هفتمین کنفرانس بین المللی انجمن رمز ایران

۲۴ و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی

انجمن رمزایران

دانشگاه صنعتی خواجه نصیرالدین طوسی

ارائه یک الگوریتم کشف Wormhole کارا و مبتنی بر آنتن‌های جهت‌دار در شبکه‌های حسگر بی سیم

فرزاد تشتریان[۱]، عباس قائمی بافقی[۲]، محمد حسین یغمائی مقدم[۳]

مشهد، دانشگاه فردوسی، گروه مهندسی کامپیوتر[۱،۲،۳]

[2,3], tashtarian@mshdiau.ac.ir[1] ghaemib}@ferdowsi.um.ac.ir{Hyaghmae,

چکیده

امروزه با توجه به کاربردهای گسترده شبکه‌های حسگر بی‌سیم، نیازمندی‌های امنیتی این شبکه‌ها روزبه‌روز در حال افزایش است. حملات بسیاری نسبت به این شبکه‌ها طراحی شده است که یکی از مهمترین و خطرناک‌ترین آنها حمله Wormhole می‌باشد که درآن یک حسگر دشمن ترافیک شبکه را از یک منطقه شبکه به همدست خود در منطقه‌ای دیگر ارسال می‌کند، که این خود باعث مشکلات فراوانی می‌گردد. ما در این مقاله الگوریتمی کارا از لحاظ مصرف انرژی ارائه نموده‌ایم که با استفاده از آنتن‌های جهتدار موجود در حسگر ها قادر به تشخیص لینک‌های معتبر می‌باشد. در روش ارائه شده، هر گره با استفاده از یک گره تصدیق کننده در همسایگی خود، وجود و یا عدم وجود Wormhole را مشخص می‌نماید. در این روش شرایطی خاص را درخصوص تعیین گره بازبین قرار داده‌ایم. نقطه قوت روش ارائه شده نسبت به دیگر روش‌های مشابه، بهینگی مصرف انرژی و افزایش تشخیص تعداد لینک‌های معتبر می‌باشد. نتایج شبیه‌سازی نیز نشان از عملکرد موثرتر روش ارائه شده نسبت به روش‌های مشابه دارد.

واژه‌های کلیدی

شبکه‌های حسگر بی‌سیم، تشخیص Wormhole، مصرف بهینه انرژی.

۱- مقدمه

شبکه‌های حسگر بی‌سیم تشکیل شده از چندین حسگر می‌باشند که در ناحیه ای دور از دسترس به جمع‌آوری اطلاعات می‌پردازند و پس از یکسری پردازش‌های اولیه آن‌ها را برای ایستگاه اصلی[۱] ارسال می‌کنند [۱].

امروزه با توجه به افزایش کاربردهای این شبکه‌ها از جمله کاربردهای محیطی، پزشکی، نظامی، صنعتی و ... و همچنین محدودیت‌هایی که از قبیل: انرژی، پهنای باند محدود، توان پردازش پایین، حافظه و... وجود خواهد داشت، نیاز به برقراری امنیت به صورت بهینه و کارا و مرتبط با نوع آن کاربردها احساس می‌شود.

شبکه‌های حسگر در خصوص اجرای الگوهای امنیتی شبکه‌های سنتی امروزی دارای محدودیت‌هایی می‌باشند. به عنوان مثال در این شبکه‌ها نمی‌توان الگوریتم امضاء دیجیتال را به کاربرد زیرا از نظر میزان حافظه و محاسبات محدودیت وجود دارد. لذا می‌بایست الگوریتم هایی را در خصوص مرتفع کردن نیاز امنیتی این شبکه‌ها به کاربرد که منابع حسگر را به شدت مورد مصرف قرار ندهند [۲].

اهداف امنیتی شبکه‌های حسگر بی‌سیم عبارتند از [۲]:

- محرمانگی داده[۲]: محرمانگی داده به مفهوم رمز نمودن داده‌ها جهت غیرقابل درک نمودن آن از دید حسگرهای غیرمجاز را می‌توان به عنوان اولین نیاز امنیتی شبکه‌های حسگر برشمرد[۳].
- صحت داده: الگوریتم‌های صحت داده در خصوص عدم دستکاری داده در بین راه توسط حسگرهای دیگر ارائه

[1] Base Station

[2] Data Confidentiality

ارائه شده‌اند. در ابتدایی‌ترین راهکار می‌توان MAC[1] پیام را محاسبه و آن را توسط پیام اصلی ارسال نمایند.

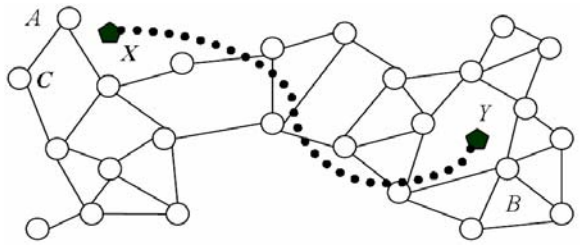
- تازگی داده‌ها[2]: امکان ارسال مجدد داده‌های قبلی را از حسگرهای دشمن گرفته و تضمین می‌کنند داده‌هایی که اخیراً توسط گیرنده دریافت شده‌اند، تازه بوده و قدیمی نمی‌باشند [۴].

- مقاومت و ضربه‌پذیری[3]: شبکه‌های حسگر باید در مقابله با حملات بسیاری مقاوم باشد و همچنین اگر حمله‌ای به طور موفق آمیزی صورت گرفت این حمله باید دارای تاثیری محلی باشد و کل شبکه را مختل نکند.

- ساختار این مقاله در ادامه بدین صورت است که در بخش دوم به بررسی انواع حملات متداول شبکه‌های حسگر و روش‌های کشف آن خواهیم پرداخت. در بخش سوم، به بررسی جزئیات الگوریتم ارائه شده و در بخش چهارم نتایج شبیه‌سازی را ارائه خواهیم نمود و در بخش پنجم نتیجه‌گیری قرار خواهدگرفت.

۲- کارهای مرتبط

حملات شبکه‌های حسگر را می‌توان از دو دیدگاه اصلی بررسی نمود؛ دیدگاه اول، حملاتی هستند که علیه مکانیزم‌های امنیتی موجود در شبکه صورت می‌گیرند و دیدگاه دوم، آن دسته از حملاتی که در خصوص عملیات عادی شبکه مانند مسیریابی، جمع‌آوری داده و... صورت می‌گیرند. همچنین نوع حمله را بر اساس قابلیت‌های حسگرهای دشمن می‌توان به دو کلاس Mote و Laptop تقسیم کرد. در نوع کلاسLaptop، حسگرها از قابلیت‌های بیشتری و محدودیت کمتری از لحاظ منابع برخوردارند، در حالیکه در کلاس Mote از لحاظ نحوه کارایی و سطح تجهیزات سخت‌افزاری مانند حسگرهای معمولی در سطح شبکه می‌باشد [۵،۶]. از بین تمامی حملاتی که در شبکه‌های حسگر صورت می‌گیرد مانند DoS، Sybil، Sinkhole، Hello Flood، حمله Wormhole را می‌توان خطرناک‌ترین و قویترین نوع آنها دانست. در این نوع حمله حسگر دشمن به ایجاد یک کانال ارتباطی در شبکه روی می‌آورد که بتواند اختلال‌هایی را در عملکرد شبکه ایجاد کند. در این حمله حسگرهای دشمن بدون اینکه حسگرهای دیگری را مورد حمله و آسیب قرار دهند اطلاعاتی را که در یک نقطه از شبکه دریافت می‌کنند برای حسگر همدست دیگر در آنسوی شبکه از طریق یک کانال مجزا و پر سرعت ارسال می‌کنند (Wormhole نوع زوج- شکل ۱).



شکل۱- وجود Wormhole با دو حسگر(X,Y)، دو حسگر A,B را به عنوان همسایه به یکدیگر معرفی می‌کند.

در بعضی از موارد تنها یک Wormhole بین دو حسگر که در شعاع یکدیگر نمی‌باشند قرار گرفته و ارتباط بین آنها را ایجاد می‌کند(Wormhole نوع فرد). کشف Wormhole نوع دوم در مقایسه با نوع اول مشکلتر خواهد بود. این نوع حمله باعث مشکلاتی در خصوص عملیات مسیریابی و جمع‌آوری داده می‌شود که در نهایت باعث مصرف انرژی و کوتاه شدن عمر شبکه می‌گردد. نکته بسیار مهم در خصوص این حمله این است که هیچ نوع الگوریتم رمز نگاری قادر به مقابله با آن نمی‌باشد و در مقایسه با دیگر حملات تشخیص و مقابله با آن بسیار سخت‌تر می‌باشد. روش‌های تشخیص حمله Wormhole را می‌توان به صورت زیر دسته‌بندی کرد:

- براساس اطلاعات زمانی [۸][۱۰] :در[۱۰] الگوریتمی ارائه شده است که لینک‌هایی با تاخیری بیش از حد معمول را به عنوان لینک مشکوک[4] فرض می‌کند و آنها را بر اساس ارسال پیام $HELLO_{req}$ و$HELLO_{rep}$ از نظر تاخیر واقعی ارتباط مورد ارزیابی قرار می‌دهد.

- براساس اطلاعات توپولوژی شبکه [۹][۷]: Hayajneh و همکارانش در[۷] روشی را جهت تشخیص وجود Wormhole در شبکه‌های حسگر بی‌سیم ارائه نمودند. در این روش نیازی به وجود تجهیزات خاص و همزمانی و یا وجود حسگرهای راهنما در شبکه نمی‌باشد بلکه این روش مبتنی بر وجود اختلافات در اطلاعات مسیریابی بین همسایه‌ها می‌باشد.

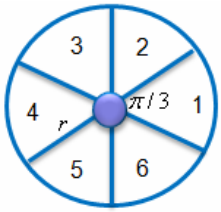
- براساس وجود حسگرهای راهنما[5] در بین حسگر های شبکه [۱۱]: Neronghny و همکارانش در [۱۱] روشی را جهت تشخیص Wormhole در شبکه مبتنی بر حسگرهای خاص منظوره ارائه داده‌اند. این روش قادر به شناسایی Wormholeهای چندگانه[6] نیز می‌باشد. این روش از حسگرهای خاص به نام "راهنما" در سراسر شبکه استفاده می‌کند که وظیفه این حسگرها تشخیص و تعیین محل Wormholeها می‌باشد.

- براساس سخت افزار خاص در حسگرها مانند GPS، آنتن‌های جهتدار [۱۲] [۸]: L. Hu و همکارانش در [۱۲] دو روش را جهت

[1] Message Authentication Code
[2] Data Freshness
[3] Robustness and Survivability

[4] Suspicious
[5] Beacon
[6] Multiple Wormhole

تشخیص Wormhole ارائه داده‌اند. روش اول تنها در خصوص شناسایی Wormholeهای زوج و روش دوم تنها در خصوص Wormholeهای زوج و فرد می‌باشد. در این دو روش از آنتن‌های جهتدار در حسگرها استفاده می‌شود. ایده اصلی اینست که اگر حسگرها بتوانند جدول همسایگی خود را به درستی ایجاد نمایند، تاثیر وجود Wormhole در شبکه به حد بسیار زیادی کاهش پیدا خواهد کرد. در این روش برای هر حسگر شش جهت(ناحیه) ارسال در نظر گرفته شده است (شکل ۲). در ابتدای کار شبکه هر حسگر (A) با ارسال پیام HELLO در هر یک از شش جهت سعی در تکمیل جدول همسایگی خود دارد.



شکل۲- ناحیه‌های ارسال درآنتن جهتدار

حسگر دریافت کننده بسته HELLO (حسگر B) اگر در ناحیه معکوس (۱و۴، ۲و۵، ۳و۶ نسبت به یکدیگر در جهت معکوس قرار گرفته‌اند) با آن قرار گرفته باشد با ارسال بسته ای رمزنگاری شده صحت وجود حسگر A را بررسی کرده و خود را به عنوان همسایه آن معرفی می کند. (تنها یک ششم حسگرهای موجود در یک سر Wormhole مورد حمله قرار خواهند گرفت زیرا فقط یک ناحیه مخالف با ناحیه ارسال قرار دارد). برای جلوگیری از ایجاد ارتباط همسایگی از طریق Wormhole، حسگر B جهت پاسخ به بسته HELLO بایستی از برخی از حسگرهای همسایه‌اش که دارای شرایطی خاص می‌باشند در خصوص تشخیص ارتباط A و B کمک بگیرد، به این حسگرها اصطلاحا بازبین گویند. اگر حسگر بازبین[۷] ای موجود باشد و به حسگرB پاسخ دهد آنگاه حسگر B، به A پاسخ مثبت ارسال کرده، در غیر این صورت(حسگر بازبین ای پاسخ آن را ندهد و یا آینکه یک حسگر معمولی شرایط حسگر بازبین را نداشته باشد) آنگاه B استنباط می‌کند که ارتباط همسایگی از طریق Wormhole صورت گرفته و در این حالت برای حسگر A پاسخی ارسال نمی‌کند. زمانی که فقط یک حسگر Wormhole بین دو حسگر قرار گیرد (Wormhole نود فرد) شرایط تشخیص Wormhole سخت‌تر می‌گردد. حسگرهای بازبین دیگر قادر به شناسایی آن نمی‌باشند و به همین دلیل شرایط حسگر بازبین را طوری تغییر داده است که ارتباط به درستی صورت گیرد. این الگوریتم گرچه وجود Wormhole را به درستی تشخیص خواهد داد و نیازی به وجود همزمانی بین حسگرها درشبکه نخواهد داشت، اما دارای مشکلات زیر می‌باشد:

- مصرف انرژی بالا: الگوریتم ارائه شده جهت تشخیص Wormhole به دلیل ارسال و دریافت بسته های اطلاعاتی متعددی، مصرف انرژی بالایی دارد.
- عدم تشخیص لینک‌های معتبر: بسیاری از لینک‌های مجاز و معتبر بین حسگرهای شبکه به دلیل عدم وجود گره بازبین ایجاد نمی‌شوند. (این حسگرها بیشتر در لبه‌های شبکه قرار دارند)

شرایط سخت تعیین گره بازبین: تعیین شرایطی سخت برای انتخاب حسگر همسایه به عنوان بازبین که بتواند هردو نوع حمله Wormhole را شناسایی کند؛

- تشخیص نادرست: الگوریتم شماره یک در [۱۲] لینک‌های غیرمجاز در اطراف Wormholeهای فرد را، معتبر تشخیص می‌دهد.

۲- الگوریتم ارائه شده

از جمله امتیازاتی که روش ارائه شده نسبت به روش‌های مشابه خود دارد می‌توان به موارد زیر اشاره نمود:

۱. عدم نیاز به همزمانی سخت بین حسگرها
۲. عدم نیاز به تجهیزات خاص مانند GPS
۳. عدم نیاز به حسگرهای خاص منظوره
۴. مصرف انرژی بهینه در خصوص تشخیص لینک‌های معتبر.

روشی که ما در این مقاله ارائه داده‌ایم، باعث می‌شود حسگرهای موجود در شبکه بتوانند همسایه‌های خود را به درستی شناسایی نمایند و در این حین از حمله حسگرهای Wormhole به حسگرهای شبکه جلوگیری نماید زیرا با انتخاب صحیح حسگرهای همسایه، حسگرهای Wormhole دیگر قادر به انتقال ترافیک شبکه از منطقه‌ای به منطقه‌ای دیگر نخواهند بود. به عبارت دیگر روش ارائه شده با تکیه بر مصرف بهینه‌تر انرژی به تشخیص حسگرهای Wormhole می‌پردازد و وجود حسگرهای Wormhole را برای حسگرهای دیگر آشکار می‌سازد.

۳-۱-فرضیات مسئله

سیستمی شامل N حسگر را که به صورت تصادفی در محیطی پخش شده‌اند را در نظر بگیرید، در این سیستم i امین حسگر(S_i) با شعاع پوشش و ارسال $T_{\text{cov erage}}$ مجهز به آنتن جهت دار با شش ناحیه درنظر گرفته شده است. دیگر تعاریف عبارتند از:

۱. $H(M)$: چکیده پیام M توسط تابع درهم ساز H
۲. K_{share}: کلید مشترک بین تمامی حسگرهای شبکه

[7] Verifier Node

۳. $E_{KAB}(M)$: پیام رمز شده توسط کلید K مشترک بین دو حسگر A و B

۴. Z_{Tx}^{A} : شماره ناحیه ای که حسگرA بسته خود را ارسال می‌کند

۵. Z_{Rx}^{A} : شماره ناحیه ای که حسگرA بسته‌ای را دریافت کرده است

۶. $\overline{Z_{Rx}^{A}}$: شماره ناحیه معکوس با ناحیه Z_{Rx}^{A}، به عنوان مثال برای حسگری با ۶ ناحیه ۱،۲،۳،۴،۵،۶ به ترتیب ناحیه‌های معکوس عبارتند از ۴،۵،۶،۱،۲،۳ .

۷. $\overline{Z_{Tx}^{A}}$: ناحیه معکوس با ناحیه Z_{Tx}^{A}.

مدل انرژی ارسال و دریافت داده مطابق با مدل انرژی در LEACH [۱۳] در نظر گرفته شده است، بدین گونه که اگر فاصله فرستنده تا گیرنده (d) بیشتر از d_0 باشد از مدل چند مسیری (اتلاف توان d^4) و در غیر این صورت از مدل فضای آزاد (اتلاف توان d^2) برای ارسال (l) بیت داده استفاده می شود.

$$E_{Tx}(l,d) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2 & d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4 & d \geq d_0 \end{cases} \quad (۱)$$

$$E_{Rx}(l) = E_{Rx-elec}(l) = lE_{elec} \quad (۲)$$

E_{elec}: مقدار انرژی مصرفی برای راه‌اندازی مدار فرستنده یا گیرنده و ε_{amp}: انرژی مورد نیاز تقویت کننده انتقالی برای دستیابی به E_b/N_0 مورد قبول، می‌باشد.

۳-۲-جزئیات الگوریتم

شبه کد الگوریتم ارائه شده در شکل ۳ مشخص شده است. در ابتدا کار شبکه، حسگر A شروع به شناسایی همسایه‌های خود می‌کند. جهت این کار بسته HELLO را در هر یک از ناحیه‌های خود به صورت همه پخشی ارسال می‌کند (خط ۲).

```
1: for i = 1: N
2:   S_i Send HELLO Packet
       (E_Kshare(HELLO | ID_i | Z^i_Tx | R)
3:   for all S_i's Neighbours
4:     S_j Receive HELLO Packet
5:     S_j Send WDR Packet
       (ID_j | H(HELLO | ID_i | Z^i_Tx, R)
6:     for all S_j's Neighbours
7:       if S_k has both Conditions
                 // S_k is Verifier
8:         S_k Send WNP Packet
                 (ID_k | R | E_Kkj(WNP))
9:       elseif has first Condition
10:        S_k Send CLEAR Packet
                 (ID_k | R | E_Kkj(CLEAR))
11:      endif
12     if S_j Receive CLEAR Packet then
13:      Send ACCEPT Packet
         (ID_j | R | E_Kji(ACCEPT))
14:    endif
15:    Next j
16: Next i
```

شکل۳- شبه کد الگوریتم ارائه شده

رمز نگاری بسته ارسالی باعث می‌گردد که Wormhole از ماهیت بسته مطلع نشود و خود را به عنوان یک حسگر معمولی معرفی نکند. حسگری که در ناحیه معکوس با ناحیه ارسال A قرار گرفته باشد(با توجه به فیلد Z_{Tx}^{A}) مراحل بعدی الگویتم را ادامه می دهد.

حسگر B که در ناحیه $\overline{Z_{Tx}^{A}}$ قرار گرفته است، با دریافت بسته HELLO و بازگشایی آن، برای مطلع شدن از وجود Wormhole بسته تقاضای WDR (Wormhole Detection Request) را به تمامی ناحیه‌های خود به جز دو ناحیه Z_{Rx}^{A} (ناحیه‌ای که پیام HELLO را از حسگر A دریافت کرده است) و $\overline{Z_{Rx}^{A}}$ (معکوس ناحیه Z_{Rx}^{A}) ارسال می‌کند (خط ۵).

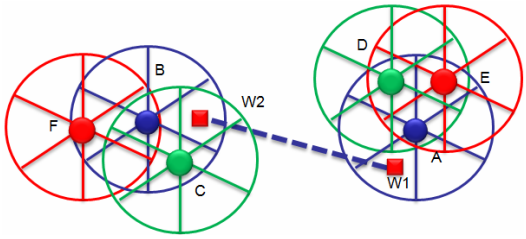
حسگر گیرنده پیام WDR(حسگرC)، اگر دو شرط زیر را داشته باشد پیام WNP (Wormhole Notification Packet) را در خصوص مطلع‌سازی حسگر B از وجود Wormhole برای آن ارسال می‌کند.این دو شرط عبارتند از:

۱- دریافت حداقل یک پیام از حسگر A.

۲- داشتن یک یا دو پیام مشابه با مقدار چکیده برابر با چکیده موجود در پیام WDR از حسگر A (پیام را به صورت همه پخشی توسط Wormhole ارسال می‌شود)

حسگری که دو شرط فوق را دارا باشد، پیام WNP را برای حسگر B ارسال می‌کند (خط ۸) اما حسگری که فقط شرط اول را دارا باشد پیام CLEAR را برای حسگر B ارسال می‌کند(خط ۱۰). حسگر B با دریافت پیام CLEAR، پیام ACCEPT را برای حسگر A ارسال می‌کند (خط ۱۳) و حسگر A آن را در جدول همسایه‌های خود اضافه می‌کند. در غیر این صورت اگر حسگر B هیچیک از پیام‌های WNP وCLEAR را دریافت نکرد، پاسخی را برای حسگر A ارسال نمی‌کند. در ادامه مراحل کار روش ارائه شده را در دو مثال زیر بررسی خواهیم کرد.

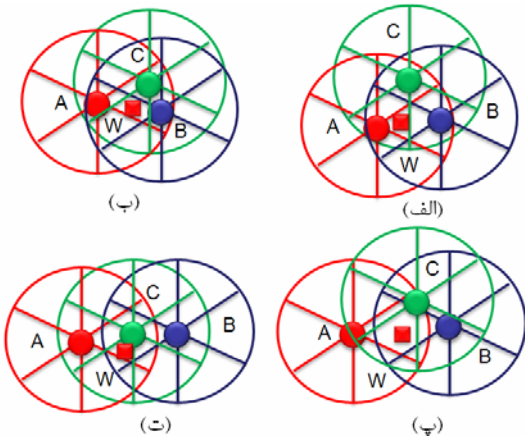
مثال اول: در شکل ۴، ابتدا حسگر A پیام HELLO را به ترتیب از ناحیه ۱ تا ۶ ارسال می کند. سپس حسگر ها وارد مرحله بعد می‌شوند و سعی می‌کنند وجود و یا عدم وجود Wormhole را کشف نمایند.



شکل۴- وجود Wormhole با دو حسگر در شبکه

حسگر E پیام A را از ناحیه ۵ دریافت می‌کند و پیام WDR را به ناحیه‌های ۶،۴،۳،۱ ارسال می‌کند. حسگر D چون فقط شرط اول را داراست پیام CLEAR را برای حسگر E ارسال می‌کند. سپس حسگرE پیام ACCEPT را برای A ارسال می‌کند. حسگر D هم به همین ترتیب با دریافت پیام CLEAR از حسگر E به همسایه‌های حسگر A می‌پیوندد. حسگر B پیام HELLO را از طریق W2 دریافت می‌کند و پیام WDR را در نواحی ۵،۳،۲ و۶ ارسال می‌کند. حسگر C با داشتن هر دو شرط (دریافت حداقل یک پیام از حسگر A و دریافت پیامی برابر با پیام دریافت شده در B) پیام WNP را برای حسگر B ارسال می‌کند و آن را از ارسال پیام ACCEPT به حسگر A باز می‌دارد؛ اما حسگر F به دلیل نداشتن شرط اول (پیامی را از حسگر A دریافت نکرده است) هیچ پیامی را به حسگر B ارسال نمی‌کند.

مثال دوم: در این مثال وجود Wormhole با یک حسگر بررسی خواهد شد (شکل ۵). در هر یک از حالات زیر حسگر A پیام HELLO را ارسال می‌کند و حسگر B جهت پاسخ به آن پیام WDR را در نواحی مشخص ارسال می‌کند.



شکل۵- وجود Wormhole با یک حسگر در شبکه

در دو حالت (الف) و (ب) وجود Wormhole توسط حسگر C به دلیل دارا بودن هر دو شرط، تشخیص داده شده و حسگر B را از ارسال پیام ACCEPT باز می‌دارد. (در حالت (ب) حسگر C دو پیام مشابه با پیام دریافتی در حسگر B دریافت می‌کند، یک پیام از حسگر A در ناحیه ۴ و یک پیام مشابه دیگر از حسگر Wormhole در ناحیه ۵).

درحالت (پ) حسگر C باز هم وجود Wormhole را تشخیص می‌دهد. اما در حالت (ت) حسگری جهت دریافت پیام WDR وجود ندارد زیرا حسگر Bپیام WDR را به نواحی ۵،۳،۲ و ۶ ارسال می‌کند و هیچ لینکی بین CوA و همچنین بین CوB ایجاد نمی‌گردد.

۴- شبیه سازی

در این قسمت الگوریتم پیشنهادی را با دو روش ارائه شده در [۱۲] به کمک نرم‌افزار MATLAB از نظر انرژی مصرفی جهت تشخیص لینک‌های معتبر و تعداد لینک‌های تشخیص داده شده با یکدیگر مقایسه نموده‌ایم.

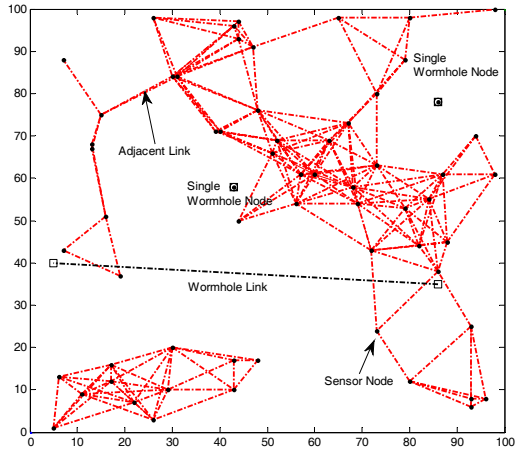
۴-۱-پارامترهای شبیه سازی و یک نمونه اجرای آن

جدول ۱ پارامترهای شبیه‌سازی را نشان می دهد.

جدول۱- پارامترهای شبیه سازی

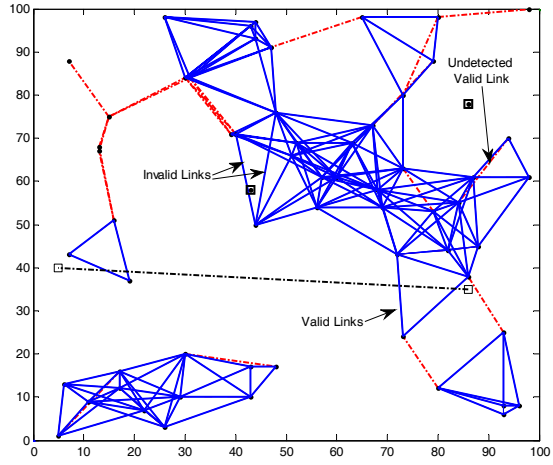
عنوان	مقدار
سایز شبکه	$100\times100m^2$
تعداد حسگر(N)	20-90
شعاع پوشش	18 m
انرژی اولیه	0.1 J
E_{elect}	50 nJ/bit
ε_{fs}	10 pJ/bit/m^2
اندازه بسته‌ها	128 byte
تعداد Wormhole های زوج	3
تعداد Wormhole های فرد	3

شکل ۶ نمونه‌ای از چیدمان تصادفی ۶۰ حسگر به همراه محدوده قابل پوشش به شعاع ۲۰ متر در محیط ۱۰۰×۱۰۰ مترمربع را نمایش می‌دهد. در این شکل لینک‌های همسایگی بین دو حسگر مجاور که در شعاع یکدیگر قرار دارند به صورت خط چین نشان داده شده است. همچنین در این شبکه یک Wormhole زوج و دو Wormhole فرد مشخص شده است.



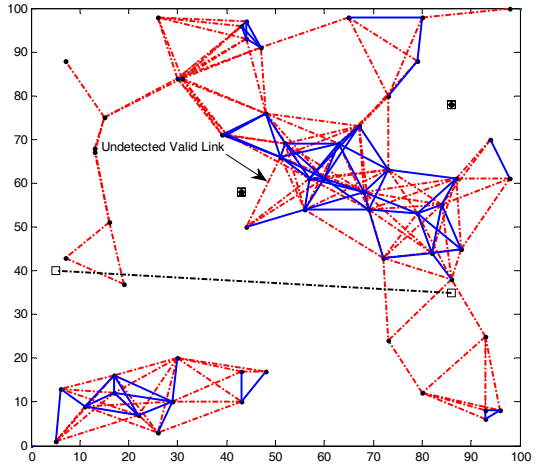
شکل۶- شبکه ای با ۶۰ حسگر به شعاع پوشش ۲۰متر

با اجرای الگوریتم شماره ۱(قابلیت کشف Wormhole های زوج) در [۱۲] برروی این شبکه، ۱۸۱ لینک از بین ۲۰۱ لینک همسایگی به عنوان لینک معتبر انتخاب شده است. از این ۱۸۱ لینک ۲ لینک نامعتبر که در شکل مشخص شده است، به عنوان لینک معتبر شناخته شده است. (شکل ۷ را مشاهده نمایید)



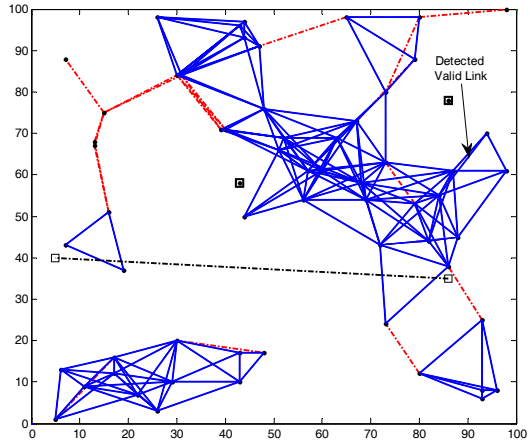
شکل۷- نمونه ای از اجرای الگوریتم شماره ۱ در [۱۲]

همچنین با اجرای الگوریتم شماره ۲در [۱۲] با قابلیت کشف Wormholeهای زوج و فرد، تنها ۵۲ لینک از بین ۲۰۱ لینک همسایگی به عنوان لینک معتبر انتخاب شده است. همانطور که در شکل ۸ مشاهده می شود ۵۶٪ از لینک‌های معتبر به دلیل عدم حضور گره بازبین با شرایطی خاص تشخیص داده نشده‌اند.



شکل۸- نمونه ای از اجرای الگوریتم شماره ۲ در [۱۲]

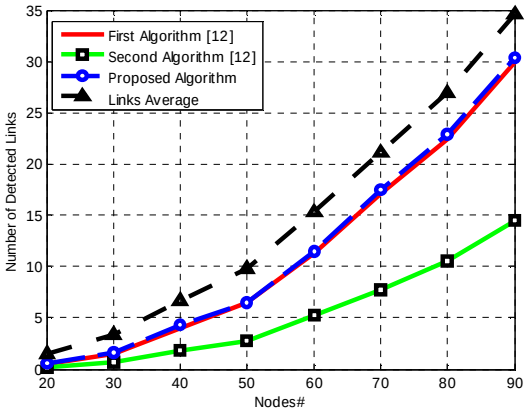
به دلیل وجود شرایط بهینه‌تر جهت انتخاب گره بازبین، الگوریتم پیشنهادی ما توانسته است ۱۸۲ لینک از ۲۰۱ لینک همسایگی موجود را به عنوان لینک معتبر و عاری از Wormhole زوج و منفرد تشخیص دهد(شکل ۹). همچنین نکته قابل توجه اینست که الگوریتم پیشنهادی این تعداد لینک معتبر را با مصرف انرژی کمتری نسبت به الگوریتم‌های مشابه خود در[۱۲] مشخص نموده است.



شکل۹- نمونه ای از اجرای الگوریتم پیشنهادی

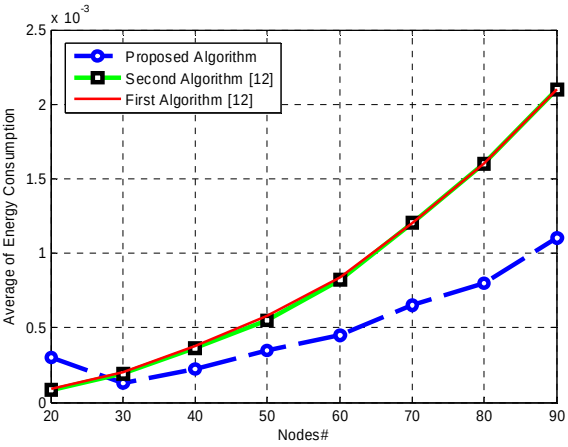
۴-۲- مقایسه انرژی و تشخیص لینک‌های معتبر

در ادامه الگوریتم پیشنهادی را از دیدگاه تعداد کل لینک‌های معتبر و همچنین مصرف انرژی در خصوص مشخص کردن لینک‌های معتبر مشخص شده، با هر دو الگوریتم ارائه شده در [۱۲]مقایسه نموده‌ایم. (تعداد دفعات اجرا در هر چگالی ۱۰۰ مرتبه می‌باشد).



شکل10- مقایسه تعداد لینک های معتبر تشخیص داده شده

همانطور که در شکل 10 مشاهده می شود، الگوریتم ارائه شده تعداد لینک‌های بسیاری را در حضور Wormhole فرد و زوج تشخیص داده است. اما الگوریتم شماره 1 در [12] که تنها قابلیت شناساییWormholeهای زوج را داشته است، برخی از لینک‌هایی که توسط Wormholeهای فرد ایجاد شده‌اند را به عنوان مسیرهای معتبر انتخاب کرده است. همچنین الگوریتم شماره 2 در [12] که قابلیت شناخت Wormholeهای فرد را نیز داراست، به دلیل قرار دادن شرایط سخت در انتخاب نود های بازبین، تعداد لینک‌های معتبر تشخیص داده شده به شدت کاهش یافته است. بهبودی که در الگوریتم ارائه شده مشاهده می‌شود به دلیل در نظر گرفتن شرط‌هایی بهینه تر در خصوص انتخاب حسگر "بازبین" می‌باشد. در حالی که در الگوریتم‌های [12] شرایطی برای انتخاب حسگر "بازبین" در نظر گرفته شده است که احتمال وجود یک حسگر "بازبین" را بسیار پایین می‌آورد. همچنین در شکل 11، انرژی مصرفی جهت تشخیص صحیح حسگرهای همسایه در چگالی‌های متفاوت با یکدیگر مقایسه شده است. همانطور که مشخص شده است انرژی مصرفی الگوریتم ارائه شده نسبت به دو الگوریتم[12] بسیار بهتر عمل کرده است و این به دلیل طراحی بهینه‌تر مراحل شناخت لینک‌های معتبر الگوریتم ارائه شده می‌باشد.



شکل11- مقایسه انرژی مصرفی درخصوص تشخیص لینک های معتبر

5- نتیجه گیری

ما در این مقاله حمله Wormhole در شبکه‌های حسگر بی سیم را به همراه انواع روش‌های مقابله با آن، مورد بررسی قرار دادیم. در این نوع حمله یک حسگر دشمن ترافیک شبکه را از یک منطقه به وسیله حسگر همدست خود به منطقه‌ای دیگر ارسال می‌کند، که این خود باعث مشکلات فراوانی می‌گردد از جمله می‌توان به مهمترین آنها یعنی انتخاب اشتباه نود همسایه و افزایش مصرف انرژی در ارسال داده‌های تکراری اشاره نمود. ما در این مقاله الگوریتمی کارا از لحاظ مصرف انرژی ارائه نموده‌ایم که با استفاده از آنتن‌های جهتدار موجود در حسگرها، هر حسگر با استفاده از یک گره تصدیق کننده در همسایگی خود، وجود و یا عدم وجود Wormhole را مشخص می‌نماید. نتایج شبیه سازی نشان از عملکرد موثرتر روش ارائه شده از لحاظ مصرف انرژی و تشخیص تعداد لینک‌های معتبر، نسبت به روش‌های مشابه خود دارد.

مراجع

[1] I. F. Akyildiz et al., “Wireless sensor networks: a survey”, Computer Networks, March 2002.
[2] Mayank Saraogi,” SECURITY IN WIRELESS SENSOR NETWORKS” Communications of the ACM Volume 47 , Pages: 53 - 57 , June 2004
[3] [3] Chris Karlof, Naveen Sastry, David Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. ACM SenSys 2004.
[4] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar. SPINS: Security Protocols for Sensor Networks. (MobiCom 2001).
[5] C. Karlof and D. Wagner. “Secure Routing in Sensor Networks: Attacks and Countermeasures”. First IEEE International Workshop on Sensor Network Protocols and Applications, May, 2003.
[6] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong,” Security in Wireless Sensor Networks: Issues and Challenges” Proceedings of 8th IEEE ICACT 2006, Volume II, February 20-22, Phoenix Park, Korea, 2006, pp. 1043-1048
[7] Thaier Hayajneh, Prashant Krishnamurthy, David Tipper ,”DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad hoc Networks” 2009 Third International Conference on Network and System Security
[8] Y.-C. Hu, A. Perrig, and D. Johnson, “Wormhole attacks in wireless networks,” IEEE Journal on Selected Areas in Communications, 2006.
[9] R. Maheshwari, J. Gao, and S. R. Das, “Detecting wormhole attacks in wireless networks using connectivity information,” INFOCOM, 2007.
[10] Farid Naït-Abdesselam," Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks" SECURITY IN MOBILE AD HOC AND SENSOR NETWORKS IEEE Communications Magazine • April 2008
[11] He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan,” Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes”,World Academy of Science, Engineering and Technology 55, 2009

[12] L. Hu and D. Evans, “Using directional antennas to prevent wormhole attacks,” NDSS, 2004.
[13] W. Heinzelman, J. Kulik, and H. Balakrishnan, “Adaptive protocols for information dissemination in wireless sensor networks”, (MobiCom’99), Seattle, WA, August 1999.