بررسی حملات شبکه‌های حسگر بی‌سیم و اثرات آن‌ها

وحیده بابائیان[1]، جواد محمودی دستجردی

1-عضو هیأت علمی دانشگاه صنعتی بیرجند، دانشکده مهندسی کامپیوتر و صنایع، بیرجند

2- کارشناس دانشگاه صنعتی بیرجند، دانشکده مهندسی کامپیوتر و صنایع، بیرجند
babaiyan@birjandut.ac.ir

خلاصه

شبکه‌های حسگر بی‌سیم به عنوان یکی از تکنولوژی حاکم در دهه ی پیش رو است که فرصت‌های زیادی را برای محققان ایجاد کرده است، این شبکه‌ها به وسیله ی صدها و یا حتی هزاران نود ساخته شده است که هر نود شامل یک یا چند حسگری است که دارای گیرنده رادیویی، یک آنتن داخلی / خارجی، یک میکروکنترلر و یک باتری است. این شبکه‌ها با انواع چالش‌های مختلفی رو به رو است پس باید یکسری اهداف امنیتی برای این شبکه‌ها در نظر بگیریم که در آن تهدیدها را تحلیل کرده و برای آن‌ها راه حل‌هایی در نظر بگیریم. در این مقاله شبیه سازی از این حملات را به وسیله ی شبیه ساز NS2 انجام می‌دهیم. با شبیه سازی حملات می‌توان عملکرد شبکه را آزمایش کرده سپس شبکه را تحت نظارت خود قرار دهیم.

کلمات کلیدی: شبکه‌های حسگر بی‌سیم، شبیه ساز NS2، حملات

1. مقدمه

شبکه‌های حسگر بی‌سیم یک سیستم ناهمگن است که از ترکیبی از سنسورها و محرک‌ها و با هدف‌های محاسباتی تشکیل شده است. این شبکه‌ها دارای صدها و یا حتی هزاران نودهای خودکار توزیع شده هستند تا بتوانند شرایط فیزیکی یا محیطی مثل دما، صدا، فشار و. . را کنترل کرده و سپس شرایط اندازه گیری شده را به‌ایستگاه اصلی منتقل کنند[1, 2]. بر اساس زیرساخت‌های موجود، شبکه‌های حسگر بی‌سیم می‌تواند تقریباً در هر محیطی به ویژه در مناطقی که اتصالات سیمی‌امکان پذیر نیست کارکنند. همچنین روش استقرار سنسورها باید در یک محیط کنترل شده باشد تا در آن نظارت و مراقبت به خوبی صورت گیرد .

از شبکه‌های حسگر بی‌سیم در میدان جنگ و برنامه‌های کاربردی تجاری مثل بررسی ترافیک و ساختمآن‌ها، کنترل محل‌سکونت، مشاهده آلاینده‌ها در محیط زیست و خانه‌های هوشمند استفاده می‌شود [3]. این شبکه‌ها به خاطر محدودیت منابعی مثل باتری، قدرت محاسبات و محدوده ارتباطی نسبت به انواع حمله‌ها آسیب پذیرند همچنین نودهای حسگر در ناحیه‌های بزرگ پیاده سازی شده و با محیط فیزیکی و مردم تعامل نزدیکی دارد. از آنجا که شبکه‌های حسگر وظایف و مأموریت‌های حیاتی را بر عهده دارند پس باید اهداف امنیتی در این شبکه‌ها را مد نظر قرار دهیم[4, 5] .

به خاطر ویژگی گسترده بودن و داشتن ارتباط ad-hoc در شبکه‌های حسگر بی‌سیم چالش‌های قابل توجهی ارائه شده است. یک شبکه ی حسگر بی‌سیم، یک شبکه خاصی است که نسبت به شبکه‌های سنتی محدودیت بسیاری دارد. [5]. حسگرها از صدها تا هزاران نود با انرژی کم تشکیل شده است که از طریق خطوط شبکه به هم متصل اند. وجود انواع مختلف برنامه‌های کاربردی در شبکه‌های حسگر باعث می‌شود که شبکه‌های حسگر بی‌سیم جزئی از زندگی انسان شود. برای به خوبی کار کردن شبکه به مقدار مورد نیاز حافظه، حافظه کد و انرژی نیاز داریم هرچند به خاطر محدود بودن اندازه‌این سنسورها این منابع محدودند. حافظه نودهای سنسور معمولاً محدود اند که اجرای مکانیزم‌های امنیتی را سخت می‌کند چرا که هر راه حل امنیتی طراحی شده باید در قالب کد، کوچک شده باشند. انرژی بزرگترین محدودیت در سنسورها است که اضافه کردن مکانیزم‌های امنیتی مثل رمز نگاری و رمزگشایی تاثیر عمیقی بر روی محاسبات انرژی می‌گذارد و این در حالی است که شارژکردن باتری یا عوض کردن آن به راحتی صورت نمی‌گیرد[4]. یکی از بزرگترین تهدیدهای امنیتی برای شبکه، رسانه ی ارتباط بی‌سیم است که به دلیل ویژگی همه پخشی بودن این شبکه‌ها، یک هکر به راحتی می‌تواند هر انتفالی را استراق سمع کند، تغییر دهد و یا جایگزین کند. رسانه بی‌سیم به مهاجم اجازه می‌دهد تا به راحتی بسته‌های معتبر را از بین ببرد و یا اطلاعات جعلی را به شبکه تزریق کند[1, 2].

وسعت ناحیه ی شبکه‌های حسگر بی‌سیم و تغییرات مکرر توپولوژی و بخش بندی شبکه خود باعث تغییر پذیری نودها و خطای نودها می‌شود، هزاران یا حتی میلیون‌ها نود بدون دانش قبلی از جایگاه خود هنگامی‌که پیاده سازی شوند می‌توانند ساختار شبکه را پیچیده کنند[4]. ماهیت ad-hoc شبکه‌های حسگر به‌این معنی است که هیچ ساختاری نمی‌تواند به صورت ایستا تعریف شود. توپولوژی شبکه همیشه به تغییرات ناشی از خطای نود، افزودن نود جدید

و یا تحرک نود حساس بوده است. نودها ممکن است به صورت هوایی مستقر شوند، بنابراین هیچ چیز از توپولوژی قبل از استقرار شناخته نمی‌شود. از آنجا که نودها ممکن است خراب شوند یا جایگزین شوند، طرح‌های امنیتی باید قادر باشند در این محیط پویا به خوبی کار کنند[2, 5].

امنیت یک از ویژگی‌های اصلی هر سیستم است این در حالی است که شبکه‌های حسگر بی‌سیم سنتی نسبت به انواع حملات آسیب پذیرند. حملات امنیتی برای شبکه‌های حسگر به خاطر دسترسی فیزیکی حسگرها و استفاده کم از ظرفیت شبکه ممکن است رخ دهد. این ضعف‌ها و حملات امنیتی در شبکه‌های حسگر بی‌سیم وجود دارد اما به وسیله ی استفاده از ساختارهای امنیتی متنوع میتوان از وقوع این حملات جلوگیری کرد. اهداف امنیتی در شبکه‌های حسگر مجازی باید شامل ویژگی‌هایی مثل اعتماد پذیری، جامعیت، در دسترس پذیری وتعیین هویت باشد در زیر ساختارهای امنیتی استاندارد را برای شبکه‌های حسگر بی‌سیم بررسی می کنیم[6]: اعتماد پذیری داده‌ها یک توانایی برای پنهان کردن ترافیک داده‌ها در مقابل هکر است پس هر ارتباط از طریق شبکه‌های حسگر امن باقی می‌ماند که خود مهمترین مسئله ی امنیتی در این شبکه است بنابرین اطلاعات باید تحت سیاستهای کنترلی مناسب قرار گیرد تا کاربران با هویت نامشخص نتوانند به اطلاعات دسترسی پیدا کنند. به طور مثال یک نود نباید داده‌هایش را برای همسایه‌هایش فاش کند چرا که یک هکر با ایجاد یک نود جعلی می‌تواند به اطلاعات دسترسی پیدا کند[4]. جامعیت داده، اعتماد پذیری داده را تأمین می کند در واقع تصدیق می کند که پیام در طول شبکه جایگزین نشده و یا تغییر نکرده است. جامعیت داده هنگامی‌زیر سؤال می‌رود که نود مخرب پیام‌های جعلی را در شبکه تزریق کند و یا شرایط نامناسب باعث صدمه زدن به کانال ارتباطی شود[7]. از زمانی که شبکه‌های حسگر بی‌سیم در محیط بی‌سیم عمومی‌استفاده شده است به مکانیزم‌های تعیین هویت برای شناسایی پیام‌های مخرب نیاز پیدا کرده‌ایم. مکانیزم‌های تعیین هویت به نود کمک می کند تا نودهایی که با آن‌ها در ارتباط است را شناسایی کند. اگر مکانیزم تعیین هویت وجود نداشته باشد،یک نود مخرب می‌تواند اطلاعات حساس را به دست آورد[7]. دسترس پذیری گره ها به توانایی نود برای استفاده از منابع می‌گویند یعنی باید شبکه‌های حسگر برای انتقال پیام‌ها در دسترس باشد و بتواند دسترس پذیری شبکه‌های حسگر را حتی در هنگام حمله ی پایدار نگه دارد[4].

2. انواع حملات امنیتی

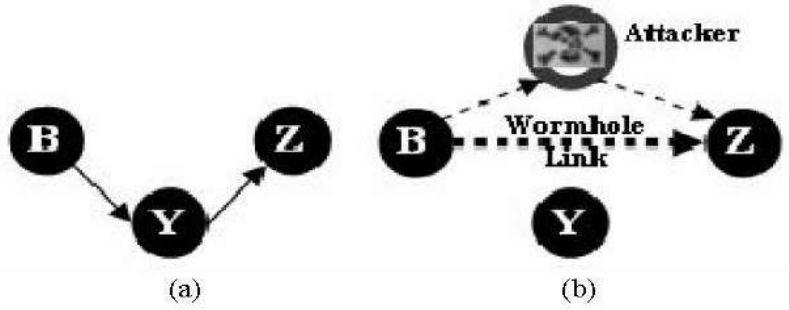
دلایل زیادی برای اهمیت امنیت در شبکه‌های حسگر وجود دارد. اولاً شبکه‌های بی‌سیم به خاطر ویژگی همه پخشی تحت حملات قرار گرفته است علاوه بر این در بیشتر موارد نودها در محیط‌های پرخطر قرار می گیرند. در این محیط‌ها امنیت فیزیکی آن‌ها تهدید می‌شود[8].

تکذیب سرویس (Dos): هر حادثه‌ای است که ظرفیت شبکه یا قابلیت‌های شبکه را به وسیله ی فعالیت‌های مخرب یا خطاهای غیر عمدی کاهش دهد. در دسترس نبودن شبکه برای کاربران قانونی یا جایگزینی داده قبل از خوانده شدن توسط نودهای حسگر باعث مختل شدن شبکه می‌شود برای نمونه در این نوع حمله هکر درخواست‌ها را به سرور زیاد می کند تا منجر به سرباری برای سرور شود یا تلاش می کند تا با استفاده از یک سیگنال با انرژی بالا، عملکرد شبکه را مختل کند، برای جلوگیری از این حملات باید از داده‌های اختصاصی شبکه مثل ID شبکه و. . . محافظت کرد [3, 9].

حمله Sybil: در این حمله یک هکر در شبکه چندین هویت را برای خود اتخاذ می کند بااستفاده از این حمله یک هکر می‌تواند در یک زمان در بیش از یک مکان قرار داشته باشد، یک نود تکی چندین هویت را به نودهای دیگر در شبکه ارائه می‌دهد تا بتواند به صورت مستقیم یا غیر مستقیم با نودهای قانونی ارتباط برقرار کرده و منابع آن‌ها را هدر دهد یا اطلاعات حساسی را از آن‌ها دریافت کند. در شبکه‌های حسگر، برنامه‌های تحمل خطا، تخصیص حافظه و توپولوژی شبکه، الگوریتم‌ها و پروتکل‌هایی هستند که به آسانی تحت تأثیر این حمله قرار می گیرند، برای جلوگیری از این حمله می‌توانیم به نودها اجازه دهیم که بسته‌ها را فقط به نودهایی ارسال کند که هویت آن‌ها تایید شده است. [3, 8, 9].

حمله Wormhole: حمله wormhole یک حمله بحرانی است که مهاجم بسته‌ها (یا بیت‌ها) را در یک مکان از شبکه ثبت می کند و آن‌ها را به محل دیگری از شبکه ارسال می کند. شکل 1 یک وضعیت در حمله wormhole را نشان می‌دهد. هنگامی که نود B (به عنوان مثال، ایستگاه پایه و یا هر حسگر دیگری) بسته‌های مسیریابی درخواستی را همه پخشی کند، مهاجم این بسته را دریافت کرده و همان بسته را برای همسایگان خود می‌فرستد در این وضعیت همسایه‌های مهاجم تصور می کنند که نود B در محدوده آن‌ها قرار دارد واین نود را به عنوان نود والد خود علامت گذاری می کنند. از این رو، حتی اگر نودهای قربانی چند گام از نود B جدا باشند، مهاجم آن‌ها را متقاعد می کند که B تنها یک گام دور از آن‌ها است، بنابرین بدین صورت یک wormhole ایجاد می‌شود[5].

شکل 1: حمله wormhole [5]



حمله sink hole: مانند حمله Wormhole است با این تفاوت که مهاجم ادعا می کند کمترین مسیر تا ایستگاه اصلی را دارد. بدین ترتیب تمام ترافیک را به سوی خود جذب می کند، برای دفاع در مقابل این حملات و همچنین حمله ی Wormhole باید از مکانیزم شمارش تعداد گام‌ها (hop-count) استفاده کنیم علاوه بر این طراحی دقیق پروتکل مسیریابی نیز می‌تواند مفید واقع شود. [3, 9].

حمله selective forwarding: در این حمله نودهای مخرب سعی می کنند که تمام ترافیک از طریق آن‌ها عبور کند سپس پیام‌های مهمی که به آن‌ها میرسد را دور بریزند و فقط یکسری از پیام‌های انتخابی خودشان را به‌ایستگاه اصلی بفرستند. شکل دیگر این حمله‌این است که تمام بسته‌هایی را که از یک یا چند نود هستند را دور بریزد، برای رفع این حمله باید از مسیرهای چندگانه استفاده کرده و همچنین به یک نود اجازه دهیم تا به صورت پویا گام بعدی خود را مشخص کند[9].

حمله Hello Flood: این حمله یکی از آسان ترین حمله‌ها در شبکه‌های حسگر بی‌سیم است. در بیشتر پروتکل‌ها، نودها نیاز دارند تا بسته‌های Hello را برای اعلان حضورخود همه پخشی کنند و این در حالی است که یک هکر می‌تواند بسته‌های Hello را با قدرت انتقال بالا همه پخشی می کند. نودهایی که پیام را دریافت می کنند تصور می کنند که نود فرستنده به آن‌ها نزدیک است پس بسته‌هایشان را به وسیله ی این نود مخرب می‌فرستند. برای جلوگیری از این حملات می‌توانیم از پروتکل‌های تعیین هویت استفاده کنیم [8] .

استراق سمع: به وسیله ی کوش دادن به داده، هکر می‌تواند به راحتی محتوای کانال ارتباطی مثل داده‌های مهم پیکربندی را کشف کند[1].

حمله ی فیزیکی: برعکس دیگر حمله‌ها، حمله ی فیزیکی نودهای حسگر را به طور همیشگی خراب می کند، به طور مثال هکرها کلیدهای رمزنگاری را خارج می کنند، در مدارات الکترونیکی خلل وارد می کنند و یا آن‌ها را با نودهای جعلی تعویض می کنند[5].

دسترسی مداوم به کانال (فرسودگی): نود مخرب پروتکل دسترسی کانال را به وسیله ی درخواست مداوم مختل می کند،که‌این در نهایت منجر به گرسنگی برای نودهای دیگر در شبکه می‌شود، برای مقابله با این حمله باید از ID شبکه و دیگر اطلاعات مورد نیاز برای پیوستن به شبکه حفاظت شود[2].

حمله RUSH: در شبکه یک نود نیاز دارد که به وسیله پروتکل مسیریابی بسته‌ها را به سمت مقصد هدایت کند برای پیدا کردن بهترین مسیر نود شروع به ارسال بسته ROUTE REQUEST می کند اگر هکر اولین کسی باشد که به بسته ROUTE REQUEST پاسخ می‌دهد آنگاه باعث می‌شود پیام‌ها به مقصد نرسند یا این که پیام‌ها از یک مسیر نامناسب به مقصد برسند که خود منجر به هدر رفتن منابع شبکه می‌شود برای مقابله با این حمله می‌توانیم پیام‌های ROUTE REQUEST را به طور تصادفی ارسال کنیم یا این که از پروتکل RAP1 استفاده کنیم[10].

3. شبیه سازی حملات در شبیه ساز NS2

با استفاده از شبیه ساز شبکه NS2، حملات در شبکه‌های حسگر بی‌سیم می‌تواند شبیه سازی شود. NS2 یک نسخه عینی از شبکه واقعی را ایجاد می کند. NS2 یک شبیه ساز مبتنی بر رویداد زمان است، کد را می‌توان در یک زمان خاص که رویداد خاصی رخ می‌دهد، نوشت و انتقال داده بین نودها و حملات نیز می‌تواند نشان داده شود. این شبیه ساز یکی از محبوب ترین شبیه سازهای منبع باز و همچنین یک ابزار شبیه سازی رایگان است که می‌تواند به صورت آنلاین دردسترس باشد. این شبیه ساز طیف گسترده‌ای از برنامه‌های کاربردی، پروتکل مانند TCP، UDP و بسیاری از پارامترهای شبکه دارد. می‌توان آن را در سیستم عامل‌های مختلف مانند سیستم عامل‌های یونیکس، مک و ویندوز اجرا کرد[11]. حملات مختلف در شبکه مانند Dos، RUSH، sinkhole و حمله Sybil را می‌توان در این شبیه ساز مورد آزمایش قرار داد. این حملات را می‌توان در شبکه‌ایجاد کرد تا از انتقال امن داده‌ها بین نودها اطمینان حاصل پیدا کنیم. پس از اجرای شبیه ساز، فایل trace ایجاد می‌شود که می‌توان ار آن برای رسم گراف استفاده کنیم. شبیه ساز NS2 از سه زبان برنامه نویسی C++، OTcl و TCL استفاده می کند.

[1] Rushing Attack Prevention

ایجاد و تنظیم اتصال بین نودها در شبیه ساز

اولین گام ایجاد نود در شبکه است. هر تعداد نود را می‌توان در شبکه تحت نظارت یک کاربر ایجاد کرد. نودها می‌توانند پویا باشند. کاربر می‌تواند منبع، مقصد و نود مخرب را هر زمان که بخواهد در شبیه ساز اجرا کند. حرکت نودها می‌تواند تولید شود و نودها را می‌توان در مناطق مختلف تقسیم بندی کرد. پس از ایجاد نودها، باید ارتباط بین نودها در شبکه‌ایجاد شود. چندین پروتکل تعریف شده وجود دارد که می‌تواند مورد استفاده قرار گیرد، یعنی TCP و UDP. TCP پروتکل ارتباطی مطمئن است که تأیید پیام ارسالی را از گیرنده دریافت می‌کند. پروتکل UDP می‌تواند زمانی مورد استفاده قرار گیرد که ترافیک زیادی در سیستم وجود داشته باشد.

در زیر چگونگی ایجاد نود در شبیه ساز را نشان می‌دهد. nn تعداد نودهایی که در حال راه اندازی هستند را نشان می‌دهد. حلقه بر اساس تعداد نود تکرار می‌شود که در هر مرحله یک نود ایجاد شده و به آن یک حرکت تصادفی اختصاص داده می‌شود.

```
for{set i 0} {$i<$val(nn)} {incr i}
{set node_($i) [$ns node]
$node_($i) random-motion 1}
```

در زیر نحوه تنظیم اتصال TCP بین نودها را نشان می‌دهد. gpsrtace فایلی است که تمام اتصالات TCP در شبکه را نشان می‌دهد.

```
set gpstrace [open gpstrace.tr w]
set tcp [new Agent/TCP]
$tcp trace rtt_
$tcp trace cwnd_
$tcp attach $gpstrace
```

ابعاد X و ابعاد Y توپوگرافی موجود در سیستم است که ابعاد ناحیه کاندید را در شبیه ساز نشان می‌دهد. محل اولیه نودها را می‌توان در یک مختصات خاص در شبیه ساز تنظیم کرد. در زیر نحوه تنظیم موقعیت گره‌ها را نشان می‌دهد. مختصات X بر روی عدد 20 تنظیم شده است و مختصات Y و Z روی 0 قرار دارند.

```
$node_(1)
setX_20.000000000000
$node_(1) setY_0.000000000000
$node_(1) setX_0.000000000000
```

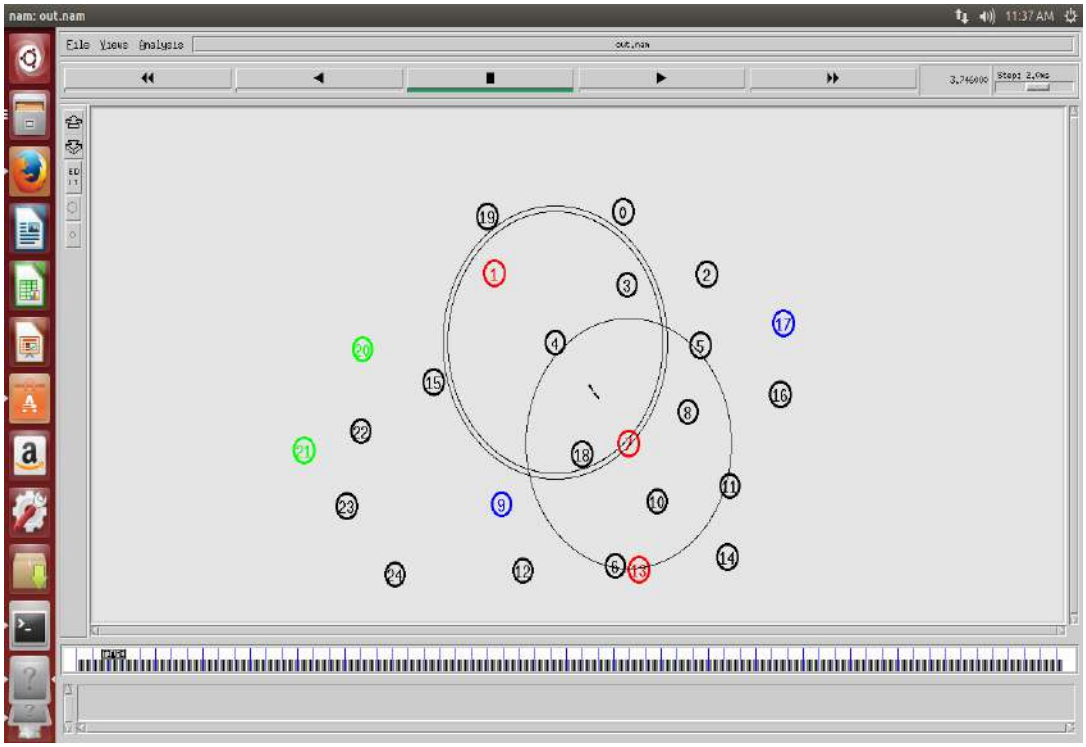
تنظیم گره مخرب: هر یک از نودهای ایجاد شده می‌تواند به عنوان یک نود مخرب عمل کند. در زیر نحوه تنظیم یک نود خاص به عنوان نود مخرب نشان داده شده است.

```
$ns at 50.0 "[$node_ (30) set ragent_] malicious"
```

حمله Sybil: حمله Sybil یکی از خطرناک ترین و مخرب ترین حمله‌ها در WSN است. این حمله که در آن یک نود به عنوان یک نود مخرب عمل می‌کند و هویت چندگانه‌ای را ادعا می‌کند. این حمله را می‌توان با تغییر فایل aodv. cc در محل نصب نرم افزار انجام داد که می‌تواند با حذف بسته‌ها در

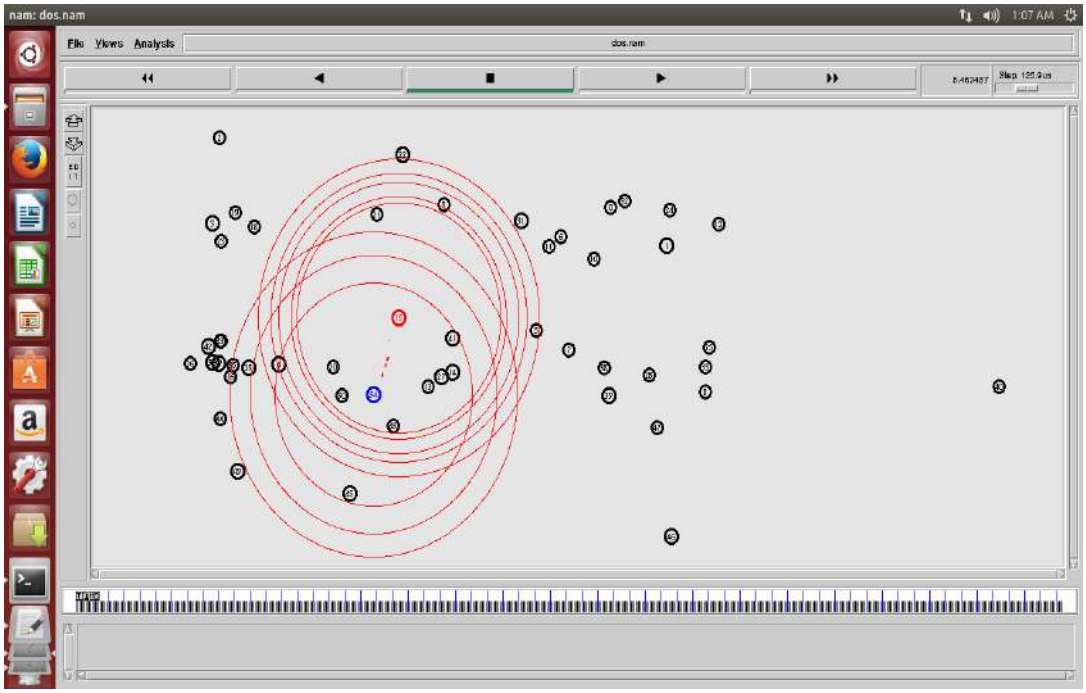
شبیه ساز نشان داده شود. این حمله یکی از حملات مشهور در شبکه‌های حسگر است. شکل 2 شبیه سازی حمله Sybil را نشان می‌دهد، نودهای سبز رنگ (20 و 21)، نودهای فرستنده، نودهای آبی رنگ (9 و 17)، نودهای گیرنده و نودهای قرمز رنگ (1و 7و 13)، نودهای مخرب هستند. در ثانیه ۳ نودهای مخرب بسته‌هایی را که از نودهای فرستنده دریافت می کنند را به نودهای گیرنده ارسال نکرده و آن‌ها را دور می‌ریزند.

شکل2. شبیه سازی حمله Sylib



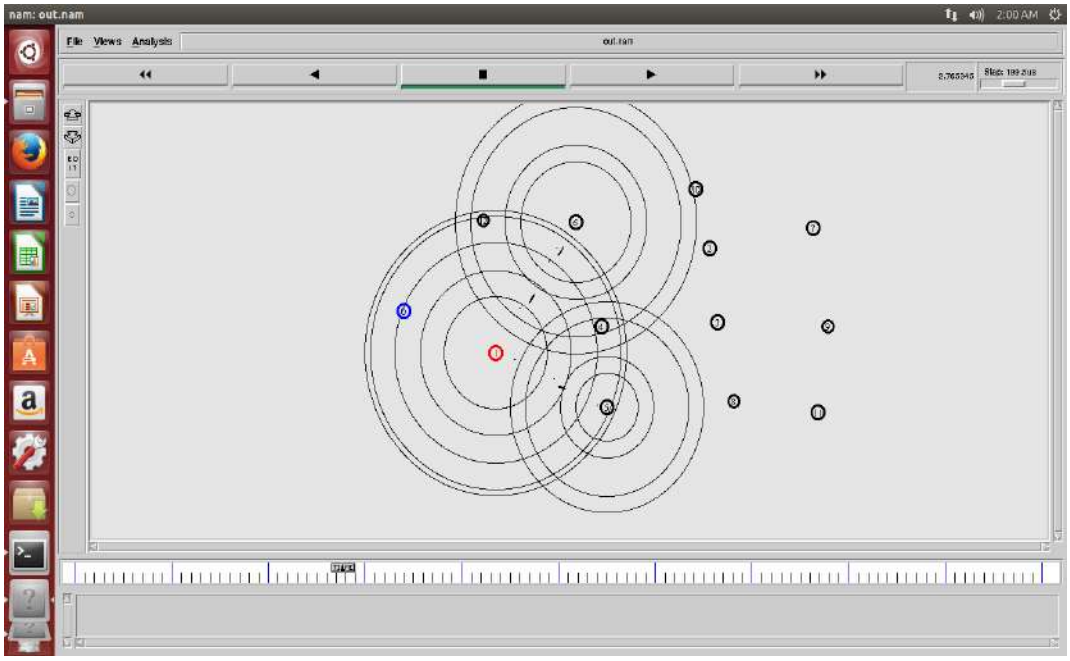
حمله انکار سرویس (DOS): حمله DOS نود هدف را با مقدار زیادی از درخواست ارتباط اشباع می کند که باعث ایجاد ترافیک جعلی می‌شود. این نوع حملات برای سرور سربار ایجاد می کند. در اینجا، حمله DOS به وسیله ی پروتکل UDP و برنامه CBR اجرا می‌شود. هنگامی که بافر پر است، نود هدف بسته‌هایی را که از نودهای مخرب و منبع می گیرد را دور می‌ریزد. شکل 3 شبیه سازی حمله انکار سرویس را نشان می‌دهد. نود قرمز رنگ (15) نود مخرب و نود آبی رنگ (34) نود هدف است در این شبیه ساز بعد از گذشت ۵ ثانیه، نود قرمز رنگ به عنوان نود مخرب عمل کرده و تعداد زیادی از بسته‌ها را به نود هدف ارسال می کند. از آنجا که اندازه بافر نودها محدود است، پس نود هدف نمی‌تواند همه بسته‌ها را اداره کند بنابرین آن‌ها را دور می‌ریزد که‌این امر منجر به از دست رفتن داده‌ها و کاهش سرویس دهی شبکه خواهد شد.

شکل 3. شبیه سازی حمله انکار سرویس



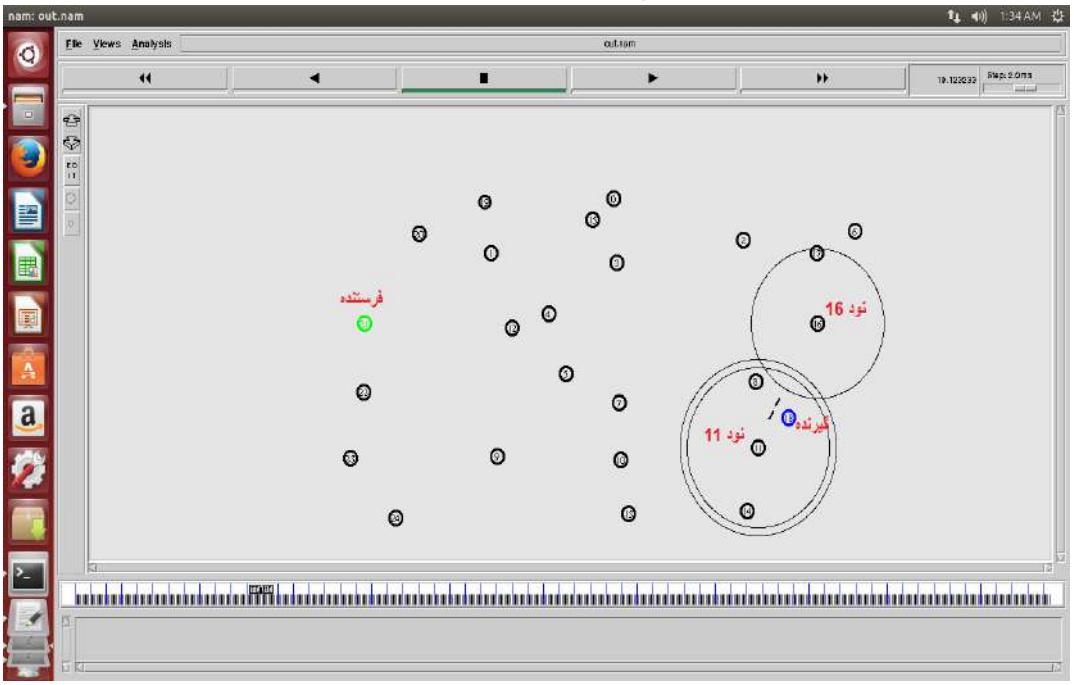
حمله Sinkhole: در این حمله، نود مخرب به نود مقصد نزدیکتر است تا بتواند حداکثر ترافیک احتمالی شبکه را مورد سوء استفاده قرار دهد. این یک حمله پیچیده است و تشخیص آن بسیار دشوار است. در شبیه ساز، نود مخرب در کنار نود مقصد قرار می‌گیرد و همه بسته‌ها را به جای انتقال به نود قانونی دریافت می‌کند. برخی از پروتکل‌های مسیریابی وجود دارند که می‌توانند در یک سطح مشخص در برابر حملات خرابکارانه مقاومت داشته باشند اما بسیاری از آن‌ها در حال حاضر تحت تاثیر حمله Sinkhole قرار دارند. شکل 4 شبیه سازی حمله را نشان می‌دهد. در مرحله اول، نود مخرب (نود قرمز رنگ) تمام اطلاعات مربوط به نودهای همسایه را می‌گیرد سپس نود مخرب به عنوان یک نود قانونی عمل کرده و حداکثر ترافیک ممکن را در شبکه دریافت می‌کند. تمام بسته‌های فرستاده شده از منبع به جای نود مقصد (نود آبی رنگ) به نود مخرب ارسال می‌شود.

شکل4. شبیه سازی حمله Sinkhole



حمله RUSH: حمله RUSH یک نوع از حملات DOS است که در آن بر روی جداول مسیر یابی تأثیر می‌گذارد. این حمله را می‌توان با اصلاح فایل Aodv. h و Aodv. cc در شبیه ساز ns2 ایجاد کرد. این فایل‌ها فایل‌های داخلی هستند که همراه با بسته ی ns2 دانلود می‌شوند. آن‌ها شامل همه کدها و راه حل‌ها در مورد مسیریابی و اطلاعات مورد نیاز برای ارسال بسته هستند. شکل 5 شبیه سازی این حمله را نشان می‌دهد با توجه به شکل نود سبز رنگ(21) نود فرستنده و نود آبی رنگ(18) نود گیرنده هستند. نود فرستنده تحت تأثیر حمله ی RUSH قرار گرفته است و مسیر نامناسبی را برای ارسال پیام به گیرنده برگزیده است. همان طور که در شکل 5 مشخص است بعد از رسیدن پیام به نود 11 به جای فرستادن پیام به نود گیرنده(18) آن را به نود 16 ارسال می کند و سپس نود 16 آن را به گیرنده ارسال می کند بنابرین پیام مسیر طولانی تری را طی می کند که خود باعث هدر رفتن منابع شبکه می‌شود.

شکل 5. شبیه سازی حمله RUSH



در جدول 1 مقایسه ای از حملات شبیه سازی شده انجام شده است. در این مقایسه هر نوع حمله از نظر تهدیدی که به شبکه وارد میکند دسته بندی شده است و در ضمن اثرات زیان بار این حمله نیز مشخص شده است

جدول1: مقایسه حملات شبیه سازی شده

نام حمله	نوع حمله	اثر
Sybol	تهدید به صحت	عدم ارسال بسته ها به مقصد
DOS	تهدید به دسترس پذیری	ارسال زیاد پیام به مقصد در نتیجه آن عدم سرویس دهی مناسب
Sinkhole	تهدید به محرمانگی	حداکثر ترافیک های ارسالی برای سایر نودها را دریافت می کند
Rush	تهدید به دسترس پذیری	هدر دادن منابع شبکه

4. نتیجه گیری

به طور کلی امنیت در شبکه‌های حسگر بی‌سیم به مسائل امنیتی آن وابسته است، مسائل امنیتی در شبکه‌های حسگر باید از ابتدای طراحی سیستم در نظر گرفته شود. هنگام توسعه ی عملکردهای امنیتی باید منابع ظرفیتی نودهای بی‌سیم(حافظه، پردازشگر، منبع انرژی) را نیز مدنظر قرار دهیم. تولیدات درشبکه‌های حسگر بی‌سیم پذیرفته نیست مگر این که امنیت در شبکه را تا حدی اطمینان بخشیم. لازم است که راه حل‌های امنیتی با تمام اهداف امنیتی (اعتماد پذیری داده، جامعیت داده، هویت پذیری و در دسترس پذیری) مطابقت داشته باشد. هنگام توسعه ی راه حل‌های امنیتی باید عوامل مختلفی مثل ویژگی‌های شبکه‌های

حسگر بی‌سیم، اهداف امنیتی، حمله‌ها، الگوریتم‌های رمزنگاری و پروتکل‌های امنیتی را مدنظر قرار داد. در این مقاله حملات مختلفی را در شبیه سازNS2 بررسی کردیم، می‌توانیم به وسیله ی این شبیه ساز، عملکرد و کارایی شبکه را مورد بررسی قرار دهیم علاوه بر این عامل‌هایی که بتوانیم عملکرد شبکه را اندازه بگیریم به وسیله ی شبیه ساز به دست می آید.

5. مراجع

1. Abdul Wahid and Pavan Kumar (2015). ” A Survey on Attacks, Challenges and Security Mechanisms in Wireless Sensor Network”. International Journal for Innovative Research in Science & Technology| Volume 1 | Issue 8 |. ISSN (online): 2349-6010.

2. Muruganandam. A, Bagyalakshmi. P (2014). ” A Study on Threats in Wireless Sensor Networks”. International Journal of Science and Research (IJSR), Volume 3 Issue 3

3. Hemanta Kumar Kalita and Avijit Kar. (2009),“Wireless sensor network security analysis”. International Journal of Next-Generation Networks (IJNGN), Vol. 1, No. 1

4. Rupinder Singh, Dr. Jatinder Singh and Dr. Ravinder Singh (2016). ”security challenges in wireless sensor networks”. International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 6, No3,

5. Vikash Kumar, Anshu Jain and P N Barwal.v, (2014), ” Wireless Sensor Networks: Security Issues, Challenges and Solutions”. International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 8, pp. 859-868.

6. Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi (2014). ” Security Issues and Attacks in Wireless Sensor Network”. World Applied Sciences Journal 30 (10): 1224-1227.

7. Murat Dener(2014). ”Security Analysis in Wireless Sensor Networks”. International Journal of Distributed Sensor Networks Volume 2014, Article ID 303501, 9 pages.

8. Mayur Dhaye, Himangi Pande (2014). ” Security in Wireless Sensor Networks: Issues and Challenges.”, International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 12, ISSN 2348 – 4853.

9. KalsoomShabana, Nigar Fida, Fazlullah Khan, Syed Roohullah Jan, Mujeeb Ur Rehman (2016). ” Security issues and attacks in Wireless Sensor Networks”. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) Volume 5, Issue 7,

10. Furrakh Shahzad, Maruf Pasha, Arslan Ahmad (2016). ” A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures”. International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 12

11. Tejaswi Singh, Aatish Gandotra (2015). ” Replication OF attacks in a wireless sensor network using NS2”. International Journal of Research in Engineering and Technology, Volume: 04 Issue: 10