ارائه الگوریتم‌هایی برای حذف و اضافه شدن امن نود در شبکه‌های حسگر بی‌سیم

معصومه لشگری[۱] *، محمدعلی منتظری[۲]، مجید مقدادی[۳]، مهدی افضلی[۴]
s_lsh2002@yahoo.co.uk, montazeri@cc.iut.ac.ir, meghdadi@znu.ac.ir, afzali@hacettepe.edu.tr

چکیده

شبکه‌های حسگر بی‌سیم متشکل از نودهایی هستند که اغلب در محیط‌های باز، پرخطر و بدون محافظ قرار دارند، همچنین داده‌های درون شبکه از طریق امواج رادیویی منتقل می‌شوند، لذا این شبکه‌ها در معرض انواع آسیب‌های غیرعمدی و یا حملات عمدی قرار دارند. اغلب حملات از طریق اضافه شدن یک یا چند نود به شبکه و یا به تسخیر درآوردن سخت افزاری یا نرم‌افزاری نودهای درون شبکه و یا از بین بردن نودهای شبکه شروع می‌شوند. لذا درصورتی که مدیریت صحیحی بر اضافه و جدا شدن نودهای شبکه اعمال شود، از نقطه شروع حملات که همان نودهای مخرب می‌باشند، با حملات مقابله می‌شود. در این مقاله الگوریتم‌هایی برای اضافه و حذف شدن امن نود و همچنین انتقال پیام در شبکه حسگر بی‌سیم خوشه‌بندی شده پیشنهاد شده‌اند، این الگوریتم‌ها به خوبی با انواع حملات مرتبط با پروتکل‌های مسیریابی مقابله کرده و نیازمندی‌های امنیتی شبکه را برآورده می‌سازند.

کلمات کلیدی: شبکه حسگر بی سیم، اضافه شدن نود، حذف نود، امنیت، حملات.

1- مقدمه

شبکه‌های حسگر بی‌سیم متشکل از یک یا چند ایستگاه پایه و تعداد زیادی نودهای حسگر کم‌هزینه و کوچک می‌باشند. نودهای شبکه دارای محدودیت‌هایی در توان مصرفی، ظرفیت حافظه و قدرت پردازش می‌باشند. ایستگاه پایه نودی با میزان انرژی بالا و تجهیزات مورد نیاز می‌باشد که واسط بین شبکه حسگر و کاربر نهایی می‌باشد[1]. در اغلب شبکه‌های حسگر بی‌سیم به دلایلی مانند بزرگ بودن شبکه، محدودیت توان ارسالی نودها و وجود موانعی مانند ساختمان‌های بلند یا کوه‌ها این امکان وجود ندارد که همه نودها بطور مستقیم و با یک گام با ایستگاه پایه و یا سایر نودها ارتباط برقرار نمایند، در نتیجه نیازمند مسیرهای چندگامه تا ایستگاه پایه می‌باشند[2]. نحوه ارتباط این نودها و مسیریابی داده‌ها برای رسیدن به ایستگاه پایه بسیار مهم و اساسی است، چرا که بر عواملی مانند مصرف انرژی، تاخیر در انتقال اطلاعات، حجم داده ارسالی و تحمل پذیری خطای شبکه موثر است[3-4]. پروتکل‌های مسیریابی روش‌هایی برای انتخاب مسیر انتقال داده‌ها از نودهای مبدا به نودهای مقصد بیان می‌کنند. بسیاری از پروتکل‌های مسیریابی بر اساس یک شاخص مانند کمترین تعداد گام، کمترین انرژی مصرف شده، کمترین فاصله و ... مسیر بهینه را انتخاب می‌کنند [5].

شبکه‌های حسگر بی‌سیم در معرض انواع آسیب‌های غیرعمدی و یا حملات عمدی قرار دارند[6-7]. اغلب حملات از طریق

---

[۱] دانشجوی کارشناسی ارشد، دانشگاه آزاد اسلامی، واحد زنجان، گروه کامپیوتر، زنجان، ایران
[2] استادیار دانشگاه صنعتی اصفهان
[۳] استادیار دانشگاه سراسری زنجان
[۴] استادیار، دانشگاه آزاد اسلامی، واحد زنجان، گروه کامپیوتر، زنجان، ایران

اضافه شدن یک یا چند نود به شبکه و یا به تسخیر درآوردن سخت افزاری یا نرم افزاری نودهای شبکه و یا از بین بردن نودهای شبکه شروع می‌شوند. لذا نیاز به وجود سطحی از امنیت در شبکه‌های حسگر بی‌سیم دیده می‌شود[8]. بدلیل محدودیت‌های شبکه حسگر بی‌سیم، روش‌های امنیتی موجود در شبکه‌های اقتضایی را نمی‌توان در این شبکه‌ها به کار برد. در اغلب پروتکل‌های مسیریابی به امنیت توجه خاصی نشده است[9].

در این مقاله الگوریتم‌هایی برای اضافه وحذف شدن امن نود و همچنین انتقال پیام در شبکه حسگر بی‌سیم خوشه بندی شده سلسله مراتبی پیشنهاد شده اند. نشان داده می‌شود که الگوریتم‌های ارائه شده به خوبی با انواع حملات مرتبط با پروتکل‌های مسیریابی مقابله کرده و مانع از بروز و گسترش آن حملات می‌شوند و همچنین نیازمندی‌های امنیتی شبکه را نیز برآورده می‌کنند. دیگر ویژگی‌های این الگوریتم‌ها عبارتند از: سربار محاسباتی ناچیز، درنظر گرفتن مسیرهای جایگزین برای انتقال داده‌ها، افزایش قابلیت اطمینان شبکه، افزایش سرعت انتقال داده‌ها، کاهش انرژی مصرفی نودها، قابلیت پیاده سازی در شبکه‌های بزرگ و چند گامه.

در ادامه، در بخش دوم پروتکل مسیریابی خوشه بندی سلسله مراتبی معرفی می‌گردد، در بخش سوم الگوریتم‌های حذف و اضافه شدن امن نود درشبکه‌های حسگر بی‌سیم ارائه و تشریح می‌گردند، در بخش چهارم نحوه ارزیابی الگوریتم‌های ارائه شده و در بخش پنجم نتیجه‌گیری مطالب بیان خواهند شد.

2- پروتکل‌های مسیریابی خوشه بندی سلسله مراتبی

در ساختار سلسله مراتبی، نودها در سطوح مختلفی نسبت به ایستگاه پایه قرار گرفته‌اند. ایستگاه پایه در سطح صفر، نودهایی که به فاصله یک قدمی ایستگاه پایه قرار دارند در سطح یک، نودهایی که در فاصله دو قدمی ازایستگاه پایه قرار دارند در سطح دو و این سطح بندی تا زمانی که تمامی نودها شبکه تحت پوشش قرار گیرند ادامه دارد[10]. خوشه‌بندی شبکه به معنی تفکیک شبکه به خوشه‌های مختلف می‌باشد. هر خوشه دارای سرخوشه‌ای می‌باشد که وظیفه تبادل پیام بین ایستگاه پایه و نودها را برعهده دارد. در شبکه‌های با این ساختار کمترین حملات قابل اعمال است و اگر نودی تسخیر شد اثر تسخیر آن محلی می‌شود، همچنین با کمک گرفتن از مفهوم ساختار سلسله مراتبی می‌توان چندین سطح از امنیت را در کل شبکه به وجود آورد[11].

3- ارائه الگوریتم‌های حذف و اضافه شدن امن نود به شبکه

در این بخش الگوریتم‌های پیشنهادی برای حذف و اضافه شدن امن نود در شبکه‌های بی‌سیم تک گامه و چند گامه شرح داده می‌شوند.

۳-۱- توزیع کلید

برای هر نود دو نوع کلید تعریف می‌شود، کلیدهای اصلی نود که برای ارتباط با ایستگاه پایه و سرخوشه مورد استفاده قرار می‌گیرند و کلیدهای کمکی که برای ارتباط با سایر نودها مورد استفاده قرار می‌گیرند. قبل از ورود نود به شبکه لازم است *ID* نود، کلیدهای اصلی و بازه زمانی که نود می‌تواند به شبکه ملحق شود در حافظه آن نود ذخیره و همچنین از طریق یک لینک امن به ایستگاه پایه ارسال شوند. ایستگاه پایه با دریافت اطلاعات فوق جدولی مشابه جدول 1 را برای آن نود تهیه می‌کند.

جدول 1: جدول داده‌های رمز نود A

ID=0125			محدوده زمانی ملحق شدن به شبکه =31 JAN 8-16				
ردیف	نودهای مرتبط	فرستنده/ گیرنده	حداقل پیام ارسالی در واحد زمان	حداکثر پیام ارسالی در واحد زمان	حداقل پیام دریافتی در واحد زمان	حداکثر پیام دریافتی در واحد زمان	کلید مشترک
1	CH_i	TR	0	2	0	3	K_{A_CHi}
2	B	T	1	5	0	0	K_{A_B}
3	C	R	0	0	0	0	K_{A_C}
4	D	TR	2	5	0	3	K_{A_D}
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

۳-۲- نمادگذاری

برای ساده سازی در بیان الگوریتم‌ها، نمادهایی بصورت زیر تعریف می‌کنیم.

$$A \rightarrow B : A,B,\{Data\}_{K_{A\_B}} \quad (1)$$

مفهوم این عبارت این است که نود A می‌خواهد پیام $Data$ را برای نود B ارسال نماید. در این پیام فرستنده، گیرنده و رمز مشترک بین نودهای A و B وجود دارد. K_{A_B} رمز مشترک بین نودهای A و B می‌باشد. $\{Data\}_{K_{A\_B}}$ یعنی اینکه داده توسط کلید K_{A_B} رمز شده است.

$$A \underrightarrow{B} C : A,C,\{\{Data\}_{K_{A\_B}},B\}_{K_{A\_C}} \quad (2)$$

مفهوم این عبارت این است که نود A می‌خواهد از طریق نود C، پیامی را برای نود B ارسال نماید. در این پیام فرستنده، گیرنده و نود واسط مشخص شده است.

$$C \underrightarrow{M\{A\}} B : C,B,\{A,\{Data\}_{K_{A\_B}}\}_{K_{C\_B}} \quad (3)$$

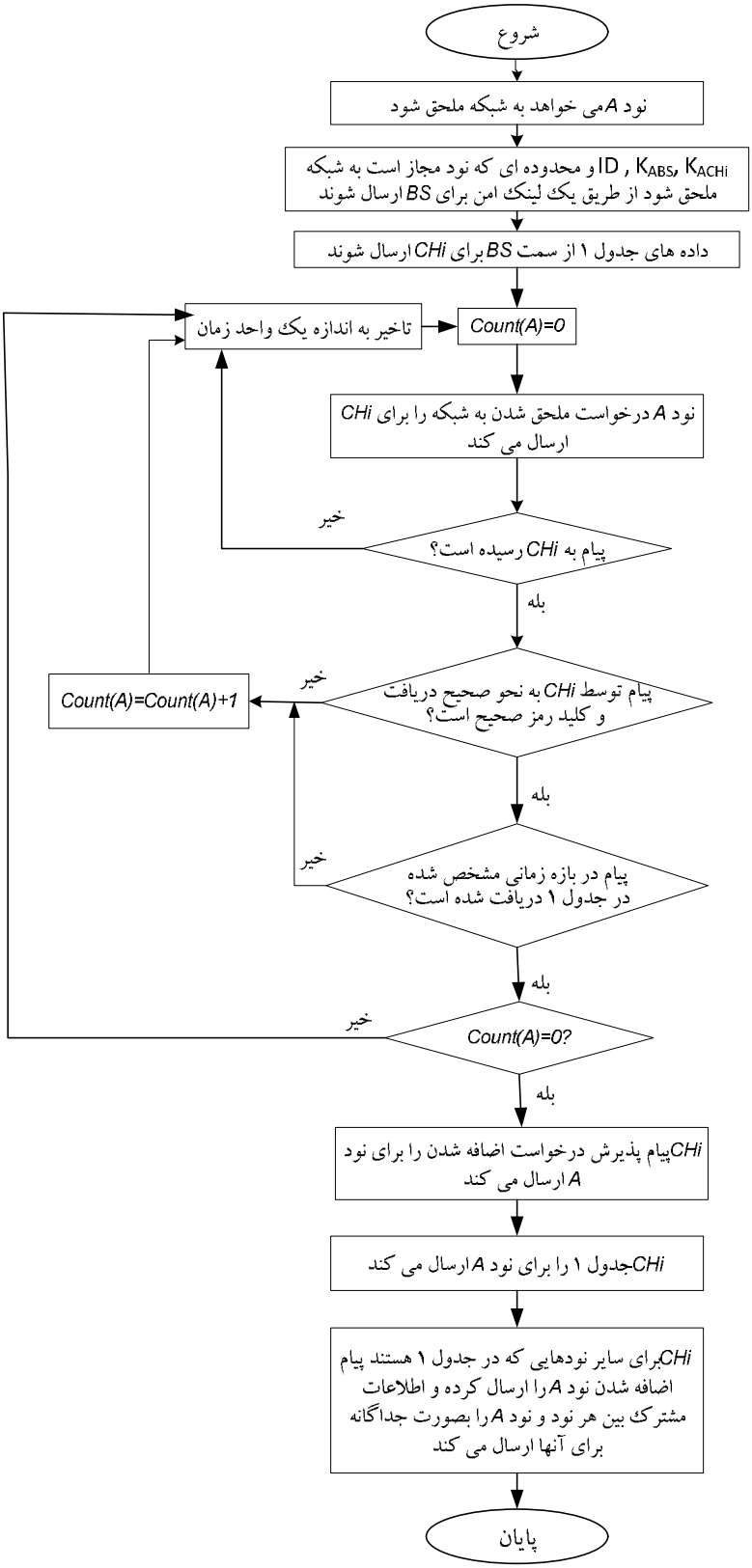
مفهوم این عبارت این است که نود C می‌خواهد پیام نود A را به نود B ارسال نماید..

$$C \underrightarrow{M\{A,B\}} D : C,D,\{A,\{Data\}_{K_{A\_B}},B\}_{K_{C\_D}} \quad (4)$$

مفهوم این عبارت این است که نود C می‌خواهد پیامی که فرستنده آن نود A و گیرنده آن نود B می‌باشد را از طریق نود D ارسال نماید.

۳-۳- الگوریتم پیشنهادی برای اضافه شدن نود در شبکه تک گامه

در شکل 1 الگوریتم اضافه شدن یک نود مانند A به شبکه تک گامه نشان داده شده است. قبل از اینکه نود بتواند درخواست ملحق شدن به شبکه را ارسال نماید لازم است ID نود،کلید اصلی نود و کلید مشترک با سرخوشه و بازه زمانی که نود مجاز است به شبکه ملحق شود از طریق یک لینک امن برای ایستگاه پایه ارسال شود. ایستگاه پایه با دریافت اطلاعات فوق جدولی مشابه جدول 1 را برای آن نود تهیه و برای سرخوشه مربوطه (CH_i) ارسال می‌کند. سپس نود A می‌تواند درخواست ملحق شدن به شبکه (JR) را برای سرخوشه ارسال کند.



شکل1: الگوریتم اضافه شدن نود در شبکه تک گامه

$$A \rightarrow CH_i \ : \ A, CH_i \ , \{JR\}_{K_{A\_CH_i}} \quad (5)$$

پس از اینکه نود A درخواست ملحق شدن به شبکه را ارسال کرد، درصورتی‌که پاسخی از سمت CH_i دریافت نکند، نود A حداقل به اندازه یک واحد زمان صبر کرده و درخواست خود را مجدداً ارسال می‌کند. درصورتی که پیام دریافتی توسط CH_i صحیح نباشد، CH_i به شمارنده‌ای که نشان دهنده تعداد پیام دریافتی از نود A در یک واحد زمان می‌باشد یکی اضافه می‌کند، این شمارنده در ابتدای هر واحد زمان مجدداً صفر می‌شود. اگر CH_i پیام را به نحو صحیح دریافت کند و کلید رمز نیز صحیح باشد، بررسی می‌کند که آیا پیام در بازه زمانی مشخص شده در جدول 1 دریافت شده است یا خیر؟ اگر پیام در بازه زمانی مشخص شده دریافت نشده باشد، شمارنده مربوط به تعداد پیام دریافتی از نود A را یکی اضافه می‌کند. اگر پیام در بازه زمانی مجاز دریافت شده باشد به منزله قبول درخواست ملحق شدن نود A به شبکه می‌باشد، در این هنگام CH_i پاسخ قبول اضافه شدن (JA) و اطلاعات جدول 1 را برای نود A ارسال می‌کند.

$$CH_i \rightarrow A: \ CH_i \ , A \ , \{JA\}_{K_{A\_CH_i}} \quad (6)$$

$$CH_i \rightarrow A: \ CH_i \ , A \ , \{Table1\}_{K_{A\_CH_i}} \quad (7)$$

CH_i برای نودهای مرتبط که در جدول 1 مشخص شده‌اند نیز پیام اضافه شدن نود A را ارسال می‌کند، همچنین اطلاعات مشترک بین هر نود و نود A را نیز از این جدول استخراج و برای نود مربوطه ارسال می‌کند. در این هنگام نود A به شبکه ملحق شده است و می‌تواند براساس ضوابط مشخص شده در جدول 1 با سرخوشه و نودهای مرتبط ارتباط داشته باشد.

۳-۴- الگوریتم حذف شدن نود در شبکه تک گامه

در شکل 2 الگوریتم حذف شدن نود در شبکه تک گامه نشان داده شده است. در حذف شدن یک نود از شبکه دو حالت وجود دارد، یا نود به صورت اختیاری و برای انجام برخی تعمیرات و یا تعویض قطعات و... می‌خواهد از شبکه خارج شود و یا اینکه به صورت غیرعادی و در اثر خراب شدن یکی از اجزاء اصلی، تمام شدن ناگهانی باطری و یا تسخیر توسط دشمن از شبکه خارج می‌شود.

در صورتی‌که نود بخواهد به صورت اختیاری از شبکه خارج شود لازم است محدوده زمانی که این نود مجاز است درخواست جدا شدن از شبکه(RR) را ارسال نماید از طریق یک لینک امن به ایستگاه پایه اطلاع داده شود. سپس ایستگاه پایه به سرخوشه مربوطه(CH_i) اطلاع می‌دهد. در اینصورت پس از اینکه نود A درخواست جدا شدن از شبکه را برای CH_i ارسال کند، اگر پیام در بازه زمانی مشخص شده ارسال شده باشد، CH_i به نود A پیام می‌فرستد که می‌تواند از شبکه جدا شود، در این هنگام به سایر نودهایی که با نود A در ارتباط هستند نیز پیام می‌دهد که نودA از شبکه خارج شده است و فرمان می‌دهد که کلیه کلیدهای مشترک بین آن نودها و نود A را حذف نمایند.

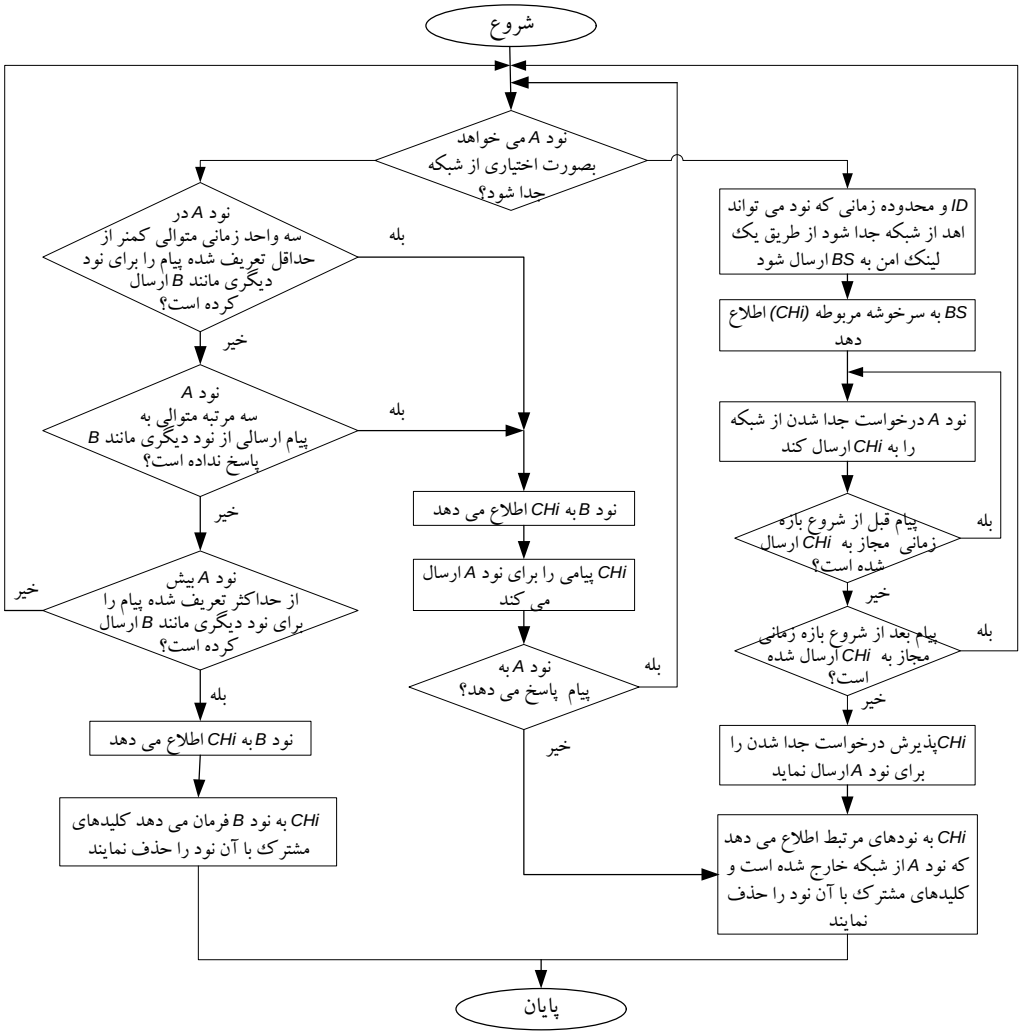
درصورتی که نود به دلایلی مانند خراب شدن ناگهانی یکی از اجزاء اصلی، تمام شدن ناگهانی باطری و یا تسخیر توسط دشمن از شبکه خارج شود و یا وظایف خود را در چارچوب تعریف شده انجام ندهد، لازم است که CH_i از این موضوع اطلاع حاصل کند و این مطلب را به ایستگاه پایه و سایر نودهای مرتبط اطلاع دهد. برای این منظور CH_i به روش‌های زیر از بروز اختلال در عملکرد نود A آگاهی می‌یابد.

الف) اگر نود A در سه بازه زمانی متوالی کمتر از حداقل تعریف شده در جدول1 برای نود دیگری مانند B پیام ارسال نماید، در این هنگام نود B به CH_i اطلاع می‌دهد، سپس CH_i مستقیماً پیامی را برای نود A ارسال می‌کند و اگر پاسخی دریافت

نکرد، به سایر نودهای مرتبط با نود A اطلاع می‌دهد که نود A از شبکه خارج شده است و فرمان می‌دهد که کلیه کلیدهای مربوط به آن نود را حذف کنند.

ب) در صورتی‌که نود A سه بار متوالی به پیام ارسالی از نود دیگری مانند B پاسخی ندهد، نود B این مطلب را به CH_i منتقل می‌نماید، CH_i مستقیماً پیامی را برای نود A ارسال می‌کند و اگر پاسخی دریافت نکرد به سایر نودهای مرتبط با نود A اطلاع می‌دهد که نود A از شبکه خارج شده است.

ج) اگر نود A بیش از حداکثر تعداد مجاز، برای نود دیگری مانند B پیام ارسال نماید، در اینصورت نود B این مطلب را به CH_i گزارش می‌دهد و CH_i به نود B فرمان می‌دهد که ارتباط خود با نود A را قطع نماید و کلیه کلیدهای مشترک بین آن نود و نود A را حذف نماید. چون ممکن است نود B به دلیل تسخیر توسط دشمن گزارش اشتباه را برای CH_i ارسال کرده باشد، لذا نباید این موضوع از طرف CH_i به سایر نودهای مرتبط با نود A اطلاع داده شود.



شکل2: الگوریتم جدا شدن نود از شبکه حسگر بی‌سیم

۳-۵- بسط الگوریتم‌های فوق در شبکه چندگامه

در شبکه تگ گامه لازم است در بدو ورود نود به شبکه، ID، دو کلید اصلی و همچنین بازه زمانی که نود مجاز است به شبکه ملحق شود مشخص و در حافظه نود ذخیره باشند. در شبکه چند گامه کلید دیگری(K_{A_all}) نیز لازم است که نود بتواند توسط آن درخواست ملحق شدن به شبکه را برای نودهای همسایه ارسال نماید. قبل از اینکه ورود نود لازم است ID نود، سه کلید ذکر شده و بازه زمانی که نود مجاز است به شبکه ملحق شود از طریق یک لینک امن برای ایستگاه پایه ارسال شوند. ایستگاه پایه نیز کلید K_{A_all} و داده‌های جدول 1 را تهیه و برای سرخوشه ارسال می‌کند. سرخوشه در ابتدای بازه زمانی که نود A مجاز است وارد شبکه شود به سایر نودهای درون شبکه، ID نود و کلید K_{A_all} را ارسال می‌کند و اطلاع می‌دهد که این نود می‌تواند درخواست ورود به شبکه را ارسال کند.

نودA در بدو ورود به شبکه درخواست ملحق شدن به شبکه را ارسال می‌کند.

$$A \rightarrow all \ : \ A, all \ , \{JR\}_{K_{A\_all}} \qquad (8)$$

هریک از نودهایی که مستقیماً پیام A را دریافت کنند از طریق مسیر خود، پیام نود A را به سرخوشه انتقال می‌دهند. اگر پیام در محدوده زمانی قابل قبول دریافت شده باشد، سرخوشه با بکارگیری هر یک از پروتکل‌های مسیریابی سلسله مراتبی، بهترین مسیرها را برای انتقال پیام از نود A به سرخوشه و یا سایر نودهای همکار انتخاب می‌کند، سرخوشه علاوه بر تعیین بهترین مسیر، سایر مسیرهای جایگزین را نیز انتخاب کرده و در حافظه ذخیره می‌کند و در صورتی که به هر دلیلی مسیر اصلی دچار مشکل شد از طریق مسیر جایگزین با اولویت بالاتر پیام‌های خود را ارسال و جدول مسیریابی جدید را برای آن نود ارسال می‌کند. علاوه بر این جدولی مشابه جدول 2 را برای آن نود تهیه می‌کند، جدول 2، تکمیل شده جدول 1 می‌باشد که ستونی با عنوان نود بلافصل به آن اضافه شده است. در حقیقت نود A با استفاده از این ستون متوجه می‌شود که پیام‌های ارسالی به هر یک از نودهای مرتبط را از طریق کدام یک از نودها ارسال نماید. سپس از طریق مسیر انتخاب شده و با استفاده از کلید رمز $K_{A\_CH_i}$ پیام پذیرش ملحق شدن به شبکه و جدول 2 را برای آن نود ارسال می‌کند. سرخوشه برای نودهایی که در جدول 2 مشخص شده اند نیز پیام اضافه شدن نود A را ارسال می‌کند، همچنین اطلاعات مشترک بین هر نود و نود A را نیز از جدول 2 استخراج و برای نودهای مربوطه ارسال می‌کند. در این هنگام نودA به شبکه ملحق شده و

جدول 2: جدول داده‌های رمز نود A در شبکه چند گامه

$ID=0125$			محدوده زمانی ملحق شدن به شبکه =31 JAN 8-16					
ردیف	نودهای مرتبط	فرستنده/گیرنده	حداقل پیام ارسالی در واحد زمان	حداکثر پیام ارسالی در واحد زمان	حداقل پیام دریافتی در واحد زمان	حداکثر پیام دریافتی در واحد زمان	کلید مشترک	نود بلافصل
1	CH_i	TR	0	2	0	3	K_{A_CHi}	C
2	B	T	1	5	0	0	K_{A_B}	D
3	C	R	0	0	0	0	K_{A_C}	C
4	D	TR	2	5	0	3	K_{A_D}	D
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

می‌تواند طبق ضوابط مشخص شده، به فعالیت‌های خود ادامه دهد.

جدا شدن یک نود در شبکه چندگامه، مشابه روش بیان شده در شبکه تک‌گامه می‌باشد، با این تفاوت که در شبکه تک گامه اگر نودی از شبکه جدا شود، مسیریابی شبکه دچار مشکل نمی‌شود ولی در شبکه چندگامه اگر نودی مانند A از شبکه جدا شود و آن نود در مسیر انتقال پیام بین سایر نودها باشد، مسیریابی دچار مشکل می‌شود، لذا سرخوشه از طریق مسیر جایگزین به سایر نودهای مرتبط اطلاع می‌دهد که نود A از شبکه خارج شده است و مسیر جایگزین را نیز برای آنها ارسال می‌کند.

برای حفظ اصالت و محرمانگی داده لازم است در ارسال هر پیام نود فرستنده، نود گیرنده و نود انتقال دهنده پیام مشخص باشند، همچنین نود انتقال دهنده پیام امکان دسترسی به محتویات پیام را نداشته باشد. فرض کنید نود A می‌خواهد پیامی را از طریق نودهای واسط C و D به نود B ارسال کند. در این صورت ارسال داده بصورت زیر خواهد بود.

$$A \underrightarrow{B} C \ : \ A, C, \{\{Data\}_{K_{A\_B}}, B\}_{K_{A\_C}} \quad (9)$$

$$C \underrightarrow{M\{A,B\}} D \ : \ C, D, \{A, \{Data\}_{K_{A\_B}}, B\}_{K_{C\_D}} \quad (10)$$

$$D \underrightarrow{M\{A\}} B \ : \ D, B, \{A, \{Data\}_{K_{A\_B}}\}_{K_{D\_B}} \quad (11)$$

4- ارزیابی الگوریتم‌های ارائه شده

برای ارزیابی الگوریتم‌های ارائه شده لازم است عواملی از جمله نحوه مقابله با حملات، برآورده سازی نیازمندی‌های امنیتی، سربار محاسباتی و حافظه اضافی مورد نیاز را درنظر گرفت.

۴-۱- مقابله با حملات

در این قسمت برخی از مهمترین حملات مربوط به پروتکل‌های مسیریابی و روش مقابله الگوریتم‌های پیشنهادی با آنها بیان می‌شوند.

الف- حمله تغییر یا جعل اطلاعات مسیریابی: در این حمله با انجام تقلید و فریب، تغییر و یا تکرار دوباره اطلاعات مسیریابی، مهاجمان ممکن است قادر باشند مسیرهای منبع را کوتاه و یا این مسیرها را طولانی نمایند و پیامهای خطای اشتباه را ایجاد نمایند. در الگوریتم‌های پیشنهادی، مسیریابی از طریق سرخوشه انجام می‌شود و با اضافه یا جدا شدن یک نود از شبکه، سرخوشه اطلاعات مسیریابی جدید را برای نودهای مرتبط ارسال می‌کند، بنابراین به نود مهاجم اجازه تغییر و یا جعل اطلاعات مسیریابی شبکه داده نمی‌شود.

ب- حمله ارسال انتخابی: در این حمله نودهای غیرمجاز ممکن است پیام‌های خاص را به نود بعدی ارسال نکنند و آنها را حذف کنند. در الگوریتم‌های پیشنهادی، با تعیین مقدار مناسب برای حداقل تعداد پیام ارسالی برای هر نود با این نوع حمله مقابله می‌شود. سرخوشه با توجه به اهمیت پیام‌های هر نود این مقدار حداقل را تعیین می‌کند. مهاجم در صورتی‌که برخی از پیام‌های ارسالی از نود A را به گیرنده ارسال نکند، گیرنده متوجه خواهد شد که تعداد پیام ارسالی کمتر از مقدار تعیین شده است و این مطلب را به سرخوشه اطلاع می‌دهد.

ج- حمله گودال: نود خرابکار با اطلاعات و مشخصات جعلی، نودهای همسایه و همجوار خود را گمراه ساخته تا اطلاعاتشان را به او بسپارند. به عنوان مثال اعلام می‌کند که فاصله‌اش تا ایستگاه پایه بسیار کم است، در این هنگام همسایگان او گمراه

شده وتصمیم می‌گیرند که او را به عنوان والد خود انتخاب کنند. در نتیجه بخشی از نودهای شبکه اطلاعاتشان را به این نود می‌فرستند و نود مهاجم می‌تواند هر گونه عمل خرابکارانه‌ای را انجام دهد. در الگوریتم‌های پیشنهادی، مسیر انتقال داده‌ها از طریق سرخوشه انجام می‌شود و با اضافه یا جدا شدن یک نود از شبکه، سرخوشه اطلاعات مسیریابی جدید را برای نودهای مرتبط ارسال می‌کند، بنابراین به نود مهاجم اجازه نمی‌دهد که خود را به عنوان والد معرفی نماید.

د- حمله سیلاب: یک مهاجم به طور مداوم به نودهای همسایه پیامی مبنی بر درخواست ارتباط با آنها ارسال می‌کند. این پیام معمولاً همراه با بسته *Hello* است. در این حالت نودهای همسایه با دریافت بسته*Hello* ، گمراه شده و پیامی را جهت تایید درخواست ارسال می‌کنند. آنقدر این عمل تکرار می‌شود تا نودهای همسایه انرژی خود را از دست داده و خاموش شوند. در الگوریتم‌های پیشنهادی مشخص شده است که هر نود با چه نودهایی می‌تواند ارتباط برقرار کند و حداکثر تعداد پیام دریافتی نیز مشخص شده است، بنابراین اگر نودی بخواهد بیش از حداکثر تعداد پیام مجاز ارسال کند، این مطلب به ایستگاه پایه اطلاع‌رسانی می‌شود.

ه- حمله سیبل: یک نود خرابکار، با جعل هویت، خودش را بجای تعداد زیادی نود جا می‌زند. پس از آن که هویت‌های مختلف زیادی را در شبکه تزریق کرد، اقدام به فریب نودهای قانونی می‌کند. به این صورت که به نودهای قانونی القاء می‌کند هویت‌هایش، مسیر ارتباطی با نودهای قانونی دیگر می‌باشد. از این رو همه بسته‌ها به این نود ارسال شده و نود خرابکار تصمیم می‌گیرد که چطور با این بسته‌ها برخورد کند. در الگوریتم پیشنهادی، اضافه شدن هر نود طبق قاعده مشخصی می‌باشد، لذا یک نود نمی‌تواند خودش را به جای تعداد زیادی نود جا بزند.

و- حمله لانه کرم: مهاجم دو نقطه از شبکه را با بستر ارتباطی نسبتاً سریعی به‌هم وصل می‌کند که به آن لانه کرم گفته می‌شود. زمانی که مسیر لانه کرم پیاده‌سازی شد، مهاجم بسته‌های ارسالی توسط نودها را از یک طرف از شبکه تسخیر می‌کند و از طریق مسیر لانه کرم آن را در طرف دیگر شبکه پخش می‌کند. در الگوریتم‌های پیشنهادی، مسیریابی از طریق سرخوشه انجام می‌شود و با حذف یا اضافه شدن یک نود از شبکه، سرخوشه اطلاعات مسیریابی جدید را برای نودهای مرتبط ارسال می‌کند، بنابراین اجازه ایجاد مسیر لانه کرم داده نمی‌شود.

۴-۲- برآورده سازی نیازمندی‌های امنیتی

در الگوریتم‌های ارائه شده در این مقاله هر پیام بصورت رمز شده ارسال می‌شود، لذا نیازمندی‌های امنیتی از قبیل احراز اصالت، حفظ صحت و محرمانگی داده، حفظ حریم خصوصی، امنیت ارتباطات برآورده می‌شوند. هر نود فقط می‌تواند با نودهای مشخصی ارتباط برقرار نماید لذا نیازمندی امنیتی کنترل دسترسی برآورده می‌شود. با انتخاب مناسب حداقل تعداد پیام ارسالی برای هر نود نیازمندی امنیتی دسترس پذیری برآورده می‌شود.

۴-۳- سربار محاسباتی

عمده ترین محاسباتی که اجرای این الگوریتم‌ها به یک شبکه حسگر بی‌سیم نا امن اضافه می‌کنند برای تولید کلید، مدیریت کلید، رمزگذاری و رمزگشایی پیام‌ها و بررسی شرایط حداقل و حداکثر پیام‌های ارسالی و دریافتی انجام می‌شود. تولید کلید در ایستگاه پایه که از توان محاسباتی بالایی برخوردار می‌باشد انجام می‌شود و از این نظر به سرخوشه و یا سایر نودها محاسبات اضافه‌ای تحمیل نمی‌شود. در این الگوریتم‌ها از روش مدیریتی تمرکز زدایی شده که از بهترین روشهای مدیریت کلید می‌باشد، استفاده شده است، از ایستگاه پایه به عنوان مرجعی قابل قبول در ابتدای راه اندازی شبکه و همچنین حذف و اضافه شدن نود استفاده می‌شود و از سرخوشه‌ها برای توزیع و مدیریت کلید استفاده می‌شوند. در هر شبکه حسگر که به

امنیت توجه شود رمزگذاری و رمزگشایی پیام‌ها امری ضروری است و سیستم‌عامل باید توانایی این کار را داشته باشد. بررسی شرایط حداقل و حداکثر پیام‌های ارسالی و دریافتی بار محاسباتی چندانی ندارد و فقط چند شرط ساده می‌باشد.

۴-۴- حافظه اضافی مورد نیاز

حافظه اضافی مورد نیاز در هر نود، برای نگهداری داده‌های موجود در جدول آن نود مورد استفاده قرار می‌گیرد. از آنجا که در این جدول کلیدهای مشترک با نودهای همکار وجود دارد، لذا نیازی به نگهداری کلید مشترک با سایر نودهای شبکه وجود ندارد و از حافظه هر نود بصورت بهینه استفاده شده است.

5- نتیجه گیری

در این مقاله الگوریتم‌هایی برای اضافه و حذف شدن امن نود و همچنین انتقال پیام در شبکه حسگر بی‌سیم خوشه‌بندی شده ارائه گردیدند. نشان داده شد که این الگوریتم‌ها به خوبی با حملات مختلف مقابله کرده و مانع از بروز و گسترش حملات می‌شوند و همچنین نیازمندی‌های امنیتی شبکه را نیز برآورده می‌کنند. دیگر ویژگی‌های این الگوریتم‌ها عبارتند از: سربار محاسباتی ناچیز، درنظر گرفتن مسیرهای جایگزین برای انتقال داده‌ها، افزایش قابلیت اطمینان شبکه، افزایش سرعت انتقال داده‌ها، قابلیت پیاده‌سازی در شبکه‌های بزرگ و چند گامه.

6- فهرست منابع

[1] *I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "A survey on sensor networks". IEEE Communications Magazine, 40(8):102–114, August 2002.*

[2] *K. Holger, and A.Willig, "A Short Survey of Wireless Sensor networks", TKN Technical Reports Series, Technical University Berlin, Berlin, pp. 1-19, Oct2003.*

[3] *I. F. Akyildiz, W. Su, E.Cayirci, "Wireless sensor networks: A survey", Computer Networks Journal, Elsevier Science, Vol. 38, No. 4, pp 393–422, March 2002.*

[4] *Holger Karl, Andreas Willig, "Protocols and Architectures for Wireless Sensor Networks", Copyright 2005 John Wiley & Sons, Ltd.*

[5] *Kemal Akkaya, Mohamed Younis "A survey on routing protocols for wireless sensor networks" Science Direct, Ad Hoc Networks 3 (2005) 325–349.*

[6] *Yanli Yua, b, Keqiu Lia, Wanlei Zhoub, Ping Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures" Journal of Network and Computer Applications, Volume 35, Issue 3, May 2012, Pages 867–880.*

[7] *C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad-Hoc Networks Journal, vol. 1, pp. 293–315, September 2003.*

[8] *John Paul Walters, Zhengqiang Liang, " Wireless Sensor Network Security: A Survey" Security in Distributed, Grid, and Pervasive Computing 2006 Auerbach Pub., CRC Press.*

[9] *Harmandeep Singh, Garima Malik "Approaches to Wireless Sensor Network: Security Protocols" WCSIT Journal ISSN: 2221-0741 Vol. 1, No. 7,302-306, 2011.*

[10] *Parul Tyagi, Surbhi Jain, "Comparative Study of Routing Protocols in Wireless Sensor Network", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012.*

[11] *S. Patel and A. K. Singh. "A Survey On Cluster Based Routing Protocol Organization For Wireless Sensor Network", Golden Research Thoughts, Volume 2, Issue. 4, Oct 2012.*