مجله علمی-پژوهشی
رایانش نرم و فناوری اطلاعات
جلد ۱، شماره ۳، سال ۱۳۹۱

# نهان‌نگاری صحبت در شبکه‌های سنسور بی‌سیم مبتنی بر تبدیل موجک

حسن فرسی [۱]، سید مرتضی نوریان [۲]
[۱] گروه مخابرات، دانشکده‌ی مهندسی برق و کامپیوتر، دانشگاه بیرجند، HFarsi@birjand.ac.ir
[۲] دانشکده‌ی مهندسی برق و کامپیوتر، دانشگاه بیرجند، Nourian_Morteza@yahoo.com

**چکیده**

*به منظور ارسال امن سیگنال صحبت محرمانه در شبکه‌های سنسور بی‌سیم، روشی بر مبنای تبدیل موجک ارائه شده است. در این روش با استفاده از خصوصیات تبدیل موجک، سیگنال محرمانه ضمن فشرده‌سازی، رمزنگاری نیز می‌شود. خروجی این فشرده‌سازی که به صورت رشته بیتی نامفهوم است، بایستی در سیگنال صحبت حامل جاسازی شود. با ۵ مرحله تبدیل موجک از سیگنال حامل و انتخاب زیرباندهای بهینه‌ی آن، عملیات جاسازی بر طبق الگوریتم ارائه شده صورت می‌پذیرد. نتایج حاصل از شبیه‌سازی‌ها نشان می‌دهد این روش ضمن بالا بردن امنیت ارسال اطلاعات محرمانه در این شبکه‌ها، از پیچیدگی محاسباتی و انرژی مصرفی کمتری نسبت به دیگر روش‌های ارائه شده در این زمینه برخوردار می‌باشد.*

**کلید واژه‌ها:** *نهان‌نگاری، شبکه‌های سنسور بی‌سیم، سیگنال محرمانه، سیگنال حامل، امنیت اطلاعات.*

## ۱. مقدمه

شبکه‌های سنسور بی‌سیم[۱]، شبکه‌هایی رو به گسترش هستند و می‌توانند نقش مهمی را در جمع‌آوری و انتقال اطلاعات ایفا کنند. کاربرد این شبکه‌ها، به ویژه در مناطق حساسی که به راحتی قابل دسترسی نیستند، به شدت در حال گسترش می‌باشد. از جمله‌ی این مناطق، می‌توان به مناطق مرزی نظامی اشاره کرد. کنترل ترافیک، مراقبت‌های بهداشتی، زیستی و دارویی، عملیات نجات و گزارش‌های نظامی-امنیتی و جاسوسی از موارد استفاده از این شبکه‌ها می‌باشند [۱و۲]. در واقع شبکه‌های سنسور بی‌سیم، شبکه‌های چند پرشه‌ای هستند که دارای ماهیت اشتراکی و قدرت مدیریت داخلی، بدون نظارت مستقیم می‌باشند[۱و۲]. این شبکه‌ها از تعداد زیادی سنسور، که در این مقاله نود نامیده می‌شوند، تشکیل شده‌اند. نودها در شبکه‌های سنسور بی‌سیم توانایی حس کردن، جمع‌آوری، انتقال اطلاعات و ارتباط با یکدیگر را دارند. با توجه به برخی از کاربردهای این شبکه‌ها، اطلاعاتی که در بین نودها انتقال پیدا می‌کنند، می‌توانند بسیار حساس و تعیین‌کننده باشند. با توجه به نحوه‌ی عملکرد این شبکه‌ها، چالش‌های امنیتی زیادی در این شبکه‌ها وجود دارد.

استراق سمع[۲] از جمله حملات رایجی است که دشمن برای دسترسی به اطلاعات محرمانه انجام می‌دهد. به این منظور اتخاذ شیوه‌ی مناسبی جهت تضمین امنیت در ارسال سیگنال‌های صحبت محرمانه، ضروری به نظر می‌رسد.

در شبکه‌های سنسور بی‌سیم به دلیل محدودیت در توانایی انجام محاسبات، انرژی، پهنای باند و انباره[۳]،

روش‌های رایج و سنتی رمزنگاری با استفاده از کدهای محرمانه، قابل پیاده‌سازی نمی‌باشد. بنابراین بایستی از روش‌هایی با پیچیدگی‌های محاسباتی کمتر و مناسب‌تر برای ارسال نامحسوس اطلاعات محرمانه، در این نوع شبکه‌ها استفاده نمود. این روش بایستی ضمن قابل پیاده‌سازی بودن از لحاظ محاسباتی، منطبق بر محدودیت‌های موجود در نودها نیز باشد.

نهان‌نگاری[4] از جمله تکنیک‌های ارسال مخفی اطلاعات می‌باشد که می‌تواند با طراحی مناسب بر خصوصیات و محدودیت‌های موجود در شبکه‌های سنسور بی‌سیم منطبق باشد. بنابراین در این مقاله سعی شده روشی بر مبنای نهان‌نگاری دیجیتال برای پنهان‌سازی اطلاعات محرمانه ارائه شود. عموماً از نهان‌نگاری به منظور رسیدن به دو هدف عمده، تصدیق مالکیت اطلاعات و ارسال نامحسوس اطلاعات محرمانه، استفاده می‌شود. در نهان‌نگاری به منظور ارسال اطلاعات محرمانه، اگرچه به ظاهر اطلاعاتی ارسال می‌شوند ولی این اطلاعات از اهمیت بالایی برخوردار نیستند و یا ممکن است اطلاعاتی نامعتبر باشند. اما مسئله‌ی حائز اهمیت در این ارتباط، اطلاعات محرمانه‌ای است که به شکل نامحسوسی انتقال می‌یابند. در واقع در این روش سیگنال صحبت محرمانه در پوشش سیگنال صحبتی که سیگنال صحبت حامل نام دارند، جاسازی و ارسال می‌شوند.

این جاسازی بایستی به شکلی صورت پذیرد که در صورت شنود ارتباط توسط دشمن، سیگنال نهان‌نگاری شده کیفیت مطلوب را داشته باشد و ایجاد تغییرات در سیگنال حامل از نظر شنیداری، به راحتی قابل تشخیص نباشد. ضمن این که سیگنال محرمانه قبل از جاسازی در سیگنال حامل با استفاده از روش معرفی شده، هم فشرده‌سازی و هم رمزنگاری می‌شود. بدین ترتیب امنیت ارسال محرمانه‌ی اطلاعات افزایش داده خواهد شد.

در این مقاله منظور از سیگنال محرمانه، همان سیگنال صحبت محرمانه و منظور از سیگنال حامل نیز سیگنال صحبت حامل می‌باشد. سیگنالی که از جاسازی سیگنال محرمانه در سیگنال حامل تولید می‌شود، سیگنال نهان‌نگاری شده نامیده شده است.

در چند سال اخیر تحقیقات زیادی در زمینه‌ی نهان نگاری دیجیتال بر روی داده‌هایی مانند صوت، تصویر، ویدیو و حتی متن‌ها و منابع اطلاعاتی، در شبکه‌های معمول صورت پذیرفته است[3-5]. ولی تحقیقاتی محدودی در این زمینه، بر روی شبکه‌های سنسور بی‌سیم انجام شده است [6-10]. از جمله تحقیقاتی که در زمینه‌ی امنیت در انتقال اطلاعات بر اساس روش‌های نهان‌نگاری در شبکه‌های سنسور بی‌سیم صورت گرفته است، به شرح زیر می‌باشد:

در [6]، الگوریتمی برای تولید شناسه‌ی امنیتی برای بسته‌های ارسالی معرفی گردیده است. این شناسه با استفاده از الگوریتم جاسازی که در آن تعریف شده، در قسمت اطلاعات انتقالی[5] بسته‌ها، جاسازی می‌شوند. این بسته‌ها در کل شبکه منتقل می‌شوند ودر ایستگاه گیرنده‌ی مرکزی، بسته‌های اصلی شناسایی و اطلاعات آن‌ها استخراج می‌شود. در [7]، روش نهان نگاری با تحمیل یکسری از محدودیت‌هایی که در حین عملیات حس کردن اطلاعات و یا پردازش اطلاعات در سنسورها اعمال می‌شود، ترکیب شده است. این محدودیت‌ها با شناسه‌ای که به صورت رمزنگاری شده در اطلاعات جاسازی شده است متناسب می‌باشد. در برخی روش‌ها نیز از نهان‌نگاری تنها برای جلوگیری از دسترسی کاربران غیر مجاز به اطلاعات [8]، و یا تضمین و تشخیص تمامیت رشته بیت‌های دریافتی [9]، استفاده شده است. در مواردی نیز به انتقال امن اطلاعات محرمانه، پرداخته شده است. در این روش داده‌های محرمانه بر طبق الگوریتم پیشنهاد شده در داده‌های معمولی، پیش از ارسال جاسازی شده و سپس ارسال می‌گردد[10].

در روش پیشنهادی دو نوع سیگنال صحبت مورد استفاده قرار می‌گیرد. سیگنال حامل که می‌تواند توسط خود نود نیز تولید شود و سیگنال محرمانه که

حاوی اطلاعات محرمانه است که نبایستی دشمن از آن اطلاع پیدا کند. مراحل انجام کار بدین شکل است که ابتدا از سیگنال حامل چند مرحله تبدیل موجک[6] گرفته می‌شود و سیگنال را به چندین زیر باند تقسیم می‌کند. سپس زیر باندهای بهینه برای جاسازی سیگنال محرمانه انتخاب می‌شوند. این زیر باندهای بهینه با توجه به روشی که برای جاسازی اطلاعات در نظر گرفته شده است، مشخص می‌شوند. در ادامه بایستی سیگنال محرمانه را برای جاسازی در سیگنال حامل آماده نمود. برای این امر ابتدا سیگنال حامل محرمانه با استفاده از تبدیل موجک فشرده‌سازی می‌شود. این فشرده‌سازی به صورت رشته بیت صورت می‌پذیرد و به نوعی همزمان عمل رمزنگاری نیز در این مرحله انجام می‌شود. سپس با استفاده از مراحل جاسازی معرفی شده، سیگنال محرمانه که به صورت رشته بیتی نامفهوم درآمده است، در داخل زیر باندهای بهینه‌ی سیگنال حامل جاسازی و سپس ارسال می‌گردد.

در این مقاله خصوصیات محیطی که در شبیه‌سازی‌ها در نظر گرفته شده، منطبق با محیط جنگلی می‌باشد[11]. کانال ارتباطی موجود بین نودهای شبکه از نوع کانال رایسین[7] فرض شده است. نرخ نمونه برداری سیگنال 8 kb/s در نظر گرفته شده است.

نودهایی که در شبکه‌های سنسور بی‌سیم مورد استفاده قرار می‌گیرند، از لحاظ توانایی در انجام عملیات‌های محاسباتی و پردازشی عمدتاً قابلیت‌های بیشتری نسبت به ریزپردازنده‌های معمولی موجود دارند. با توجه به این مطلب در این مقاله توانایی انجام محاسبات با استفاده از ریزپردازنده‌های PIC[8]، که قابلیت پردازش دیجیتال سیگنال‌های صوت و صحبت را دارا هستند، به عنوان نمونه‌ای از نودهای شبکه‌ی سنسور، مورد آزمایش قرار گرفته است. این مقاله دارای ساختاری به صورت زیر می‌باشد:

ابتدا ساختاری که برای شبکه‌های سنسور بی‌سیم در نظر گرفته شده است و نحوه‌ی ارسال و بسته‌بندی اطلاعات به طور مختصر توضیح داده خواهد شد. در بخش سوم به بررسی دلایل استفاده از نهان‌نگاری در شبکه‌های سنسور پرداخته شده است. در بخش چهارم دلایل استفاده از روش پیشنهادی به منظور نهان‌نگاری صحبت در شبکه‌های سنسور بی‌سیم بررسی شده است. سپس در بخش پنجم نحوه‌ی انتخاب زیرباندهای بهینه مورد بررسی قرار می‌گیرد. در بخش ششم روش پیشنهادی به منظور فشرده‌سازی و رمزنگاری سیگنال محرمانه معرفی می‌شود. در بخش هفتم مراحل و چگونگی عملیات نهان‌نگاری در روش پیشنهادی بیان می‌شود. در بخش هشتم نحوه‌ی استخراج و بازیابی سیگنال محرمانه مورد بررسی قرار می‌گیرد. در بخش نهم نتایج و ویژگی‌های حاصل از اعمال این روش، بر شبکه‌های سنسور بی‌سیم ارائه شده است.

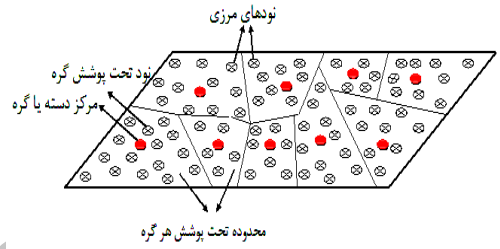
## 2. شبکه‌های سنسور بی‌سیم

در این بخش، ابتدا ساختار کلی در نظر گرفته شده برای شبکه‌های سنسور بی‌سیم و سپس نحوه‌ی ارسال و بسته‌بندی اطلاعات در نودهای این شبکه‌ها به اختصار توضیح داده می‌شود.

### 2.1. ساختار شبکه‌های سنسور بی‌سیم

شبکه‌های سنسور بی‌سیم از تعداد زیادی سنسور، که به آنها نود گفته می‌شود، تشکیل شده است. این نودها یا بر طبق الگوی خاص و یا به صورت تصادفی در محیط پخش می‌شوند[1و2]. نودها با توجه به برد کمی که دارند از طریق ارتباط با یکدیگر، اطلاعات را منتقل می‌کنند. نودهای کل شبکه برای ارتباط با یکدیگر به نوعی به محدوده‌های متفاوتی دسته بندی[9] می‌شوند. در بین نودهای فعال در هر مرحله‌ی کاری شبکه، نودهایی وجود دارند که توانایی و برد بیشتری نسبت به دیگر نودها دارند. به این نودها گره یا مرکز دسته[10] گفته می‌شود. هر گره تعدادی نود را تحت

پوشش قرار می‌دهد، که این نودها یا به طور مستقیم و یا توسط دیگر نودها با مرکز دسته یـا گـره در ارتبـاط هستند. با توجه به این تعریف شبکه بـه محـدوده‌هـای متفاوت دسته‌بندی می‌شوند که هر محدوده شامل یک نود به عنوان مرکز دسته یا گره و نودهای تحت پوشش آن می‌باشد. در شکل 1، نمایی سـاده از تقسـیم‌بنـدی محدوده‌های مختلـف، نمـایش داده شـده اسـت. ایـن محدوده‌ها، از طریـق گـره‌هـا و یـا نودهـای مـرزی بـا یکدیگر در ارتباط هستند [1و2].




***شکل 1: تقسیم‌بندی نودهای شبکه‌ی سنسور بی‌سیم به محدوده‌های مختلف***

گره‌ها اطلاعات خود را بـه سـمت دروازه‌ی ارسـال اطلاعات که سینک[11] نامیده می‌شود ارسال می‌کننـد و از طریق سینک با ایستگاه مرکزی[12] در ارتباط هستند. این دسته‌بندی نودها و گره‌ها پس از هر دوره‌ی کـاری در نظر گرفته شده برای نودها به روز می‌شوند و ممکن است با توجه به انـرژی ذخیـره شـده در نودهـا تغییـر کنند.

### 2.2. نحوه‌ی بسته‌بندی و ارسال اطلاعات

با توجه به مدل ارائه شده در [6 و10] بسته‌ها بدین ترتیب مدل می‌شوند:

$$Packet = (head, send\text{-}data)$$

در اینجا سربرگ[13] بسته شامل اطلاعاتی همچون اطلاعات مسیریابی و طول پاکت ودیگر پارامترهایی است که در اینجا طبق استاندارد zigbee در نظر گرفته می‌شوند. قسمت اطلاعات انتقالی[14] محتوی اطلاعات یا سیگنال‌هایی است که هم در پروسه‌ی حس کردن توسط هر نود، جمع‌آوری می‌شود. پس هر بسته اغلب شامل یک سربرگ و داده‌های جمع‌آوری شده در $k$ چرخه‌ی کاری نود $(S_1,S_2,\ldots,S_k)$ می‌باشد. هر المان دیتای جمع آوری شده، $S_i$، به شکل $Si = (t,d_1,d_2,\ldots,d_n)$ که $i$ به چرخه‌های کاری نود در پروسه‌ی حس کردن اطلاعات اشاره دارد $[(i=1,2,\ldots,m)]$. $t$ اشاره به زمان زمان حس کردن اطلاعات دارد و $dj=(j=1,2,\ldots,n)$ المان‌هایی است که برای نود بایستی اطلاعات مربوط به آنها را حس کند. این اطلاعات می‌توانند از نوع صوت، تصویر، ویدئو و حتی مقادیر مربوط به پارامترهایی مانند دما و رطوبت باشند.

ارسال توسط نود زمانی صورت می‌گیرد که بافر نود کاملا پر شده باشد، [6 و 10]، پس تا زمان کامل شدن بافر، چرخه‌های کاری نود (حس کردن اطلاعات ) ادامه می‌یابد. در نتیجه‌ی این ارسال با تأخیر، این امکان فراهم می‌آید که نهان‌نگاری در فریم‌های بزرگ‌تری از سیگنال حامل، صورت بپذیرد که در کاهش محاسبات بسیار مؤثر است.

## 3. دلایل استفاده از نهان‌نگاری در شبکه‌های سنسور بی‌سیم

یکی از راه‌های جلوگیری از استراق سمع، رمزنگاری اطلاعات می‌باشد. دو روش کلی برای رمزنگاری اطلاعات وجود دارد، رمزنگاری با کلیدهای متقارن و یا رمزنگاری با کلیدهای عمومی[15]، که به دلیل محدودیت‌ها و چالش‌های امنیتی که ماهیت شبکه‌های سنسور بی‌سیم دارند، در این شبکه‌ها قابل پیاده‌سازی نمی‌باشند[1و6]. دلیل این مسئله آن است که اساساً در شبکه‌های سنسور بی‌سیم به دلیل محدودیت انباره، انرژی و قابلیت‌های محاسباتی و پردازشی، نمی‌توان از رمزنگاری با کلیدهای عمومی استفاده نمود. در مورد رمزنگاری با کلیدهای متقارن نیز به دلیل عدم نظارت مستمر و مستقیم بر نودهای شبکه، که از چالش‌های اساسی این نوع شبکه‌ها می‌باشد، در صورتی که دشمن

به اطلاعات یک نود دسترسی پیدا کند و بتواند این کلیدها را بدست آورد، به راحتی می‌تواند اطلاعات کل شبکه را شنود کند و در ایستگاه مرکزی این امر قابل تشخیص نباشد.

با توجه به این که دشمن می‌تواند به راحتی از برقراری ارتباط بین نودها با خبر باشد، بایستی از روش‌هایی استفاده نمود که دسترسی به اطلاعات محرمانه امکان‌پذیر نباشد. در واقع در اینجا باید از روش‌هایی استفاده نمود که هر نود به نوعی بتواند تأمین کننده‌ی امنیت اطلاعات محرمانه‌ی خود باشد. رمزنگاری و نهان‌نگاری دو روش متداول در تأمین امنیت اطلاعات محرمانه در این گونه موارد می‌باشند. طبق توضیحات ارائه شده رمزنگاری سنتی در شبکه‌های سنسور بی‌سیم نمی‌تواند روش مناسبی در انتقال اطلاعات محرمانه باشد. بنابراین نهان‌نگاری به عنوان روش دیگر، که با استفاده از آن هر نود می‌تواند امنیت اطلاعات خود را تا حدود زیادی تأمین کند، مورد توجه قرار می‌گیرد. ویژگی نهان‌نگاری این است که اطلاعات محرمانه در قالب اطلاعات معمولی ارسال می‌شوند و در صورت استفاده از روشی مناسب که کیفیت سیگنال نهان‌نگاری شده را حفظ کند، چنانچه اطلاعات شنود هم شود قابل تشخیص نمی‌باشد. در این صورت احتمال دسترسی دشمن به اطلاعات محرمانه بسیار پایین است ضمن این که ارتباط به راحتی می‌تواند در قالب یک سری اطلاعات معمولی همچنان برقرار باشد. حتی در برخی موارد می‌توان اطلاعات محرمانه را در قالب اطلاعاتی جعلی ارسال و دشمن را در صورت شنود اطلاعات گمراه نمود. با توجه به تنوع روش‌های موجود برای نهان‌نگاری صحبت، می‌توان روش‌هایی را اتخاذ نمود که بر محدودیت‌های شبکه‌های سنسور منطبق باشد و بتواند امنیت مورد نیاز را برای اطلاعات هر نود فراهم آورد.

## 4. چگونگی انتخاب روش مناسب به منظور نهان‌نگاری در شبکه‌های سنسور بی‌سیم

در نهان‌نگاری سیگنال صحبت در شبکه‌های سنسور بی‌سیم بایستی از روش‌هایی برای پردازش سیگنال صحبت استفاده نمود که قابل پیاده‌سازی بر روی نودهای شبکه‌های سنسور بی‌سیم نیز باشند و بتوانند حداکثر امنیت را با کمترین هزینه فراهم آورند. ضمن این که روش مورد استفاده به منظور نهان‌نگاری، با توجه به محدودیت‌ها و ویژگی‌های موجود در شبکه‌های سنسور بی‌سیم بایستی شرایط یک نهان‌نگاری کور و مقاوم را فراهم کند.

روش‌های زیادی برای نهان‌نگاری سیگنال صحبت ارائه شده که با توجه به ارتباط بین نودها (بی‌سیم)، نوع نهان‌نگاری مورد نیاز (کور و مقاوم) و به ویژه محدودیت‌های موجود در نودهای شبکه‌های سنسور، نمی‌توان از بسیاری از این روش‌ها استفاده نمود. ضمن این که روش مورد استفاده بایستی تا حد امکان دارای نرخ جاسازی بالا باشد به شرطی که به کیفیت سیگنال نهان‌نگاری شده آسیبی وارد نکند. نرخ جاسازی بالا باعث می‌شود که حجم ثابتی از سیگنال محرمانه را بتوان در مراحل کمتری ارسال نمود. در نتیجه هم میزان انرژی در هر نود و هم زمان روشن بودن نودهای فعال در شبکه کاهش می‌یابد، که هر دو عامل باعث افزایش طول عمر کل شبکه می‌گردند.

با توجه به این که اطلاعات به کار برده شده، سیگنال صحبت می‌باشد، استفاده از برخی خصوصیات سیگنال صحبت به منظور نهان‌نگاری در این گونه شبکه‌ها می‌تواند راهگشا باشد. سیگنال‌های صحبت چه در فضای زمانی و چه در فضای فرکانسی دارای خصوصیاتی می‌باشند که می‌توانند در ارائه‌ی روشی مناسب در نهان‌نگاری سیگنال صحبت در شبکه‌های سنسور بی‌سیم مؤثر باشند. خصوصیاتی مانند تفاوت بین محدوده‌ی مقادیر نمونه‌ها در فرکانس‌های مختلف و تفاوت‌های فرکانسی سیگنال صحبت که متناسب با

آستانه‌ی شنوایی انسان از 100 HZ تا 4 KHZ تغییر می‌کند.

با در نظر گرفتن کلیه‌ی عوامل موجود، در این مقاله روشی بر مبنای تبدیل موجک به منظور نهان‌نگاری سیگنال صحبت در این نوع شبکه‌ها پیشنهاد شده است. در ادامه مشاهده خواهد شد که این روش ضمن قابل پیاده‌سازی بودن بر نودهای شبکه‌های سنسور و انطباق با محدودیت‌های این شبکه‌ها، از هر دو فضای زمانی و فرکانسی سیگنال صحبت با کمترین پیچیدگی محاسباتی و به خوبی استفاده نموده است.

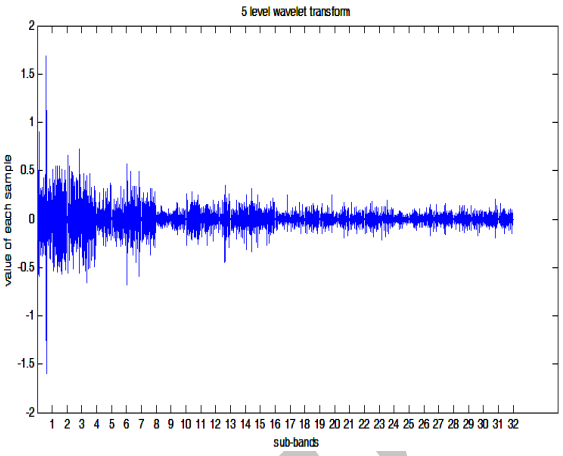
از خصوصیات دیگر استفاده از تبدیل موجک به منظور نهان‌نگاری صحبت در این نوع شبکه‌ها این است که هنگامی که نویز پردازش کم باشد، تبدیل موجک برای کاربردهای نهان‌نگاری با نرخ داده‌ی بالا مناسب است[12]. با توجه به این که اساساً نودها نمی‌توانند پردازش‌های سنگینی را بر روی سیگنال صحبت انجام دهند، در نتیجه بدیهی است که نویز پردازش به خودی خود کم است و با در نظر گرفتن این که در این شبکه‌ها به جاسازی با نرخ بالا نیاز است، این روش حتی می‌تواند کارایی مناسبی در افزایش طول عمر شبکه، نسبت به دیگر روش‌ها که نرخ جاسازی کمتر دارند، داشته باشد.

## 5. انتخاب زیرباندهای بهینه

در نهان‌نگاری سیگنال محرمانه مهم‌ترین اصل، جاسازی سیگنال محرمانه به گونه‌ای است که حتی‌الامکان قابل تشخیص نباشد. به این معنا که سیگنال محرمانه به طریقی در سیگنال حامل جاسازی شوند که در صورت شنود سیگنال ارسالی، مشخص نباشد سیگنال دستکاری شده است. برای این که دستکاری سیگنال حامل قابل تشخیص نباشد، با استفاده از محدوده‌ی آستانه‌ی شنوایی انسان، نهان‌نگاری به شکلی انجام می‌شود که به سختی قابل تشخیص باشد.

بر طبق [13و14] آستانه‌ی شنوایی انسان بر روی پهنای باند 100HZ است. بالاترین فرکانس قابل شنود انسان تا 4KHZ است. برای ایجاد تغییرات نامحسوس در سیگنال با استفاده از تبدیل موجک این پهنای فرکانسی به زیرباندهایی در حدود 100HZ تفکیک می‌شود. برای این منظور از 5 مرحله تبدیل موجک و بانک فیلتر Haar استفاده می‌شود. پس از 5 مرحله تبدیل موجک، سیگنال به 32 زیر باند با پهنای باند در حدود 100HZ تفکیک می‌شود. هر یک از این زیر باندها شامل نمونه‌هایی[16] از سیگنال است که معمولا دارای مقادیر نزدیک به هم هستند. این مقادیر در زیر باندهای پایینی از نمونه‌های با ارزش‌تر سیگنال شروع می‌شود که به عنوان تقریبی از خود سیگنال شناخته می‌شوند و تا زیرباندهای بالایی که شامل نمونه‌های کم اهمیت‌تر هستند ادامه می‌یابد. زیر باندهای بالایی بیشتر شامل جزئیات سیگنال هستند. شکل 2، زیرباندهای حاصل از 5 مرحله تبدیل موجک یک سیگنال صحبت با 320000 نمونه را نمایش می‌دهد. با اعمال این تبدیل بر روی سیگنال، سیگنال به 32 زیرباند که هر کدام حاوی 10000 نمونه هستند، تقسیم می‌شوند.

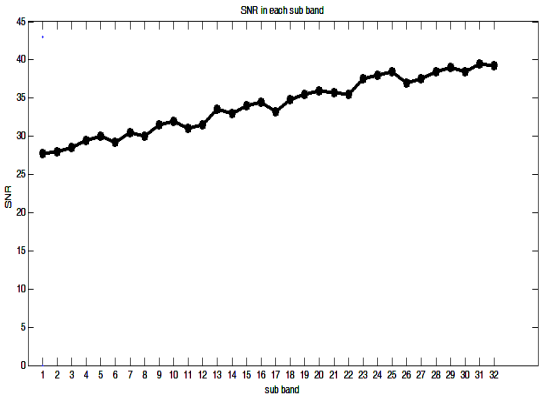
برای انتخاب زیرباندهای بهینه ابتدا بایستی نحوه‌ی جاسازی اطلاعات محرمانه در زیرباندهای سیگنال حامل مشخص شود. در این تحقیق اطلاعات محرمانه در کم ارزش‌ترین بیت‌های[17] هر نمونه از زیر باندهای بهینه‌ی سیگنال جاسازی می‌شود. در واقع در این روش بیت‌های کم ارزش هر نمونه انتخاب می‌شود و بیت‌های اطلاعات محرمانه طبق الگوریتم جاسازی ارائه شده، در آنها قرار می‌گیرد.




*شکل 2: زیر باندهای حاصل از 5 مرحله تبدیل موجک سیگنالی با 320000 نمونه*

به منظور یافتن زیر باندهای بهینه‌ی سیگنال با توجه به این روش جاسازی، در هر یک از زیرباندها در 32مرحله، تعداد مشخصی بیت با این روش جاسازی می‌شود و سپس با عکس تبدیل موجک، SNR در هر مرحله محاسبه می‌شود. زیرباندهای مراحلی که بیشترین SNR را دارا هستند، انتخاب می‌شوند و در اولویت برای جاسازی اطلاعات قرارمی‌گیرند. این مراحل چندین بار با تعداد بیت‌های محرمانه‌ی متفاوت تکرار می‌شود.

مقادیر مشخص شده در نمودار شکل 3 از متوسط‌گیری تعداد متفاوتی از بیت‌های اطلاعات محرمانه که در هر زیرباند جاسازی شده است بدست آمده است. با توجه به شکل 3 مشخص می‌شود که در زیرباندهای بالایی سیگنال‌های حامل که از لحاظ اهمیت در درجه‌ی کمتری نسبت به زیر باندهای دیگر هستند، SNR بزرگتر است. یکی از دلایل این امر آن است که با توجه به مقادیر کوچک این زیرباندها، تغییرات LSB این نمونه‌ها نیز کوچک‌تر بوده است.




*شکل 3: تغییرات زیرباندهای مختلف سیگنال نهان‌نگاری شده نسبت به سیگنال حامل (SNR)*

SNR مشخص شده برای هر زیر باند با استفاده از فرمول (1) بدست آمده است:

$$SNR = 10\log_{10}\frac{S^2}{(S-SW)^2} \qquad (1)$$

که در این فرمول S و SW به ترتیب بیان‌گر سیگنال حامل و سیگنال نهان‌نگاری شده هستند.

## 6. فشرده‌سازی و رمزنگاری سیگنال محرمانه

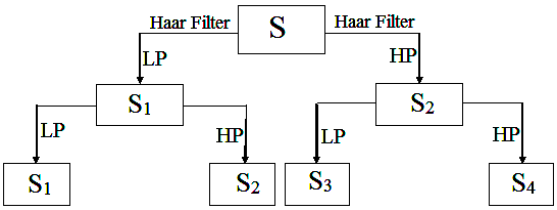
پس از 5 مرحله تبدیل موجک بر روی سیگنال حامل، سیگنال محرمانه بایستی پردازش شود. با توجه به خواص شبکه‌های سنسور بایستی توجه داشت که حتی‌الامکان کمترین حجم اطلاعات ارسال شود. از طرفی بایستی سیگنال محرمانه در گیرنده به خوبی قابل تشخیص باشد. همچنین همان طور که اشاره شد، سیگنال حامل بایستی تا حد امکان دچار تغییرات نامحسوسی شود تا در صورت شنود، نهان‌نگاری قابل تشخیص نباشد. بدین منظور تا جایی که به اصل سیگنال محرمانه خدشه‌ای وارد نشود بایستی حجم این سیگنال را کاهش داد تا بتوان حجم مشخصی از سیگنال محرمانه را تحت سیگنال حامل با کمترین تغییرات و مراحل ارسال، انتقال داد.

در این قسمت روش جدیدی برای فشرده‌سازی

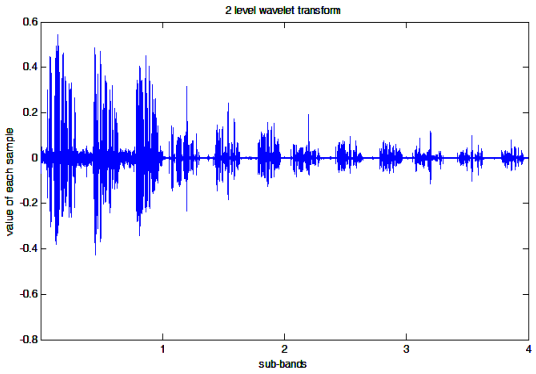
همراه با رمزنگاری سیگنال محرمانه ارائه شده است. در این روش اصول کار بر مبنای تبدیل موجک و نگاشت مقادیر نمونه‌های هر زیرباند به مقادیر کمتر به منظور تخصیص تعداد بیت کمتر به برخی نمونه‌ها، می‌باشد.

ابتدا از سیگنال محرمانه تبدیل موجک می‌گیریم. در اینجا از دو مرحله تبدیل موجک استفاده شده است. تعداد مراحل تبدیل موجک با توجه به دقت و میزان فشرده‌سازی مورد نیاز تغییر پیدا کند. با افزایش مراحل تبدیل موجک دقت در این روش بالاتر رفته ولی بطور طبیعی میزان فشرده‌سازی پایین می‌آید. بنابراین بایستی تعادل نسبی بین دقت مورد نیاز و میزان فشرده‌سازی برقرار نمود. یکی از مسائل قابل توجه در معیار دقت، خصوصیات مسیر ارتباطی یا همان ویژگی‌های کانال ارتباطی بین نودها است. با توجه به محیط و کانالی که در این تحقیق انتخاب شده و ویژگیهای مربوط به آن و در نتیجه SNR دریافتی در گیرنده که در شبیه‌سازی‌ها بدست آمده، فرض شده با دو مرحله تبدیل موجک میزان دقت و فشرده‌سازی مورد نیاز حاصل خواهد شد.

پس از دو مرحله تبدیل موجک سیگنال محرمانه به 4 زیرباند تقسیم خواهد شد. همان طور که در شکل 5 مشخص است، زیرباندهای پایینی دارای نمونه‌های با مقادیر بیشتر هستند. در واقع طبق تعریف تبدیل موجک، به نوعی تقریبی از خود سیگنال محرمانه نیز به حساب می‌آیند. در زیرباندهای بالایی نمونه‌ها مقادیر کمتری دارند و بر طبق تعریف تبدیل موجک، حاوی جزئیات سیگنال هستند. مقادیر موجود در زیر باندهای پایینی معمولا در محدوده‌ی بالاتری قرار دارند. همین تفاوت بین مقادیر نمونه‌ها در زیر باندهای مختلف، مبنای ارائه‌ی این روش فشرده‌سازی برای سیگنال صحبت می‌باشد.




*شکل 4: فلوچارت تبدیل موجک به همراه شماره‌گذاری زیر باندها*




*شکل 5: مقادیر نمونه‌ها در زیرباندهای حاصل از دو مرحله تبدیل موجک یک سیگنال با 80000 نمونه*

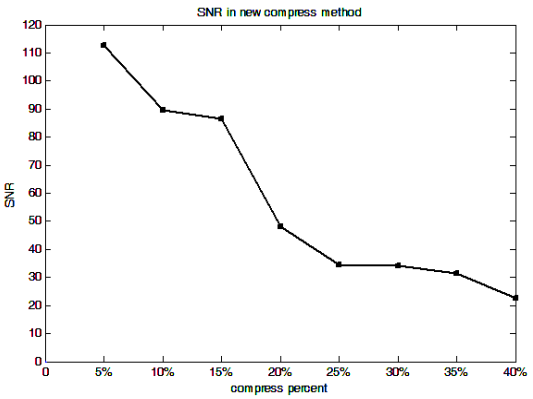
در این روش فشرده‌سازی برای نمایش نمونه‌ها، با توجه به مقادیر و اهمیت نمونه‌های هر زیر باند، تعداد بیت متفاوتی به هر زیر باند تخصیص داده می‌شود. به زیرباندهای پایینی که نمونه‌های آن مقادیر بیشتری دارند و از اهمیت بیشتری برخوردارند تعداد بیت بیشتری تخصیص داده خواهد شد و به زیرباندهای پایینی که اهمیت کمتری دارند و مقادیر آنها در محدوده‌ی کمتری هستند، تعداد بیت کمتری تعلق می‌پذیرد.

روند فشرده‌سازی در این مقاله به این صورت است که از سیگنال محرمانه فریم به فریم، تبدیل موجک گرفته می‌شود. با توجه به نحوه‌ی بسته‌بندی و ارسال اطلاعات در شبکه‌های سنسور بی‌سیم و حجم در نظر گرفته شده‌ی سیگنال محرمانه در این مقاله که در حدود 20% درصد سیگنال حامل برای جاسازی می‌باشد، پس از مشخص شدن زیرباندها و مقادیر نمونه‌های هر زیرباند، مقادیر نمونه‌های موجود در هر

زیرباند، با توجه به کیفیت و دقت مورد نیاز، به مقادیر کمتر با رشته بیت کمتر، به صورت یکتا، نگاشت می‌شوند.

فرض کنید هر نمونه از هر فریم سیگنال محرمانه با 32 بیت نمایش داده می‌شود. با تبدیل موجک زیرباندهای پایینی، نمونه‌های با مقادیر بیشتر و زیرباندهای بالایی، نمونه‌های با مقادیر کمتر را در بر می‌گیرند (شکل 5). پس به زیرباند اول که از اهمیت بیشتری نیز برخوردار است 32بیت اختصاص داده می‌شود. به زیر باند دوم که نسبت به زیر باند اول از مقادیر و اهمیت کمتری برخوردارند 24بیت و به زیر باندهای 3و4، 16بیت اختصاص داده می‌شود. در این صورت رشته بیتی که سیگنال با آن نمایش داده می‌شود، بیش از 31% فشرده‌سازی شده است.

با عکس عملیات نگاشت در گیرنده، که به صورت یکتا و یک به یک، صورت گرفته است، سیگنال بازیابی می‌شود. با توجه به آزمون‌های شنوایی انجام شده بر روی سیگنال صحبت، با این روش می‌توان رشته بیت سیگنال را تا 37% با کیفیت قابل قبولی فشرده‌سازی نمود(شکل 6). در این حالت سیگنال دارای SNR در حدوده 30dB و دارای کیفیت مناسب به لحاظ شنوایی می‌باشد.

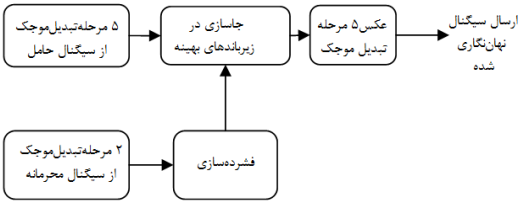



***شکل 6: مقادیر SNRهای مربوط به فشرده‌سازیهای متفاوت سیگنال طی دو مرحله تبدیل موجک***

حال این رشته بیت بایستی به نحوی داخل سیگنال حامل جاسازی شود که قابلیت بازیابی داشته باشد و گیرنده بتواند مستقل از سیگنال حامل، سیگنال محرمانه را استخراج کند.

## 7. مراحل و چگونگی عملیات نهان‌نگاری

در شکل 7 مراحل نهان‌نگاری نشان داده شده است.




***شکل 7: فلوچارت مراحل انجام عملیات نهان‌نگاری در روش پیشنهادی***

مراحل انجام نهان‌نگاری به این ترتیب صورت می‌پذیرد که ابتدا از سیگنال حامل، که بخشی از انباره‌ی هر نود به آن اختصاص پیدا می‌کند، 5 مرحله تبدیل موجک گرفته می‌شود. این تبدیل زمانی صورت می‌پذیرد که اطلاعات جمع‌آوری شده در انباره به حجم مورد نظر برای ارسال رسیده باشد. سپس رشته بیت حاصل از حجم مشخصی از سیگنال محرمانه، داخل زیرباندهای بهینه‌ی سیگنال حامل قرار می‌گیرند. در برخی روش‌ها، نمونه‌ها عیناً جایگزین نمونه‌های زیرباندهای بهینه شده‌اند[13]، اما در روش جاسازی پیشنهادی، نمونه‌ها به صورت رشته بیت در LSB نمونه‌های موجود در زیرباندهای بهینه جاسازی می‌شوند. این جاسازی با بهره‌گیری از الگوریتم جاسازی ارائه شده در [10]، صورت پذیرفته است. رشته بیت حاصل از سیگنال نهان‌نگاری شده، در قسمت اطلاعات انتقالی بسته‌های ارسالی نود ذخیره سازی می‌شوند و پس از پر شدن انباره‌ی نود ارسال می‌شوند. در جدول 1 نتایج حاصل از اعمال هر دو روش نشان داده شده است. در مراحل آزمایش 16 زیرباند بالایی به عنوان زیرباندهای بهینه انتخاب

شده‌اند. برای نمایش تفاوت در توزیع‌های مختلف، از معیار SNR بهره گرفته شده است.

البته نتایج جدول 1، نتایج حاصل از کل روش پیشنهادی نیست و صرفاً مقایسه‌ای بین روش‌های جاسازی صورت گرفته است. در این مقایسه سیگنال محرمانه بدون فشرده‌سازی در زیرباندهای بهینه جاسازی شده‌اند. برای دقت بیشتر در محاسبات فریم‌ها کوچک انتخاب شده‌اند.

همان طور که در جدول مشخص است هر چه رشته بیت محرمانه گسترده‌تر توزیع و جاسازی شود، تغییرات سیگنال نامحسوس‌تر و در نتیجه امنیت ارسال بیشتر است. به عنوان مثال فرض کنید هر فریم از سیگنال محرمانه بخواهد در 5 فریم از سیگنال حامل جاسازی شود. به عنوان مثال در هر فریم سیگنال حامل که 160 نمونه است به طور میانگین بایستی 32 نمونه جاسازی شود. در این صورت به هر یک از زیر باندهای بهینه دو نمونه برای جاسازی تعلق می‌پذیرد. در صورتی که این دو نمونه مستقیماً با دو نمونه دیگر جایگزین شوند، SNR در حدود 39dB می‌باشد. در حالی‌که در LSB هر 5 نمونه از هر یک از زیرباندهای بهینه توزیع شوند، SNR تا حدود 75dB خواهد رسید که تشخیص سیگنال حامل و سیگنال نهان‌نگاری شده در این صورت بسیار سخت‌تر خواهد بود. ضمن این که با این روش حجم اطلاعاتی که تاحد امکان می‌تواند نامحسوس جاسازی شود، بالاتر می‌رود.

***جدول 1: مقایسه تفاوت در توزیع‌های مختلف در روش جاسازی پیشنهادی با استفاده از معیار SNR***

| | | | |
|---|---|---|---|
| تعدادنمونه‌های‌هرفریم‌سیگنال‌حامل | 160 | 160 | 160 |
| تعدادنمونه‌های‌هرفریم‌سیگنال‌محرمانه | 16 | 32 | 48 |
| جاگزینی نمونه به نمونه | 63 | 39 | 21 |
| توزیع درLSB دو نمونه‌از هر زیرباند | 89 | 48 | 35 |
| توزیع درLSB سه نمونه از هر زیرباند | 97 | 62 | 39 |
| توزیع درLSB چهار نمونه‌از هرزیرباند | 102 | 71 | 41 |
| توزیع درLSB پنج نمونه‌از هر زیرباند | 107 | 75 | 43 |

حال مسئله‌ای که مطرح می‌شود چگونگی جاسازی رشته بیت حاصل از فشرده‌سازی سیگنال محرمانه است. با توجه به این که نمونه‌های این سیگنال طی فشرده‌سازی انجام شده، با تعداد بیت‌های متفاوتی نمایش داده شده‌اند، بایستی راه‌کاری برای جاسازی این رشته بیت اتخاذ شود که گیرنده مستقل از سیگنال حامل بتواند بیت‌های آن را به خوبی استخراج کند.

با توجه به روش ارائه شده در [13]، و نتایج حاصل از آزمایشات انجام شده می‌توان نتیجه گرفت که جاسازی اطلاعات در زیرباندها، تأثیر چندانی بر تبدیل موجک ندارد. بر پایه‌ی این ویژگی می‌توان روشی ارائه نمود که رشته بیت حاصل از فشرده‌سازی سیگنال محرمانه را به خوبی استخراج نماید و با استفاده از همین قابلیت سیگنال محرمانه را با دقت مناسبی بازیابی نمود.

با توجه به جدول 1، مشاهده می‌شود که با جاسازی مناسب می‌توان تا حدود 25% از حجم سیگنال حامل، سیگنال محرمانه در آن جاسازی نمود. با توجه به فشرده‌سازی ارائه شده این مقدار می‌تواند تا 40% افزایش پیدا کند.

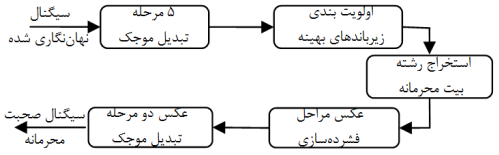
از این قسمت بحث به بعد، بحث بر روی رشته بیت حاصل از فشرده‌سازی سیگنال محرمانه می‌باشد. همان طور که اشاره شد در این فشرده‌سازی به زیرباندهای مختلف تعداد بیت‌های متفاوتی تعلق می‌پذیرد. پس روند کار بدین صورت ادامه می‌یابد که ابتدا رشته بیت مربوط به نمونه‌های هر یک از 4 زیرباند سیگنال محرمانه که در مرحله‌ی فشرده‌سازی حاصل شده‌اند، مشخص می‌شوند. با توجه به حجم اطلاعاتی که بایستی در سیگنال حامل جاسازی شوند، تعداد زیرباندهای بهینه انتخاب شده و رشته بیت محرمانه به ترتیب عملکرد بهینه‌ی زیرباندها، در آنها جاسازی می‌شوند. به عنوان مثال اگر حجم رشته بیت محرمانه برای هر بار ارسال توسط نود، در حدود 20% حجم رشته بیت نمایشگر سیگنال حامل باشد، جاسازی به

این ترتیب صورت می‌پذیرد که ابتدا رشته بیت نمایش دهنده‌ی مقادیر نمونه‌های زیر باند اول سیگنال محرمانه، که دارای مقادیر بیشتر و اهمیت بالاتری می‌باشند، به ترتیب در زیرباندهای 21-32 سیگنال حامل که علاوه بر بهینه بودند تغییرات در آنها کمتر محسوس است، جاسازی می‌شوند. سپس نوبت به رشته بیت مربوط به زیر باند دوم سیگنال محرمانه می‌رسد که به ترتیب در زیرباندهای 13-20 سیگنال حامل جاسازی می‌شوند و در نهایت رشته بیت مربوط به زیرباندهای سوم و چهارم که اهمیت و حجم کمتری دارند و در زیرباندهای 9-12 جاسازی می‌شوند. با توجه به شکل 3 مشاهده می‌شود که زیرباندهای 1- 8 مناسب جاسازی نمی‌باشند.

با اعمال این دسته‌بندی برای جاسازی اطلاعات مقداری از کیفیت نهان‌نگاری کاسته می‌شود. به عنوان مثال با توجه به جدول 1، SNR برای این حجم در نظر گرفته شده برای جاسازی (مستقل از فشرده‌سازی) بایستی در حدود 75dB باشد این در حالیست که SNR بدست آمده پس از اعمال این دسته‌بندی در روش جاسازی در حدود 69dB می‌باشد. استفاده از زیرباندهایی که نسبت به زیرباندهای بهینه حساسیت بیشتری نسبت به جاسازی اطلاعات دارند می‌تواند یکی از دلایل مهم این کاهش کیفیت باشد.

## 8. استخراج و بازیابی سیگنال محرمانه در گیرنده مستقل از سیگنال حامل

پس از نهان‌نگاری و ارسال سیگنال، سیگنال نهان‌نگاری شده از طریق نودهای موجود در مسیر ارتباطی به سمت گیرنده‌ی مرکزی ارسال می‌شوند. گیرنده پس از دریافت سیگنال نهان‌نگاری شده بایستی بتواند سیگنال محرمانه را مستقل از سیگنال حامل بازیابی کند. در این مرحله گیرنده با انجام عکس مراحل جاسازی رشته بیت بدست آمده از فشرده‌سازی سیگنال محرمانه را از رشته بیت سیگنال دریافتی استخراج می‌کند. پس از این مرحله با عکس عملیات فشرده‌سازی که به صورت یکتا صورت پذیرفته است، سیگنال محرمانه را بازیابی می‌کند(شکل 7).




***شکل 8: فلوچارت مراحل بازیابی سیگنال محرمانه در گیرنده***

مطابق فلوچارت ارائه شده در شکل 8، گیرنده پس از دریافت سیگنال نهان‌نگاری شده از آن 5 مرحله تبدیل موجک می‌گیرد. پس از تبدیل موجک، زیرباندهای بهینه‌ی سیگنال که را با توجه میزان فشرده‌سازی و حجم اطلاعات محرمانه، هم در نود فرستنده و هم در گیرنده تعریف شده است، انتخاب می‌کند. سپس با انتخاب LSB، نمونه‌های زیرباندهای بهینه، عکس الگوریتم جاسازی را انجام می‌دهد. در این مقاله با توجه به استفاده از الگوریتم جاسازی ارائه شده در [10]، از عکس این الگوریتم که در همین مقاله ارائه شده است، به منظور استخراج رشته بیت جاسازی شده، استفاده می‌شود.پس از استخراج رشته بیت نوبت به بازیابی سیگنال محرمانه می‌رسد. در این مرحله با توجه به این که در مرحله‌ی جاسازی، رشته بیت حاصل از فشرده‌سازی هر زیرباند سیگنال محرمانه، در زیرباندهای مشخصی از سیگنال حامل جاسازی شده‌اند، رشته بیت مربوط به هر زیرباند به راحتی استخراج می‌شوند. پس از مشخص شدن رشته بیت محرمانه، عکس مراحل فشرده‌سازی مربوط به هر زیرباند صورت می‌گیرد و مقادیر نمونه‌های سیگنال محرمانه که نگاشت یکتایی داشته‌اند بدست می‌آیند. سپس با عکس تبدیل موجک دو مرحله‌ای، سیگنال صحبت محرمانه حاصل می‌شود. البته پس از طی این مراحل، کیفیت سیگنال محرمانه کاهش پیدا می‌کند. به طور مثال، در موردی که در بخش قبل در نظر گرفته شده SNR، تا حدوده 57dB پایین می‌آید.

## 9. نتایج حاصل از شبیه‌سازی‌ها

در بخش‌های قبلی نتایج مربوط به هر مرحله از روش پیشنهادی مورد بررسی قرار گرفت. در این قسمت روش ارائه شده از لحاظ امنیت ارسال، کیفیت سیگنال بازیابی شده، انرژی مصرفی در طی انجام این مراحل در نودها، مورد بررسی قرار می‌گیرد.

در کانال مورد استفاده برای شبیه‌سازی، برای اعمال تلفات مسیر و اثر محوشدگی به ترتیب روابط (2) و (3) استفاده شده است[11]. $d_0$ فاصله‌ی مبنا که 100 متر در نظر گرفته شده است و d فاصله نود گیرنده و فرستنده از یکدیگر می‌باشد. ضمن این که SNR گیرنده با توجه به فاصله‌ی کم بین نودها و توان پایین آنتن‌ها، در حدوده 6/3dB فرض شده است.

$$L(db) = -85.65 + 95.4\log_{10} d(m) \qquad (2)$$

$$K(db) = 10 - 39\log_{10}(\frac{d}{d_0}) \qquad (3)$$

### 9.1. امنیت در ارسال

در روش‌هایی که تا به حال در این زمینه ارائه شده، یا اطلاعات محرمانه به طور مستقیم و بدون رمزنگاری در جاسازی می‌شوند[10]، و یا این که با استفاده از رمزنگاری مشخص صورت می‌پذیرند[13]. مسئله‌ی مهم در این شبکه‌ها آن است که بایستی با کمترین هزینه‌ی محاسباتی با دقت مناسبی بتوان اطلاعات محرمانه را رمزنگاری نمود. در صورتی که اطلاعات محرمانه رمزنگاری نشوند، در صورت آنالیز دقیق دشمن و دسترسی به الگوریتم جاسازی، ممکن است اطلاعات محرمانه فاش شوند. در روش پیشنهادی، با توجه به کلیدهای امنیتی که در [10] مورد استفاده قرار گرفته، و در کل شبکه به اشتراک گذاشته می‌شوند، نوع فشرده‌سازی انجام شده که همراه با رمزنگاری نیز می‌باشد، تشخیص سیگنال محرمانه بسیار سخت می‌کند. فرض کنید دشمن با آنالیز سنگین شبکه بتواند به انجام نهان‌نگاری داخل سیگنال‌های ارسالی پی‌ببرد، حال بایستی به کلیدهای امنیتی که بین نودهای خودی به اشتراک گذاشته شده‌اند دسترسی پیدا کند تا بتواند به نحوه‌ی جاسازی اطلاعات دسترسی پیدا کند. فرض کنید به این کلیدهای امنیتی و الگوریتم جاسازی نیز دسترسی پیدا کرد، با استخراج بیت‌های جاسازی شده با رشته بیت نامفهومی برخورد خواهد کرد که جز گیرنده‌ی مرکزی توانایی بازیابی آن را نخواهد داشت. در نتیجه می‌توان گفت این روش از لحاظ امنیتی کیفیت قابل قبولی را ایجاد می‌کند.

یکی از معیارهای مهم بررسی امنیت در مسائل نهان‌نگاری به منظور پنهان‌سازی سیگنال‌های محرمانه این است که سیگنال نهان‌نگاری شده دارای کیفیت مناسبی باشد و تشخیص آن از سیگنال حامل به راحتی امکان پذیر نباشد. در جدول 2 کیفیت سیگنال نهان‌نگاری شده نسبت به سیگنال محرمانه اولیه (قبل از فشرده‌سازی) بر اساس معیار SNR مقایسه شده است. لازم به ذکر است درصدهای بیان شده در جدول که اشاره به میزان جاسازی در سیگنال محرمانه دارد، با در نظر گرفتن 31% فشرده‌سازی بیان شده است. به عنوان مثال اگر هدف جاسازی حجم معادل % 25 سیگنال حامل، از سیگنال محرمانه باشد با 31% فشرده‌سازی سیگنال محرمانه، 25% سیگنال حامل معادل 36% سیگنال محرمانه می‌باشد. هر نمونه از سیگنال حامل 16 بیتی در نظر گرفته شده است و سیگنال‌ها دارای نرخ نمونه برداری 8 kb/s می‌باشند.

***جدول 2. مقایسه سیگنال نهان‌نگاری شده با سیگنال حامل بر حسب معیار SNR***

| SNRسیگنال‌نهان‌نگاری شده(dB) | درصد جاسازی درسیگنال حامل(dB) |
|---|---|
| 94/7 | 8 % |
| 81/3 | 14 % |
| 68/9 | 22 % |
| 54/6 | 29 % |
| 42/5 | 36 % |
| 38/3 | 43 % |

با توجه به جدول مشاهده می‌شود که با شرایط ذکر شده تا 36% جاسازی، سیگنال نهان‌نگاری شده دارای کیفیت مطلوبی می‌باشد و به این ترتیب این روش توانسته با نرخ جاسازی مناسب، کیفیت قابل قبولی را ایجاد نماید.

### 9.2. کیفیت سیگنال بازیابی شده

در بخش‌های قبلی کیفیت سیگنال محرمانه‌ی بازیابی شده در طی اجرای مراحل این روش جاسازی، مورد بررسی قرار گرفت. اما در شبکه‌های سنسور بی‌سیم سیگنال بایستی از محیطی که شبکه در آن قرار دارد، عبور کرده و دچار تغییراتی ناشی از تلفات کانال مورد استفاده می‌شود. در [11]، مدلی برای این محیط ارائه شده و میزان تلفات آن بررسی شده است. با توجه به [11]، بایستی حتی‌الامکان سیگنال نهان‌نگاری شده با کیفیت بالاتری در فرستنده تولید شود تا سیگنال محرمانه در گیرنده قابل تشخیص باشد. منظور از قابل تشخیص بودن این است که حداقل بتوان اطلاعات اصلی سیگنال صحبت محرمانه را تشخیص داد. در بازیابی سیگنال محرمانه ممکن است سیگنال نهان‌نگاری شده و در نتیجه سیگنال محرمانه، تحت تأثیر شرایط کانال کیفیت مطلوبی نداشته باشد. اما چون در گیرنده مهم اطلاعات سیگنال است نه کیفیت سیگنال در نتیجه چنانچه سیگنال بازیابی شده کیفیت مطلوبی نداشته باشد ولی بتوان اطلاعات آن را تشخیص داد، با توجه به محدودیت‌های زیادی که در این شبکه‌ها وجود دارد، چنین کیفیت نامطلوبی نیز قابل قبول است. با توجه به مدل کانال[11]، نتایج مثال قسمت قبل (9.2) از کانالی با مشخصات ارائه شده در ابتدای این بخش عبور داده و نتایج حاصل از مقایسه‌ی آن با سیگنال محرمانه‌ی اولیه (قبل از فشرده‌سازی) بر حسب معیار SNR در جدول 3، بیان شده است.

**جدول 3. کیفیت سیگنال بازیابی شده با در نظر گرفتن کانال و بدون در نظر گرفتن کانال**

| SNRمحرمانه‌ی بازیابی شده با در نظر گرفتن کانال (dB) | SNRمحرمانه‌ی بازیابی شده بدون در نظر گرفتن کانال(dB) | درصد جاسازی در سیگنال حامل |
|---|---|---|
| 65/78 | 151/81 | 8 % |
| 51/63 | 139/78 | 14 % |
| 42/27 | 112/54 | 22 % |
| 35/93 | 108/35 | 29 % |
| 26/58 | 102/83 | 36 % |

همان طور که مشخص است کیفیت سیگنال بازیابی شده با شبیه‌سازی کانال ارتباطی به شدت افت کرده است. اما آزمایشات شنوایی نشان داده با SNR در حدود $26_{dB}$ نیز اطلاعات اصلی سیگنال قابل تشخیص می‌باشد. بنابراین اگرچه کیفیت سیگنال بازیابی شده در حد مطلوبی نیست اما می‌توان گفت روش ارائه شده، با در نظر گرفتن جمیع شرایط، توانسته با این نرخ جاسازی، کارایی مناسبی داشته باشد.

### 9.3. مصرف انرژی

در شبکه‌های سنسور بی‌سیم یکی از محدودیت‌های اساسی محدودیت در انرژی است. انرژی مصرفی در شبکه‌های سنسور بی‌سیم برای دریافت هر بیت در هر نود در حدود 5μj و برای ارسال هر بیت در حدود 1μj می‌باشد. از طرفی هزینه‌ی انرژی مصرفی برای انجام پردازش هر بیت در نود فرستنده در حدوده 3000 برابر کمتر از ارسال آن بیت می‌باشد[1و6و10]. در نتیجه چنانچه بتوان با انجام مقداری پردازش اضافه، حجم اطلاعات ارسالی را کاهش داد، می‌توان هزینه‌ی محاسبات را صرفه‌جویی نمود. در روش پیشنهادی با توجه به فشرده‌سازی صورت گرفته در نود فرستنده، حجم بیشتری از اطلاعات محرمانه را می‌توان در سیگنال حامل جاسازی نمود. بنابراین حجم مشخصی از اطلاعات محرمانه را می‌توان در مراحل ارسال

کمتری، نسبت به روش‌های دیگر [10]، ارسال نمود. اگر فرض شود نودی بخواهد 100Kbitاطلاعات محرمانه را ارسال کند و در هر بار ارسال نیز 100Kbit اطلاعات ارسال می‌کند، تفاوت تعداد مراحل ارسال در دو روش ارائه شده در این مقاله و [10] مشخص می‌شود. با توجه به یکسان بودن الگوریتم جاسازی در هر دو روش، فرض می‌شود تا 25% از حجم اطلاعات حامل می‌توان اطلاعات محرمانه در آن جاسازی نمود. در این صورت بایستی 4 مرحله ارسال برای ارسال این حجم از اطلاعات محرمانه صورت بپذیرد. اما با توجه به 31% فشرده‌سازی انجام شده، 25% حجم اطلاعات حامل در حدوده 36% اطلاعات محرمانه می‌باشد. در واقع با روش پیشنهادی می‌توان این حجم از اطلاعات محرمانه را در 3 مرحله ارسال نمود. در این صورت به جای 4 مرحله ارسال، 3 مرحله ارسال انجام می‌شود.

حال فرض کنید قبل از هر مرحله ارسال، با توجه به مراحل محاسباتی، به طور متوسط در حدوده 1000 بار پردازش بر روی هر بیت انجام می‌شود(این مقدار تقریبی از کلیه‌ی محاسبات انجام شده بر روی رشته بیت‌های سیگنال‌های محرمانه و حامل، در کلیه‌ی مراحل می‌باشد). تعداد بیت‌های مورد پردازش قرار گرفته در هر مرحله 135kbit می‌باشد(100kbit حجم سیگنال حامل و حدود 35kbit حجم سیگنال محرمانه می‌باشد). در نتیجه انرژی صرفه‌جویی شده به دلیل کاهش 1 مرحله ارسال برابر است با 0/1 ژول و کل انرژی مصرفی ناشی از محاسبات اضافی انجام شده در حدوده 0/045 ژول می‌باشد. بنابراین با این فرض 0/055 ژول انرژی در هر چرخه‌ی کاری در هر نود ذخیره می‌شود که با توجه به کل انرژی مصرفی در حالت عادی که برابر 0/4 ژول می‌باشد، در حدوده % 14 صرفه‌جویی انرژی صورت گرفته است.

## 10. نتیجه‌گیری

برای داشتن یک نهان‌نگاری مناسب و مقاوم در برابر حملات دشمن از قبیل استراق سمع، مهمترین مسئله ارائه‌ی راه‌حلی منطبق با خواص شبکه‌های سنسور بی‌سیم می‌باشد. در روش ارائه شده در این مقاله، سعی بر این بوده که ضمن بالا بردن امنیت شبکه و مقابله با این گونه حملات رایج در این شبکه‌ها، طول عمر شبکه افزایش نیز پیدا کند. با بهره‌گیری از روش فشرده‌سازی ارائه شده، حجم اطلاعات محرمانه‌ی ارسالی کاهش می‌یابد در نتیجه نودها حجم ثابتی از اطلاعات محرمانه را در مراحل کمتری، نسبت به دیگر روش‌های موجود، ارسال می‌نمایند و بنابراین هزینه‌های ارسال کاهش می‌یابد. با کاهش هزینه‌های ارسال انرژی مصرفی نودها کاهش می‌یابد و در نتیجه طول عمر شبکه نیز افزایش پیدا می‌کند. این روش بر روی شبکه‌های سنسوری که به صورت بدون تأخیر ارسال انجام می‌دهند، نیز قابل پیاده‌سازی می‌باشد.

## 11. مراجع


[1] S. Misra and I. Woungang and Ch. S.Misraand Guide *to Wireless Sensor Networks.* Springer-Verlag London Limited 2009.

[2] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication.* Cambridge University Press 2005.

[3] H. C. Yin, F. Lin Qiu, and R. Ding. "A Survey of Digital Watermarking," *Journal of Computer Research and Development*, vol.42, no. 7, pp. 1093-1099, 2005.

[4] R. Agrawal and J. Kiernan "Watermarking relational databases," *in Proceeding of the 28th VLDB Conference*. Hong Kong, China: VLDB Press, 2002, pp. 155–166.

[5] R. Sion, M. Atallah, and S. Prabhakar, "Rights protection for relational data," *in Proceedings of ACM SIGMOD. San Diego, CA*, USA: ACM Press, 2003, pp. 98–109.

International Conference on , Taichung, pp. 507-512, 11-13 June 2008.

[14] L. Rabiner and B.H. Juang, Fundamentals of Speech recognition, Prentice Hall, 1993.

[6] X. Dong and X. Li "An Authentication Method for Self Nodes Based on Watermarking in Wireless Sensor Networks." Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference 24-26 Sept. 2009and pp: 1- 4.

[7] J. Feng and M. Potkonjak "Real-time watermarking techniques for sensor networks," *in SPIE Security and Watermarking of Multimedia Contents. Santa Clara*, CA, USA: SPIE Press, 2003, pp. 391–402.

[8] R. Sion and M. Atallah and S. Prabhakar "Resilient rights protection for sensor streams," *in Proceeding of the 30th VLDB Conference*. Toronto: VLDB Press, 2004, pp. 732–743.

[9] H. Guo and Y.Li and S.Jajodia "Chaining watermarks for detecting malicious modifications to streaming data," Information *Sciences*, no. 177, pp. 281–298, 2007.

[10] X. Xiao and X. Sun and L.Yang "Secure data transmission of wireless sensor network based on information hiding," *in Proceedings of The Fourth Annual International Conference on Mobile and Ubiquitous Systems*: Computing, Networking and Services. Philadelphia, PA, USA: IEEE Press, 2007, pp. 1–6.

[11] C. Oestages, *Propagation Modeling for Wireless Sensor Networks*. Universite catholique delouvain, UCL, pp. 68-70.

[12] N. Cvejic, T. Seppanen, "Water marking Bit Rate in Diverse Signal Domains," Inter national Journal of Signal Processing, Volume 1 No.1 (2004).

[13] Sh.H. Chen and SH.Y. Yu, "Speech Watermarking Based on Wavelet Transform and BCH Coding" Sensor Networks, Ubiquitous and Trustworthy Computing, IEEE International Conference on , Taichung, Sensor Networks, Ubiquitous and Trustworthy Computing, IEEE

[1] Wireless Sensor Networks(WSNs)
[2] Eavesdrop
[3] Storage
[4] Watermarking
[5] Send-Data
[6] wavelet
[7] Raician Channel
[8] DSPIC30f4011, DSPIC30f4013
[9] Clustering
[10] Cluster Head
[11] Sink
[12] Base Station
[13] Head
[14] Send-Data
[15] Public keys
[16] Samples
[17] Lost Significant Bits(LSB)