm problem $P_{h2} = d_2 G$.

شکل ۱: فلوچارت پیشنهاد شده رمزنگاری اصلاح شده منحنی بیضوی



شکل ۲: مدل چهارچوب سیستم های حسگر بیسیم

به طورکلی کاربران ممکن است با چهارچوب‌های چرخشی احساس راحتی بیشتری کنند. این چهارچوب‌ها دارای دو عضو هستند: چیدمانی از کاربرها و یک سرور مجزا. این در حالی است که در سیستم اعتبارسنجی خریدار درWSN ها سه بخش وجود دارد: گره‌های مختلف، یک درگاه دسترسی و چیدمانی از کاربران. در یک ساختار حس‌گر راه دور گره‌های فراوانی وجود دارند که در یک محدوده جذاب ارسال می‌شوند. این گره‌ها به همراه هم کار می‌کنند تا داده‌ها را از دنیای فیزیکی جمع‌آوری و ثبت کرده و از نظر ظرفیت نیز تحت کنترل قرار دارند. علاوه بر این، این گره‌ها معمولا مورد بی توجهی واقع شده و رقبا می‌توانند آنها را به راحتی برای دستیابی به پارامترهای ناشناخته جمع‌آوری کنند. گره درگاه بر نام‌نویسی‌ها تمرکز می‌کند. یک روش اعتبارسنجی در WSN ها غالبا از ۴ مرحله ضروری تشکیل شده‌است: ثبت‌نام، ورود، چک، و اسم رمز.

۵- نتیجه‌گیری

در شبکه‌های حس‌گر بی‌سیم، محدودیت انرژی گره‌ها نقش اساسی در طراحی هرگونه پروتکلی برای پیاده‌سازی دارد. WSN ها به سرعت رشد کرده و کاربردهای گوناگون می‌یابند، در نتیجه نیاز به امنیت در آنها ضروری می‌شود. واضح است که سیستم رمزنگاری، قابل اعتمادترین و موثرترین سیستم برای عملیات رمزنگاری و رمزگشایی آسان اطلاعات است. این سیستم همچنین در معرض حملات مختلف داخلی و خارجی قرار دارد. در این تحقیق روش جدیدی به کار گرفته شد که با تلاش کمتر، قابلیت رمزنگاری و رمزگشایی هر متن ساده به مقادیر معادل ASCII برای هر کاراکتر کدگذاری شده را دارد و امنیت لازم در شبکه های حسگر بیسیم را تامین می کند .

منابع

۱. اسدنجفی، نرگس و ملامطلبی، مهدی،۱۳۹۹،بهبود احراز هویت در خانه هوشمند مبتنی بر رمز یکبار مصرف و رمزنگاری منحنی بیضوی، فصلنامه علوم و فناوری های پدافند نوین، دوره: ۱۱، شماره: ۴ https://civilica.com/doc/1184755،

۲. امینی آذر، وهاب و فرحی، رسول و دشتی، فاطمه،۱۴۰۲،ارائه یک راهکار رمزنگاری سبک وزن به منظور تامین امنیت داده در اینترنت اشیا،دوفصلنامه فناوری اطلاعات و ارتباطات ایران، دوره: ۱۶، شماره: ۶۱ https://civilica.com/doc/2137614،

۳. بقایی نژاد، مجید و نادری راد، منا و شورابی ثانی، سامان،۱۳۹۴،سیستم نوین ارزان قیمت نظارت بر سلامت سازه پل در قسمت عرشه با استفاده از شبکه های حس گر بی سیم مبتنی بر اندازه گیریدما و رطوبت،هفتمین کنفرانس ملی مهندسی برق و الکترونیک ایران،گناباد، https://civilica.com/doc/459512

٤. بهروزیان، میثم،۱۴۰۴،چارچوب ترکیبی یادگیری فدرال و رمزنگاری منحنی بیضوی برای تشخیص ناهنجاری در شبکه های اینترنت اشیاء با تضمین حریم خصوصی و کارایی بهینه، https://civilica.com/doc/2409777

۵. تاتی، رضا،۱۴۰۳،تجزیه و تحلیل عملکرد شبکه های حسگر مبتنی بر ZigBee برای نظارت بر سلامت،اولین کنفرانس بین المللی فناوری اطلاعات، مدیریت و کامپیوتر،ساری، https://civilica.com/doc/2084098

٦. تیموری یانسری، رمضان و آجودانی، مجتبی و مسیبی، سیدرضا،۱۴۰۲،کاربرد شبکه های حس گر بی سیم در نظارت بر مراقبت های بهداشتی هوشمند - وضعیت فعلی و مسیرهای آینده،ششمین همایش ملی فناوریهای نوین در مهندسی برق، کامپیوتر و مکانیک ایران،تهران، https://civilica.com/doc/1744240

۷. حکمتیان، ایران،۱۳۹۶،طراحی یک سیستم بازیابی اطلاعات محرمانه مبتیی بر رمزنگاری می‌حنی بیضوی،نخستین کنفرانس ملی پیشرفت ها و فرصت های فناوری اطلاعات و ارتباطات،تهران، https://civilica.com/doc/781781

۸. حمیدزاده، جواد و ابوالفتح زاده امینجان، محمود و زرقانی، محمد،۱۳۹۴،استفاده از منطق فازی در فرآیند رمزنگاری و رمزگشایی اطلاعات بر رویGPU ،چهاردهمین کنفرانس سیستم های فازی ایران،تبریز، https://civilica.com/doc/730921

۹. ذوقی، محمدرضا و کهایی، محمدحسین،۱۳۸۷،انتخاب حس گرهای فعال در شبکه های حس گر بی سیم بر اساس GDOP،شانزدهمین کنفرانس مهندسی برق ایران،تهران، https://civilica.com/doc/47670

۱۰. رضایی ادریانی، سجاد و سجادیه، مهدی،۱۴۰۱،رای گیری الکترونیکی بر اساس رمزنگاری همریخت در گروه خم بیضوی، مجله فناوری های نوین مهندسی برق در سیستم انرژی سبز، دوره: ۱، شماره: ۳ https://civilica.com/doc/1535501،

۱۱. رمضانی، فاطمه و چمکوری، علیرضا،۱۴۰۴،بهبود امنیت داده در رایانش ابری عمومی با استفاده از یک معماری ترکیبی مبتنیAES, ECC ،دومین کنفرانس ملی علم داده در کاربردهای مهندسی،تبریز، https://civilica.com/doc/2459124

۱۲. سراج، سعید و فاتحی پیکانی، سلمان،۱۳۹۶،معرفی شبکه های چند شیبی و الگوریتم های برگشتی هوشمند به منظور کنترل ترافیک درتقاطع ها،دومین کنفرانس بین المللی مهندسی عمران،معماری ومدیریت بحران،تهران، https://civilica.com/doc/662048

۱۳. سلطانی، ایمان و مختاری، شیوا،۱۳۹۸،الگوریتم رمزنگاریAES ،ششمین کنگره ملی تازه های مهندسی برق و کامپیوتر ایران با نگاه کاربردی بر انرژی های نو،تهران،https://civilica.com/doc/923878

۱۴. سیادتیان، سیدمهدی و فراهی، احمد،۱۴۰۰،مروری بر روشهای رمزنگاری پایگاه داده های ابری،چهارمین کنفرانس بین المللی مهندسی برق، کامپیوتر و مکانیک،تهران،https://civilica.com/doc/1271653

۱۵. شاعری نیا، رضا و حسینی، سید اکبر و حاجیان، رحمان و عرفانی، سیدحسین،۱۴۰۴،ارائه یک طرح احراز هویت و توافق کلید ایمن و کارا مبتنی بر رمزنگاری منحنی بیضوی برای محیط های اینترنت اشیاء صنعتی،نخستین همایش ملی "هوش مصنوعی و پژوهش های نوظهور:همگرایی انسان و سیستم های هوشمند،تهران،https://civilica.com/doc/2323300

۱۶. شریفی، محمدعلی و پارسا، حسین و سیاح مقدم، امین،۱۴۰۳،بهبود الگوریتم های رمزنگاری با سیستم تراختنبرگ مطالعه ای درباره سرعت و امنیت،سومین کنفرانس بین المللی پژوهش در ریاضیات، فیزیک و محاسبات عددی،تهران،https://civilica.com/doc/2191132

۱۷. شفارودی، رضا،۱۴۰۳،ساختارهای جبری در رمزنگاری پست کوانتومی،اولین همایش بین المللی معلمان استعدادیاب و فرهنگ ساز در توسعه آموزش های فنی و حرفه ای و کاردانش در مسیر توسعه پایدار،https://civilica.com/doc/2227400

۱۸. شورابی ثانی، سامان و کلاته عربی، منا و خزاعی، علی اکبر،۱۳۹۵،مانیتورینگ سلامت سازه های بتنی با استفاده از شبکه های حسگر بی سیم، مجله تحقیقات بتن، دوره: ۹، شماره: ۱ ،https://civilica.com/doc/1995110

۱۹. شورابی ثانی، سامان و کلاته عربی، منا،۱۳۹۴،مانیتورینگ سلامت سازه های بتنی با استفاده ازشبکه های حسگر بی سیم،کنفرانس بین المللی پژوهش های نوین در عمران، معماری و شهرسازی،تهران،https://civilica.com/doc/449667

۲۰. عطایی نژاد، مریم و براتی، حمید،۱۳۹۸،یک روش احرازهویت دوطرفه مبتنی بر رمزنگاری منحنی بیضوی در سیستم رادیوشناسه،سومین کنفرانس ملی کامپیوتر، فناوری اطلاعات و کاربردهای هوش مصنوعی،اهواز،https://civilica.com/doc/1015586

۲۱. عماد، فرزانه،۱۴۰۳،بهبود روشهای تضمین امنیت داده با استفاده از مکانیزمهای کنترل دسترسی در رایانش ابری،هفتمین همایش ملی فناوریهای نوین در مهندسی برق، کامپیوتر و مکانیک ایران،تهران،https://civilica.com/doc/2050311

۲۲. کبودی، وحید و کبودی، سعید و حبیبی زادنوین، احمد،۱۳۹۶،مروری بر روش های مدیریت انرژی در شبکه های حس گر بی سیم با استفاده از خوشه بندی غیر فعال،دومین کنفرانس بین المللی پژوهش های دانش بنیان در مهندسی کامپیوتر و فناوری اطلاعات،تهران،https://civilica.com/doc/695979

۲۳. کشاورزی، پرویز و جعفری، محبوبه،۱۳۹۷،افزایش سرعت پیاده سازی سخت افزاری در رمزنگاری منحنی بیضوی در میدان محدود اول،اولین کنفرانس ملی مهندسی برق، کامپیوتر و فناوری ارتباطات،اصفهان،https://civilica.com/doc/936173

۲۴. مزینانی، سید مجید و جعفری نژاد، آزاده و زمردیان، محمد احسان،۱۳۹۲،مسیریابی آگاه از طیف چند مسیری در شبکه های حس گر رادیو شناختگر با کاربرد شبکه های هوشمند،شانزدهمین کنفرانس دانشجویی مهندسی برق ایران،کازرون،https://civilica.com/doc/265489

۲۵. مصلحی، بهزاد و منتظری، محمد علی،۱۳۹۱،سر خوشه‌های قراردادی یک پروتکل ارتباطی خوشه بندی بهبود یافته در مصرف انرژی برای شبکه‌های عسگر بی‌سیم،همایش منطقه ای علوم کامپیوتر، مهندسی کامپیوتر و فناوری اطلاعات،دورود،https://civilica.com/doc/173491

۲۶. نوری، داود و یغمایی مقدم، محمدحسین و نیکوقدم، مرتضی،۱۳۹۲،مدیریت کلید با استفاده از رمزنگاری منحنی بیضوی برای خوشه بندی امن در شبکه های حسگر بیسیم،دهمین کنفرانس بین المللی انجمن رمز ایران،یزد،https://civilica.com/doc/788029

۲۷. نیک خواه، حسین،۱۳۹۷،افزایش امنیت و کاهش مصرف انرژی در شبکه حسگر بی سیم با استفاده از رمزنگاری منحنی بیضوی،دومین همایش بین المللی مهندسی برق،علوم کامپیوتر و فناوری اطلاعات،همدان،https://civilica.com/doc/766403

۲۸. همتی، سارا و تقی پورعیوضی، شیوا،۱۳۹۵،بررسی انواع روش و الگوریتم های رمزنگاری،اولین مسابقه کنفرانس بین المللی جامع علوم مهندسی در ایران،بندرانزلی،https://civilica.com/doc/545454

1. Ahmed A. Alkadhmawee and Songfeng Lu,(2016). “Prolonging the Network Lifetime Based on LPA-Star Algorithm and Fuzzy Logic in Wireless Sensor Network,” World Congress on Intelligent Control and Automation (WCICA), IEEE, 2016

2. Pawgasame, W.,(2016). “A survey in adaptive hybrid wireless Sensor Network for military operations”. IEEE, in Second Asian Conference Defence Technology (ACDT), pp. 78-83, 2016

3. J. Zhang and V. Varadharajan,(2010). “Wireless sensor network key management survey and taxonomy”, Journal of Network and Computer Applications, vol. 33, pp. 63-75, 2010

4. Omer K. Jasim, Safia Abbas and El-Sayed M. Horbaty, (2015). “Evolution of an Emerging Symmetric Quantum Cryptographic Algorithm”, Journal of Information Security, Vol. 6, pp. 82-92, 2015

5. Ayman T., Ayman K. and Ali C., (2014). "Authentication Schemes for Wireless Sensor Networks," in Mediterranean Electrotechnical Conference (MELECON), IEEE, pp. 367-372, 2014

6. P.Kumara Swamy, Dr.C.V.Guru Rao, Dr.V.Janaki, "Functioning of secure key authentication scheme in" in International Journal of Pure and Applied Mathemat, Volume 118, Issue 14, Page No(s) 27- 32, MAR. 2018, [ISSN(Print):1314-3395]

7. Srinivas Aluvala, K. Raja Sekar,, Deepika Vodnala, (2016). "A Novel Technique for Node Authentication in Mobile Ad-hoc Networks" in Elsevier - Perspectives in Science, Volume 8, Issue 1, Page No(s) 680 - 682, SEP. 2016, [ISSN(Print):2213-0209], DOI:10.1016/j.pisc.2016

8. B. Vijay Kumar, Srinivas Aluvala, K. Sangameshwar, (2017). "Energy Mapping Approach for QoS in MANETs" in International Journal of Computer Sciences and Engineering, Volume 5, Issue 10, Page No(s) 273 - 275, OCT. 2017, [ISSN(Print):2347-2693, ISSN(Online): 2347-2693]

9. Y.Nagender, Y. Chanti, B. Vijay Kumar, D.Mahesh, (2017). "Protection Issues and Disputes in Wireless Sensor Networks" in International Journal on Computer Science and Engineering (IJCSE), Volume 9, Issue 12, Page No(s) 706 - 713, DEC. 2017, [ISSN (Print):2229-5631, ISSN (Online): 0975-3397]
10. C. Y. Chong, S. P. Kumar, (2003)."Sensor Networks: Evolution, Opportunities, and Challenges" Proceedings of the IEEE Transaction on Computers, Vol. 91, pp.23-27, May, 2003.
11. G. J. Pottie, W. J. Kaiser, "Wireless Integrated Sensor Networks,(2000)." Communications of the ACM, May 2000. An overview with more of a signal processing viewpoint
12. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci,(2002). "A Survey on Sensor Networks," IEEE Communications, Aug. 2002, pp.102-114

13. F. Akyildiz, W. Su, Y. Sankarsabramaniam and E. Cayirci,(2002). "Wireless Sensor Networks: A Survey," Computer Networks, Vol. 38, pp. 393-422, March 2002
14. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister,(2000). "System architecture directions for networked sensors," In Proceedings of the 9 th International Conference on Architectural Support for Programming Languages and Operating Systems, November 2000
15. J. N. Alkaraki and A.E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey,(2004)." IEEE Journal of Wireless Communications, vol. 11, No. 6, Dec. 2004, pp. 6-28
16. D. Estrin, R. Govindan, J. Heidemann, and Satish Kumar,(1999). "Next Century Challenges: Scalable Coordination in Sensor Networks," In Proceedings of Mobicom'99, 1999
17. K. Sohraby, D. Minoli, T. Znati,(2007). "Wireless Sensor Networks: Technology, Protocols and Applications, " Published by WILEY INTERSCIENCE- 2007
18. C. Schurgers, M. B. Srivastava,(2001). "Energy Efficient Routing in Wireless Sensor Networks," Proceedings of the IEEE Military Communications Conference (MilCom'01): Communications for Network-Centric Operations- Creating the Information Force, McLean, VA, Oct. 2001
19. D. Kofman Ravi Mazumdar, N. Shrof Vivek, P. Mhatre, Catherine Rosenberg,(2005). "A minimum cost heterogeneous sensor network with a lifetime constraint," IEEE Transactions on Mobile Computing, 04(1):4-15, Jan/Feb 2005
20. B. Banerjee, and S. Khuller,(2001). "A Clustering Scheme for Hierarchical Control in Multi-Hop Wireless Networks," Proc of INFOCOM, April 2001

Investigating the application of elliptic curve cryptography in securing wireless sensor networks

Mohammad Hadinia
Master's degree in Information Technology Engineering, Information Security major, Imam Reza International University (PBUH)

Abstract -Wireless sensor networks are one of the important and influential technologies that are increasingly being used in various sectors of human society today. A wireless sensor network consists of a large number of sensor nodes that are widely distributed in an environment and collect information from the environment. Wireless sensor networks (WSN) are becoming a significant technology for a wide range of applications. Recent advances in WSN have facilitated the realization. Wireless sensor networks have faced many challenges in terms of application due to their diversity in different sciences. Due to the rapid growth of wireless sensor networks (WSN) in today's world, these networks have entered all branches of science and engineering And because of these wide applications of wireless sensor networks, these networks are more exposed to security threats and attacks. It is necessary to provide an effective key management scheme for wireless sensor networks, taking into account the unique characteristics of sensors, which can protect these networks from all attacks and threats and establish security. In this paper, with the help of elliptic curve cryptography (ECC), a modified security method is presented to protect wireless sensor networks. Taking advantage of the advantage of ECC, this scheme operates based on converting plain text to ASCII code values and based on binary operations used in encryption, which can greatly reduce the computational complexity and provide the security required for wireless sensor networks.

Keywords: Network security, wireless sensor, elliptic curve cryptography.