ISSN: 2745-3673
http://www.Rcsj.ir

مجلـه‌ی علمی پژوهش در علوم رایانه (سال سوم)
شماره ۱۲ / زمستان ۱۳۹۷ / ص ۲۴-۱۷

سیستم تشخیص نفوذ متمرکز مبتنی بر تشخیص ترکیبی در شبکه های حسگر بی سیم خوشه بندی

میترا نجفی اسفتانی [۱] ، غلامحسین اکباتانی فرد [۲]

[۱] دانشجو کارشناسی ارشد مهندسی نرم افزار، موسسه آموزش عالی مهرآستان.

[۲] عضو هیئت علمی گروه کامپیوتر ، موسسه آموزش عالی مهرآستان.

نام نویسنده مسئول:
میترا نجفی اسفتانی

چکیده

شبکه‌های حسگر بی‌سیم ، در معرض انواع تهدیدات مختلف امنیتی قرار می‌گیرند ، که می‌توانند عملکرد این شبکه‌ها را کاهش دهند و باعث شوند حسگرها اطلاعات نادرستی را به گره‌های چاهک بفرستند.پروتکل‌های مسیر امنیتی، معتبر و مدیریت کلید نمی‌توانند امنیت لازم را برای شبکه‌های حسگر بی‌سیم تضمین نمایند. سیستم تشخیص نفوذ راه-حلی را برای غلبه بر این مشکل با کمک تجزیه و تحلیل شبکه به منظور تشخیص رفتارهای غیرعادی گره‌های حسگر فراهم آورده است. ما در این پروژه سعی کردیم یک سیستم تشخیص نفوذ ترکیبی در شبکه‌های حسگر بی‌سیم ارائه کنیم که در آن جهت بهره‌گیری از مزایای سیستم‌های تشخیص سوءاستفاده و سیستم‌های تشخیص ناهنجاری، این دو را با هم ترکیب کرده تا دقت تشخیص در حد سیستم تشخیص سوء استفاده داشته باشد و بتواند نفوذهای جدید را تشخیص دهد و با روش‌های خوشه‌بندی در شبکه و انتخاب گره سرخوشه با بیشترین انرژی به کاهش مصرف انرژی در شبکه کمک خواهیم کرد.

واژگان کلیدی: شبکه‌ی حسگر بی‌سیم، تشخیص نفوذ ترکیبی، تشخیص سوء استفاده، مبتنی بر ناهنجاری، مبتنی بر خوشه بندی.

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۱۲ ، زمستان ۱۳۹۷، ص ۲۴- ۱۷

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

شبکه‌های حسگر بی‌سیم، نسل جدیدی از سیستم‌های تعبیه شده‌ی بلادرنگ با محدودیت محاسباتی، انرژی و حافظه هستند. شبکه های حسگر بی سیم از صدها یا هزاران حسگر تشکیل شده‌اند، که معمولا در محیطی دور از دسترس پخش می‌شوند. وظیفه‌ی اصلی این حسگرها جمع‌آوری اطلاعات از محیط پیرامون و ارسال آن به ایستگاه‌پایه است. ایستگاه‌پایه یک گره‌ی قدرتمند است که دارای قدرت محاسباتی، انرژی و توان و هم‌چنین فضای حافظه‌ی بالاست. هر گره‌ی حسگر از واحد حسگر، واحد محاسباتی، حافظه و واحد ارتباط بی‌سیم با محدوده‌ی محدود تشکیل شده است. حافظه‌ی بالا در ایستگاه‌پایه باعث شده تا این مکان محلی برای ذخیره‌سازی داده‌های به‌دست آمده از محیط اطراف و هم‌چنین کلیدهای رمزنگاری که در حین ارتباطات استفاده می‌شوند، باشد. هم‌چنین قدرت محاسباتی بالا در ایستگاه‌پایه باعث شده تا این مکان بتواند عملیات سنگین‌تری را با توان‌عملیاتی بالاتری انجام دهد و طول عمر بیشتری داشته باشد[۱].

در شبکه‌ی مذکور گره‌های حسگر برای تأمین انرژی خود به باتری‌هایی با توان محدود وابسته هستند. هم‌چنین به‌دلیل به‌کارگیری این نوع شبکه‌ها در محیط‌های خطرناک و دور از دسترس، شارژ کردن یا تعویض منبع انرژی این گره‌ها بسیار سخت یا گاهی غیرممکن است. بنابراین، یکی از چالش‌های اصلی شبکه‌های حسگر بی‌سیم، انرژی محدود گره‌های حسگر است. این شبکه نسبت به شبکه‌های دیگر دارای آسیب‌پذیری بالایی هستند؛ که این امر ناشی از خصوصیات این شبکه‌ها می‌باشد[۲].

بی‌سیم بودن شبکه‌های حسگر باعث می‌شود که حسگرها با امواج رادیویی با هم در تماس باشند که به‌صورت ذاتی امنیت این شبکه-ها را پایین می‌آورد و همین‌طور تحرک و پویایی حسگرها باعث شده که این شبکه‌ها بیشتر در معرض نفوذ مهاجمان باشند؛ زیرا هنگام جابه‌جایی با شبکه‌های دیگر ارتباط برقرار می شود و این ارتباط سطح امنیت شبکه‌های حسگر بی‌سیم را پایین می‌آورد[۱]. کارایی این‌گونه از شبکه‌ها به طول عمر گره‌های حسگر و پوشش شبکه‌ای وابسته است. لذا تلاش برای بهینه کردن مصرف انرژی و مدیریت پویای توان مصرفی گره‌های حسگر بسیار حائز اهمیت است. انتقال اطلاعات درون شبکه‌ای بیشترین مصرف انرژی را در این نوع شبکه به‌خود اختصاص می‌دهد. خوشه‌بندی از راه‌حل‌های رایج کاهش تعداد انتقالات درون شبکه‌ایی است. در خوشه‌بندی، گره‌های حسگر به خوشه‌های متعددی گروه‌بندی می‌شوند و در هر خوشه یک گره به‌عنوان سرخوشه انتخاب می‌شود. وظیفه‌ی سرخوشه دریافت داده از گره‌های دیگر و ارسال آن به ایستگاه‌پایه است. انتخاب سرخوشه‌ی مناسب، به‌صورت چشم‌گیری مصرف انرژی را در این شبکه‌ها کاهش می‌دهد که این کاهش مصرف انرژی منجر به افزایش طول عمر شبکه می‌گردد[۲].

۱-کارهای پیشین

حمله sink hole از طریق الگوریتمی که در [۹] ارائه شد حتی در حضور نودهای تبانی کننده تشخیص داده شد. در قدم اول لیستی از نودهای مشکوک از طریق تخمین ناحیه حمله ارائه می‌کند. نویسنده فرض کرده که ایستگاه مرکزی مکان نودها را می‌داند. به عنوان مثال ایستگاه پایه با کمک مکانیزم‌های محلی سازی مکان نودها را به دست آورده است. ناسازگاری در داده‌ها در ایستگاه مرکزی با روش‌های آماری تشخیص داده می‌شود. ایستگاه پایه مکان sink hole را با دایره‌ایی در منطقه حمله که از نودهای مشکوک تشکیل شده تخمین می-زند. شعاع این دایره باید طوری باشد تا همه نودهای مشکوک را دربرگیرد. در قدم بعدی مهاجک با آنالیز الگوهای مسیریابی در مناطق تحت تأثیر قابل شناسایی است. ایستگاه پایه پیامی درخواستی که ID تمامی نودهای تحت تأثیر(آسیب دیده) در آن است را همه‌پخشی می‌کند. یک شناسه زمانی timestamp هم با کلید خصوصی ایستگاه در پیام درخواست قرار داده می‌شود تا از حمله ارسال دوباره جلوگیری شود. نودهای آسیب دیده با ID خود، ID پرش بعدی و هزینه مسیریابی (به عنوان مثال تعداد پرش) به نود دریافت کننده درخواست پاسخ می‌دهند. پیام پاسخ در مسیر معکوس همه پخشی می‌شود (پرش بعدی و هزینه مسیریابی) توسط یک حمله تحت تأثیر قرار می‌گیرد. ایستگاه پایه با ساخت یک درخت از اطلاعات پرش بعدی می‌تواند الگوهای مسیریابی را تجزیه و تحلیل کند. در حمله sink hole تمامی ترافیک به سمت مقصدی هدایت می‌شود که نشان دهنده هویت نود مهاجم است.

در [۱۰] یک طرح تشخیص نفوذ متمرکز ارائه کرده که از دو ویژگی برای تشخیص حمله ارسال انتخابی و سیاه‌چاله استفاده می‌کند. IDS این مقاله مبتنی بر ماشین بردار پشتیبان و پنجره لغزان است. معماری IDS متمرکز ارائه شده در این مقاله در ایستگاه پایه عمل تشخیص نفوذ را انجام می‌دهد. این مقاله با دقت بالایی دو حمله ارسال انتخابی و سیاه‌چاله را تشخیص می‌دهد.

سیستم تشخیص نفوذ مبتنی بر خوشه‌بندی [۱۱] برای تشخیص حملات مسیریابی در wsn ارائه شده است. عامل IDS در هر گره حسگر با اطلاعات همسایه و قوانین مسیریابی به تشخیص حمله می‌پردازد. در این مقاله هم عامل تشخیص نفوذ محلی وجود دارد و هم عامل تشخیص نفوذ سراسری. ارسال و دیرافت بسته‌ها توسط عامل محلی نظارت می‌شود و لیستی از نودهای مهاجم (لیست سیاه) نگه داری می‌شود. ارتباطات با نودهای همسایه در عامل تشخیص نفوذ سراسری نظارت می‌شود. برای تشخیص ناهنجاری، سربار ارتباطات با

ISSN: 2745-3673
http://www.Rcsj.ir

اطلاعات از پیش تعیین شده و دوپرشی همسایه چک می‌شود. سرخوشه هشدارها را دریافت می‌کند، اگر تعداد هشدارها از یک آستانه مطمئن بالاتر بود، لیست سیاه به روز رسانی شده با این گره جدید به گره‌های حسگر دیگر ارسال می‌شود و نود مهاجم در خوشه را ایزوله می‌کند. این مقاله حملات selective forwarding, sinkhole, hello flood, and wormhole attacks را با کمک قوانین از پیش تعیین شده تشخیص می‌دهد.

در[۱۲] نویسنده ها یک سیستم تشخیص نفوذ چندلایه‌ایی معرفی کردند که معماری آن از تبادلات و همکاری بین سه لایه مجاور شبکه، فیزیکی و mac استفاده می‌کند. ایده اصلی مقاله به این صورت است که بعد از اینکه نود حسگری یک پیام RTS از یک گره مهاجم دریافت کرد، جستجو می‌کند که آیا این گره یک گره همسایگی در مسیرش است یا خیر (با مراجعه به جدول مسیریابی در لایه شبکه). علاوه بر این هویت نود مهاجم با اندازه گیری شاخص توان سیگنال دریافتی RSSI در بسته دریافت شده چک می‌شود (در لایه فیزیکی). بنابراین گره‌هایی که با گره‌های حسگر تبادل پیام RTS و CTS دارند اگر در جدول مسیریابی آن‌ها نباشند، سریعاً به عنوان یک گره مهاجم تشخیص داده می‌شوند.

در [۱۳]یک سیستم تشخیص نفوذ هوشمند در شبکه حسگر بی سیم ارائه شده است. این مقاله دو ایده اصلی دارد. در اولین مرحله هر گره در یک فاصله زمانی هر گره عضوی که متعلق به یک خوشه است ID خودش، تعداد بسته‌های ارسالی و دریافتی‌اش را به سرخوشه ارسال می‌کند. در مرحله بعد سرخوشه چک می‌کند که آیا ID گره تغییر کرده است یا خیر. اگر ID گره‌ایی تغییر کرده، سرخوشه تعداد بسته‌های دریافتی و ارسالی را در آن فاصله زمانی محاسبه می‌کند. سرخوشه تعداد بسته‌های از بین رفته را هم محاسبه می‌کند[۱۴].

در [۱۵] یک سیستم تشخیص نفوذ متمرکز مبتنی بر تشخیص سوء استفاده ارائه شده است. در این مقاله ابتدا شبکه با پروتکل مسیریابی LEACH به خوشه‌هایی تقسیم می‌شود. در این مقاله شبکه به سه سطح طبقه‌بندی می‌شود. سطح پایینی، میانی، بالایی. سطح پایینی از همه گره‌های حسگری تشکیل شده که اطلاعات را از محیط جمع آوری می‌کنند. سطح میانی شامل سرخوشه‌ها می‌شود که اطلاعات را به صورت دوره‌ایی (در آغاز هر دور ارتباط) یک بسته کنترلی به ایستگاه پایه ارسال می‌کنند. ایستگاه پایه نشان دهنده‌ی سومین سطح است که سطوح میانی و پایینی را نظارت می‌کند. این مقاله از یک سیستم تشخیص نفوذ متمرکز مبتنی بر امضای حملات استفاده می‌کند تا حملات ارسال انتخابی و سیاه‌چاله را تشخیص دهد. منظور از سیستم تشخیص نفوذ متمرکز قرار دادن موتور تشخیص در ایستگاه پایه است تا در مصرف باتری گره‌های حسگر صرفه‌جویی شود. در آغاز هر دور ارتباطی سرخوشه‌ها قبل از تجمیع داده بسته کنترلی را به ایستگاه پایه ارسال می‌کنند با یک ارتباط تک پرشه. سیستم تشخیص نفوذ در این مقاله سه فاز جمع آوری داده، کنترل قوانین و تشخیص نفوذ را دارد. در مرحله اول همه گره‌های حسگری که در سطح میانی هستند (سرخوشه) بسته‌های کنترلی را به ایستگاه پایه می‌فرستند. در مرحله بعد امضای قوانین به همه داده‌های دریافتی اعمال می‌شود و در مرحله آخر سیستم تشخیص نفوذ در ایستگاه پایه حمله را تشخیص می‌دهد و یک هشدار با شناسه نود مهاجم در شبکه انتشار می‌دهد.

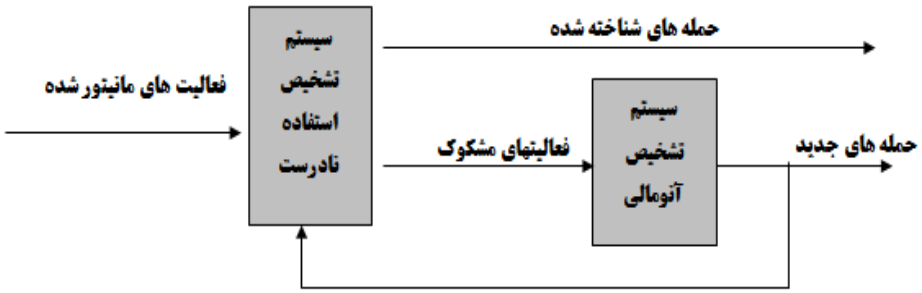
۲-روش پیشنهادی

در این مقاله قصد داریم به این نتیجه برسیم که چگونه می‌توان یک سیستم تشخیص نفوذ ترکیبی در شبکه‌های حسگر بی‌سیم ارائه کرد که در فاز ابتدایی سیستم تشخیص سوء استفاده، حملات شناخته شده را به‌عنوان حملات اصلی شناسایی کند و فعالیت‌های مشکوک را به یک سیستم تشخیص ناهنجاری بدهد تا حمله‌های جدیدی را کشف کند و چگونه حملات جدید به پایگاه‌داده حملات در ایستگاه‌پایه اضافه شود.

همان‌طور که گفته شد، سه نیازمندی اصلی شبکه‌های حسگر بی‌سیم امنیت، انرژی و مقیاس‌پذیری است. برای تأمین امنیت در این شبکه‌ها از یک سیستم تشخیص نفوذ ترکیبی استفاده خواهیم کرد.

۱. سیستم تشخیص نفوذ در ایستگاه‌پایه قرار می‌گیرد.
۲. گره‌های سرخوشه اطلاعات را به ایستگاه‌پایه ارسال می‌کنند(برای صرفه‌جویی در انرژی گره‌های عضو خوشه)
۳. هم گره‌های عضو خوشه و هم سرخوشه می‌توانند مهاجم باشند.

ISSN: 2745-3673
http://www.Rcsj.ir



شکل1-1. سیستم تشخیص نفوذ ترکیبی

برای رفع مشکل محدودیت انرژی و تأمین مقیاس‌پذیری از یک پروتکل مسیریابی خوشه‌بندی کارا استفاده خواهیم نمود.
پیشنهاد ما استفاده از پروتکل لیچ است. لیچ یک پروتکل خوشه‌بندی خود سازمانده است که بار انرژی را بر روی حسگرهای شبکه توزیع می‌کند. در لیچ گره‌ها خودشان را در خوشه‌های محلی سازماندهی می‌کنند، به‌طوری‌که یک گره در خوشه به‌عنوان سرخوشه عمل می‌کند. برای این‌که با تمام شدن انرژی گره‌ی سرخوشه، کل خوشه از کار نیفتد و عمر خوشه تمام نشود، گره‌های با انرژی بالا در خوشه به‌صورت چرخشی و تصادفی سرخوشه می‌شوند.

۲-۱-فاز خوشه بندی

در روش پیشنهادی ما ، انتخاب سرخوشه برای ارسال اطلاعات با توجه به منابع مورد نیازگره ها یعنی انرژی مصرفی صورت گیرد.

انرژی مصرفی برای ارسال یک پیغام lبیتی در مسافت d برابر:

(۱)

$$E_{tx} = \begin{cases} l.E_{elect} + l.\epsilon_{fs}.d^2 & if\ d \le d_0 \\ l.E_{elect} + l.\epsilon_{mp}.d^4 & if\ d > d_0 \end{cases}$$

دراین رابطه E_{elect} انرژی لازم برای فعالسازی مدارات الکتریکی است. ϵ_{fs} و ϵ_{mp} به ترتیب انرژی های لازم برای انتقالیک بیت در مدل فضای باز و مدل چند مسیره هستند.d_0 مقدار آستانه فاصله است:

(۲)

$$d_o = \sqrt{\frac{\epsilon_{fs}}{\epsilon_{mp}}}$$

در روش پیشنهادی ، انتخاب سرخوشه برای ارسال اطلاعات با توجه به منابع مورد نیازگره ها یعنی انرژی مصرفی صورت گیرد. هرگره برای ارسال اطلاعات در پردازنده خود با استفاده از پردازش فازی،با توجه به فاصله مبدا تا مقصد ، مقدار بهینه انرژی مصرفی و نوع تقویت کننده خود از پایگاه قوانین خود را مشخص نموده و از مناسب ترین سر خوشه برای ارسال اطلاعات استفاده می کند.

در نتیجه با جایگذاری متغییر X به جای Єfs و Єmpخواهیم داشت:

$$E_{Tx}(l,d) = L\ .E_{elec} + L\ .X$$

(۳)

که این روش کاهش مصرف انرژی در بین گره های شبکه وکاهش تعداد گره های مرده در طول زمان و افزایش عمر شبکه را در پی خواهد داشت.

۲-۲-فاز تشخیص نفوذ

ما از دو موتور تشخیص نفوذ مبتنی بر امضا و تشخیص ناهنجاری بصورت ترکیبی استفاده نمودیم . با استفاده از ماشین بردار پشتیبانی با دسته بندی رفتارها در دو کلاسه نرمال و غیر نرمال ، داده های غیر نرمال را برچسب گذاری وبه سیستم تشخیص

ISSN: 2745-3673
http://www.Rcsj.ir

نفوذ آموزش می دهیم .سپس با استفاده از مدل یادگیری شده برای داده های تست استفاده می کنیم.اما متنوع بودن حمله ها و حجم زیاد داده ها آنالیز و کشف حمله های جدید را با مشکل روبرو می کند . برای حل این مشکل قبل از انجام آموزش ، داده ها توسط روش مینیمم- ماکزیمم بردار پشتیبان نرمالیزه شود.وقتی داده های مورد بررسی را توسط روشهای نرمال سازی به شکل ساده تری تبدیل نماییم ، می توان کارایی روش را بهبود نیز داد. در این روش داده ها از فضای قبلی به فضای جدید توسط تبدیل خطی زیر انتقال داده می شوند.

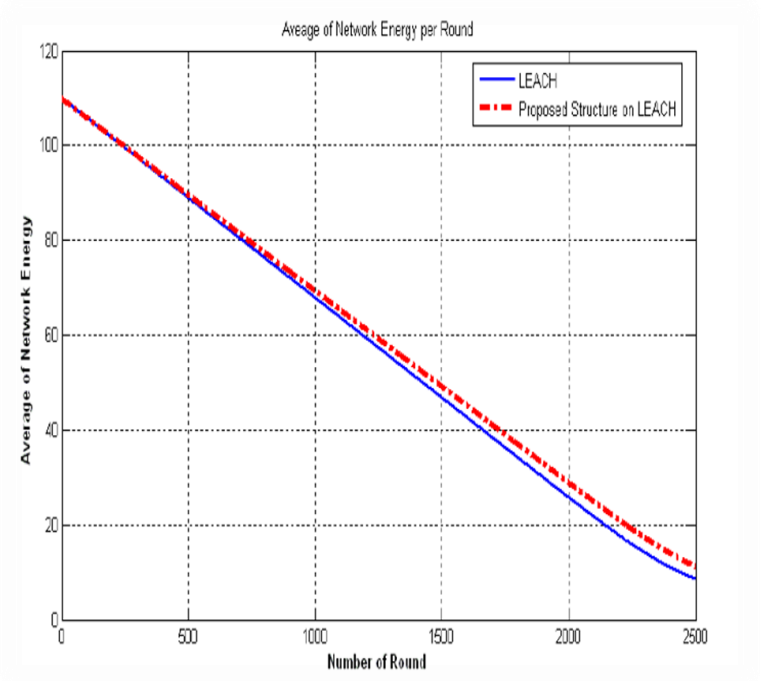
$$Xi = Newmin + (Newmax - Newmin) * (\frac{Xi - Xmin}{Xmax - Xmin})$$

جدول۱-مقایسه نرخ تشخیص

روش SVM	نرخ تشخیص
بدون نرمال سازی	98/31%
نرمال سازی	98/35%

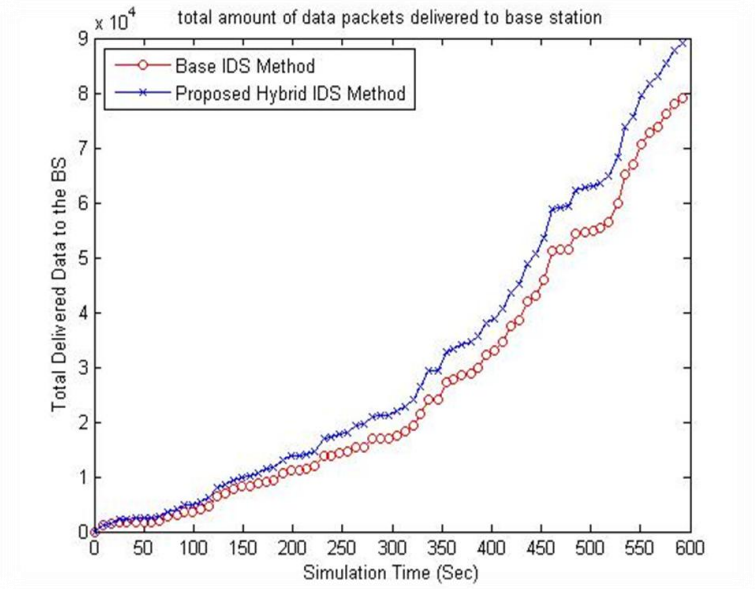
۳-شبیه سازی

نمودار زیر میانگین انرژی مصرفی شبکه را نشان می دهد که همان طور که مشاهده می نمایید الگوریتم پیشنهادی نسبت به الگوریتم لیچ در مصرف انرژی کارآمد تر است.

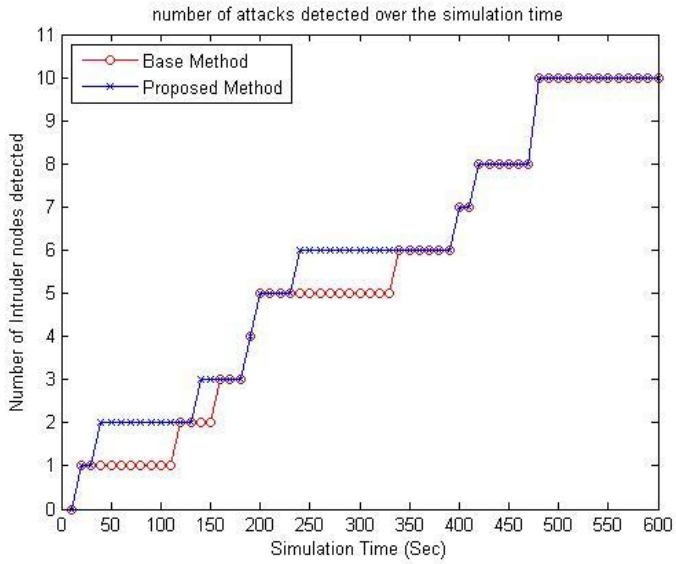


نمودار۱ -میانگین انرژی مصرفی شبکه

ISSN: 2745-3673
http://www.Rcsj.ir



نمودار۲-تعداد داده های ارسالی به ایستگاه پایه



نمودار ۳-تعداد گره های مهاجم شناسایی شده

ISSN: 2745-3673
http://www.Rcsj.ir

نتیجه گیری

یک الگوریتم تشخیص نفوذ ترکیبی ارائه دادیم که مبتنی بر الگوریتم خوشه بندی لیچ و تشخیص ترکیبی دو روش مبتنی بر امضاء و تشخیص ناهنجاری است که هم از نظر مصرف انرژی بهینه می باشد و هم نرخ تشخیص نفوذ بالایی دارد. این سیستم ترکیبی می تواند راه حل مناسبی برای کاهش نرخ مثبت نادرست باشد. نتایج نشان می دهد که روش ارائه شده ، یک الگوریتم کارا برای تشخیص نفوذ با نرخ تحویل بسته بالا است که میانگین انرژی باقی مانده در آن بالا و تعداد بسته های گم شده پایین می باشد.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] Brian Caswell, Jay Beale, and Andrew R Baker, “Snort IDS and IPS Toolkit”, Syngress,Publishing, 2007.
[2] Ronald L. Krutz, “Securing SCADA Systems”, Wiley, 2005.
[3] Paul Innella and Oba McMillan, “An Introduction to Intrusion Detection Systems”, 2001.
[4] Brian Caswell, Jay Beale, and Andrew R Baker, “Snort IDS and IPS Toolkit”, Syngress
[5] Publishing, 2007.
[6] Rebecca Gurley Bace ،“Intrusion Detection” ،Macmillan Technical Publishing, 2000
[7] Christopher Krugel, Thomas Toth, “Applying Mobile Agent Technology to Intrusion Detection”, Technical University Vienna, 2000
[8] Mats Person ،“Mobile Agent Architectures” ،Defense Research Establishment, 2000
[9] Jose Durate ،Luiz Fernando ،“Micael: An Autonomous Mobile Agent System to Protect New Generation Networked Applications” ،URFJ – Rio de Janeiro, 2001
[10] Ramana, K.V., Basha, K., Neural Image Recognition System with Application to Tuberculosis Detection,IEEE proceeding of International Conference of Information Technology,2004
[11] Noria Foukia ،“Intrusion Detection with Mobile Agent” ،University of Geneva, 2001
[12] D. Niculescu, B. Nath, ”Ad Hoc Positioning System (APS)”, IEEE Global Telecommunications Conference 2001, Vol. 5 , pp. 2926-2931, November 2001.
[13] Christopher Krugel ،Thomas Toth, “Sparta, A Mobile Agent based Intrusion Detection System” ،Technical University Vienna, 2000
[14] Christopher Krugel ،Thomas Toth, “Flexible, Mobile Agent Based Intrusion Detection for Dynamic Networks”،Technical University Vienna, 2001
[15] B. M. J. Yick, and D.Ghosal, "Wireless sensor network survey," Computer networks, 2008.
[16] G. Bontempi and Y. Le Borgne, “An adaptive modular approach to the mining of sensor network data”, Workshop on Data Mining in Sensor Networks, SIAM SDM, Newport Beach, CA, USA, April 2005.
[17] T. H. Hai, Huh, E. N., & Jo, M, "A lightweight intrusion detection framework for wireless sensor networks," Wireless Communications and Mobile Computing, vol. 10, pp. 35–52, 2010.
[18] D. Boubiche, & Bilami, A," Cross layer intrusion detection system for wireless sensor network,"International Journal of Network Security & Its Applications, vol. 4, pp. 35–52, 2012.
[19] A. R. Sardar, Sahoo, R. R., Singh, M., Sarkar, S., Singh, J. K., & Majumder, K, "Intelligent intrusion detection system in wireless sensor network," in In Proceedings of the 3rd international conference on frontiers of intelligent computing: theory and applications, 2014.
[20] N. A. Alrajeh, & Lloret, J., " Intrusion detection systems based on artificial intelligence techniques in wireless sensor networks," International Journal of Distributed Sensor Networks,2013.
[21] F. Hidoussi, H. Toral-Cruz, D. E. Boubiche, K. Lakhtaria, A. Mihovska, and M. Voznak,"Centralized IDS Based on Misuse Detection for Cluster-Based Wireless Sensors Networks,"Wireless Personal Communications, vol. 85, pp. 207-224, 2015.
[22] S.kaplantzis, A.Shilton,N.Mani,”detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines”IEEE,1-4244-1502,2007