
بسم الله الرحمن الرحيم

دانشگاه گیلان

دانشکده‌ی پردیس بین‌الملل (انزلی)

پایان‌نامه‌ی کارشناسی ارشد

در رشته‌ی مهندسی فناوری اطلاعات – گرایش تجارت الکترونیک

طراحی سطح بالای یک سیستم تشخیص نفوذ مبتنی بر عامل و سیاست، با قابلیت پیکربندی مجدّد دینامیک برای شبکه‌های حسگر بی‌سیم

از

حسین جدیدالاسلامی

استاد راهنما

دکتر شهریار محمدی

خرداد ۱۳۹۰

دانشکده‌ی پردیس بین‌الملل (انزلی)

گروه مهندسی فناوری اطلاعات

گرایش تجارت الکترونیک

طراحی سطح بالای یک سیستم تشخیص نفوذ مبتنی بر عامل و سیاست، با قابلیت پیکربندی مجدّد دینامیک برای شبکه‌های حسگر بی‌سیم

از

حسین جدیدالاسلامی

استاد راهنما

دکتر شهریار محمدی

استاد مشاور

دکتر رضا ابراهیمی آتانی

خرداد ۱۳۹۰

تقدیم به:

یوسف گمگشته‌ی زهرا (عج)

تشکّر و قدردانی:

با سپاس فراوان از زحمات بی‌دریغ اساتید گرامی دکتر شهریار محمدی و دکتر رضا ابراهیمی آتانی، که اینجانب را در انجام این پژوهش یاری نموده‌اند.

فهرست مطالب

فهرست جدول‌ها

فهرست شکل‌ها

چکیده

طراحی سطح بالای‌یک سیستم تشخیص نفوذ مبتنی بر عامل و سیاست، با قابلیت پیکربندی مجدّد دینامیک برای شبکه‌های حسگر بی‌سیم

حسین جدیدالاسلامی

شبکه‌های حسگر بی‌سیم، شبکه‌هایی متشکّل از تعداد زیادی نود حسگر با تراکم بالا، کاربردهای متنوّع در حوزه‌های نظارت و ردیابی، منابع محدود و بدون زیرساخت هستند. این شبکه‌ها به دلایلی مانند کانال ارتباطی ناامن و ارتباطات بی‌سیم، مشکلات امنیتی فراوانی دارند. بنابراین، تأمین امنیت یک نیازمندی حیاتی برای این شبکه‌ها است.

از سوی دیگر، جهت مواجهه‌ی با انواع نفوذها در حوزه‌ی امنیت اطلاعات، مکانیزم‌های امنیتی فراوانی ایجاد شده‌اند؛ یکی از مهم‌ترین این ابزارها، سیستم تشخیص نفوذ می‌باشد. سیستم تشخیص نفوذ، سیستمی نرم‌افزاری یا سخت‌افزاری است که می‌تواند بر ترافیک محیط عملیاتی مورد نظر نظارت کند، آن را تحلیل نموده و حملات را کشف نماید. بنابراین، می‌توان با بهره‌گیری از سیستم‌های تشخیص نفوذ در حوزه‌ی شبکه‌های حسگر بی‌سیم، سطح امنیت را در این شبکه‌ها افزایش داد. در این زمینه تحقیقاتی انجام شده است که غالباً ناقص و خاص-منظوره هستند و عملاً اثری از تحقیق جامعی در این حوزه دیده نمی‌شود.

این تحقیق بر آن است که با توجه به ادبیات موضوع و تحقیقات انجام شده، به بررسی موضوع حیاتی امنیت و حل مسأله‌ی تشخیص نفوذ در شبکه‌های حسگر بی‌سیم، البته با دیدی جامع و دقیق بپردازد. بدین منظور با بررسی ابعاد مختلف سیستم‌های تشخیص نفوذ، شبکه‌های حسگر بی‌سیم و امنیت در این شبکه‌ها، ۳ پیشنهاد ارائه نموده است: نخست، بکارگیری یک معماری تشخیص نفوذ سلسله‌مراتبی، خوشه‌بندی، توزیعی، استاتیک و ناهمگن؛ دوم، بکارگیری پروتکل مسیریابی سلسله‌مراتبی LEACH، البته با تغییرات اندک؛ سوم، بهره‌گیری از دو نوع سیستم تشخیص نفوذ به نام‌های سیستم تشخیص نفوذ مبتنی بر سرخوشه ، مستقرّ بر سرخوشه‌ها و سیستم تشخیص نفوذ مبتنی بر سطح کل شبکه‌ی حسگر بی‌سیم ، مستقرّ بر روی سرور مدیریت مرکزی. بنابراین هدف این پایان‌نامه استقرار همه‌ی انواع سیستم‌های تشخیص نفوذ در قالب یک راه‌حل جامع و یکپارچه، به عنوان یک لایه‌ی دفاعی-امنیتی جدید و افزودن آن به زیرساخت امنیتی شبکه‌های حسگر بی‌سیم می‌باشد.

کلید واژه: شبکه‌ی حسگر بی‌سیم، امنیت، تشخیص نفوذ، سیستم تشخیص نفوذ، حمله، دینامیک، مسیریابی، عامل، سیاست، تشخیص، پاسخ، ردیابی.

فصل ۱:

کلیات تحقیق

۱-۱- مقدّمه

پیشرفت‌ها در ارتباطات بی‌سیم، ایجاد و توسعه‌ی شبکه‌های حسگر بی‌سیم ارزان[1] و با توان مصرفی پایین (منابع محدود)[2] را ممکن ساخته است. شبکه‌های حسگر بی‌سیم (WSNs)[3] سیستم‌هایی همگن یا ناهمگن متشکّل از تعداد زیادی ابزار کوچک، به نام نودهای حسگر، هستند که محیط‌های مختلف را به صورت مشارکتی نظارت می‌کنند؛ یعنی نودهای حسگر علاوه بر عملکرد مستقلّ و خودمختار، با همدیگر همکاری می‌کنند و برای رسیدن به یک دید سراسری و جامع از محیط عملیاتی، داده‌های محلی‌شان را ترکیب می‌نمایند [۱و۲]. در شبکه‌های حسگر بی‌سیم علاوه بر نودهای حسگر، دو مؤلفه‌ی مهم دیگر به نام‌های "نقاط تجمّع"[4] (معادل سرخوشه‌ها و محل استقرار CIDSها) و "ایستگاه پایه"[5] (معادل سرور مرکزی و محل استقرار WSNIDS) هم وجود دارند، که در مقایسه با حسگرهای معمولی منابع قوی تری دارند. نقاط تجمّع اطلاعات را از حسگرهای اطراف‌شان جمع‌آوری می‌کنند، آن‌ها را مجتمع (خلاصه سازی)[6] کرده و سپس به ایستگاه‌های پایه برای پردازش‌های بعدی ارسال می‌کنند (مطابق شکل (۱-۱)) [۱-۳]. عواملی مانند ماهیّت مشترک، بی‌سیم، حفاظت نشده و ناامن کانال ارتباطی، رسانه‌ی انتقال غیرقابل اعتماد و همگانی، استقرار در محیط‌های باز و خطرناک، عملکرد خودکار و بی مراقب و منابع محدود، شبکه‌های حسگر بی‌سیم را برای انواع حملات مستعد و آسیب‌پذیر می‌سازد [۱و۴]؛ به علاوه، شبکه‌های حسگر بی‌سیم، علی‌رغم داشتن کاربردهای بسیار زیاد و متنوّع (در حوزه‌های نظارت و ردیابی)، با ریسک‌های بزرگی مواجه اند؛ از جمله از دست دادن اطلاعات، سرویس‌ها و کنترل شبکه؛ بنابراین امنیت یک نیازمندی حیاتی برای این شبکه‌ها است. با توجه به این که استفاده از اکثر تکنیک‌های امنیتی شبکه‌های سنّتی، در این نوع از شبکه‌ها غیرممکن است [۲و۳]؛ بنابراین مکانیزم‌های امنیتی-دفاعی که بتوانند عملیات متداول این شبکه‌ها را تضمین کنند، باید متناسب با مکانیزم‌های خودمختار و مستقلّ درون خود این نوع شبکه‌ها باشند. این پژوهش در جستجوی مکانیزم امنیتی کاملی برای تأمین ارکان اساسی امنیت شامل محرمانگی ،یکپارچگی، دسترس پذیری [7] و احراز هویّت[8]، البته با توجه به محدودیت‌ها و موانع موجود در این شبکه‌ها، می‌باشد. در حال حاضر تحقیق برای ارائه‌ی راه‌حل‌های امنیتی برای شبکه‌های حسگر بی‌سیم عمدتاً در ۳ دسته‌ی مدیریت کلید (برقراری کلیدهای رمزنگاری بین نودها برای فراهم کردن رمزنگاری و احراز هوّیت)، احراز هوّیت و مسیریابی امن (پروتکل‌هایی

[1] Low-cost
[2] Low-power
[3] Wireless Sensor Networks
[4] Aggregation points
[5] Base-station
[6] Aggregate
[7] Availability
[8] Authenticity

برای محافظت اطلاعات از افشاء غیرمجاز و تحویل کامل و درست آن‌ها به ایستگاه پایه) و خدمات امن (محلی کردن، تجمّع و همزمان سازی امن) متمرکز است [۱و۵]. همه‌ی پروتکل‌های امنیتی ارائه شده تاکنون، متّکی بر فرضیات ویژه‌ای در باره‌ی ماهیّت حملات هستند. بنابراین، با توجه به محدودیت‌های مختلف شبکه‌های حسگر بی‌سیم، لازم است که یک خط دفاعی دیگر به زیرساخت امنیتی این شبکه‌ها افزوده گردد؛ پیشنهاد ارائه شده افزودن‌یک لایه‌ی دفاعی-امنیتی دیگر به نام سیستم تشخیص نفوذ می‌باشد؛ که می‌تواند تلاش‌های مربوط به ایجاد ناامنی و ورود غیرمجاز را کشف کند و هنگام رخداد حملات، حتّی حملات جدید (آنومالی‌ها)، هشدار داده و اقدامات لازم و عمدتاً از قبل تعیین شده را اجرا نماید.

توجه داشته باشید که رویکرد پیشنهادی روش‌های تشخیص، معماری‌ها، روش‌های تصمیم‌گیری و پاسخ‌دهی موجود را توسعه داده و مجتمع می‌کند. هم‌چنین، با اتّخاذ یک رویکرد مبتنی بر عامل و سیاست برای مشاهده‌ی ترافیک، با فرآیند تشخیص چندعامله برای کشف کردن حملات با نرخ خطای پایین‌تر بطور تطبیقی، و فراهم کردن‌یک لایه‌ی تحلیل ضمنی کارآ برای کاربر همراه است؛ لایه‌ی تحلیل تصمیمات کاربر را در باره‌ی آنومالی‌های کشف شده، با ارائه دادن اطلاعات اضافی از منابع داده‌ای مرتبط، پشتیبانی می‌کند و مسئول بصری‌سازی و تجسّم آنومالی‌ها و وضعیت لایه‌ی تشخیص[1] نیز می‌باشد. سیستم تشخیص نفوذ پیشنهادی مبتنی بر تحلیل پیام‌های داده‌ای استماع شده، رویدادهای[2] کشف شده (توسط سرخوشه‌ها و سرور مرکزی) و استنتاج رفتار شبکه می‌باشد. مهم‌ترین محورهای پژوهشی این پایان‌نامه عبارتند از:

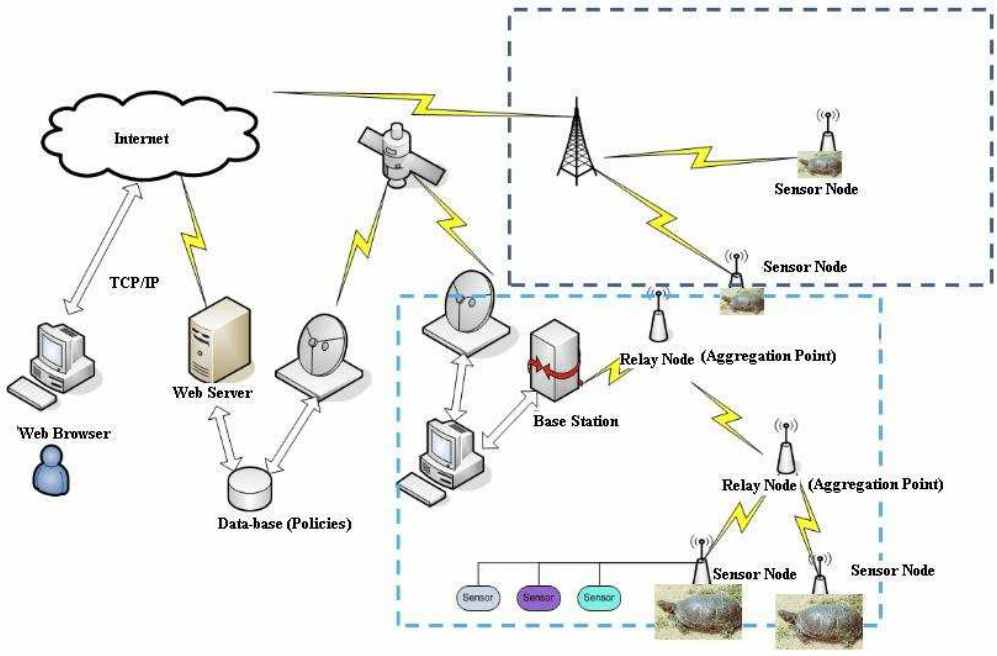
- معرفی شبکه‌های حسگر بی‌سیم
- امنیت در شبکه‌های حسگر بی‌سیم و ارائه‌ی دیدی کلی از انواع حملات در این شبکه‌ها و مقایسه‌ی آن‌ها بایکدیگر از ابعاد مختلف
- بررسی سیستم‌های تشخیص نفوذ و ابعاد مختلف آن‌ها
- بررسی تشخیص نفوذ در شبکه‌های حسگر بی‌سیم
- پیشنهادیک مدل جامع، سلسله‌مراتبی و توزیع‌شده‌ی تشخیص نفوذ و معماری مؤلفه-محور سیستم تشخیص نفوذ مبتنی بر عامل و سیاست در شبکه‌های حسگر بی‌سیم

در این پایان‌نامه به تعریف نیازمندی‌ها، بررسی طرح‌های ممکن و پیشنهاد یک معماری مؤلفه-محور مناسب و اختصاصی برای تشخیص نفوذ و هم‌چنین معماری برای سیستم تشخیص نفوذ در WSNها خواهیم پرداخت. به علاوه، این پژوهش ما را قادر می‌سازد تا با چالش‌های امنیتی موجود در شبکه‌های حسگر بی‌سیم، اهداف و توانایی‌های مهاجمان آشنا شویم؛ هم‌چنین روش‌ها، آثار و نتایج حملات بر روی شبکه‌های حسگر بی‌سیم را شناسایی نماییم، و بتوانیم با افزودن‌یک لایه‌ی امنیتی-دفاعی جدید، به نام سیستم تشخیص نفوذ، به زیرساخت امنیتی این شبکه‌ها، مشکل تشخیص نفوذ در این شبکه‌ها را تا حدودی

[1] Detection Layer Status
[2] Events

مرتفع نماییم؛ در نتیجه، حملات را کشف و مدیریت کنیم و متناسب با نوع و ماهیّت حملات به آن‌ها واکنش به موقع و متناسب نشان دهیم.

خلاصه این که، این پژوهش بر امنیت شبکه‌های حسگر بی‌سیم متمرکز است و می‌خواهد مشکل تشخیص نفوذ در شبکه‌های حسگر بی‌سیم را مرتفع نماید. در نتیجه برای رسیدن به این هدف، این پژوهش شبکه‌های حسگر بی‌سیم، ابعاد مختلف آن‌ها و انواع حملات ممکن در این حوزه را بررسی کرده است؛ به علاوه، اهداف و توانایی‌های مهاجمان را شناسایی کرده و با آثار و نتایج حملات بر روی شبکه‌های حسگر بی‌سیم آشنا شده است. هم‌چنین، به بررسی ابعاد مختلف سیستم‌های تشخیص نفوذ و معماری‌های پایه‌ی این سیستم‌ها، هم‌چنین به بررسی معماری‌های دو نمونه سیستم تشخیص نفوذ (به نام‌های OSSEC و SNORT)، پرداخته است و در انتها، یک معماری تشخیص نفوذ و معماری سیستم تشخیص نفوذ متناسب با نیازها، خصوصیات و محدودیت‌های خاص این شبکه‌ها ارائه نموده است (به نام WSNIDS).



شکل ۱-۱: معماری ارتباطی شبکه‌های حسگر بی‌سیم

۱-۲- تعریف موضوع

مشکلی که امروزه با آن مواجه هستیم، حفاظت شبکه‌های‌مان در برابر انواع حملات می‌باشد. این مشکل در حوزه‌ی شبکه‌های حسگر بی‌سیم با توجه به کاربردهای فراوان و عمدتاً امنیتی-اطلاعاتی و خصوصیات ویژه‌ی این شبکه‌ها، از اهمیت بیشتری برخوردار است. تاکنون برای حفاظت از این شبکه‌ها در برابر انواع نفوذها، معماری‌ها و مدل‌هایی ارائه شده‌اند؛ امّا هیچ‌یک از

آن‌ها دیدی جامع و کلی به این مسأله نداشته‌اند و عمدتاً تک‌بعدی و خاص‌منظوره (مثلاً برای یک نوع حمله‌ی خاص) طراحی و پیاده‌سازی شده‌اند؛ امّا طرح پیشنهادی در این پایان‌نامه با دیدی جامع و همه‌منظوره و با در نظر گرفتن ابعاد و خصایص مختلف شبکه‌های حسگر بی‌سیم،یک معماری جامع و کامل برای حل مشکل تشخیص نفوذ در این شبکه‌ها ارائه می‌نماید. خصیصه‌ی اصلی این معماری آن است که در ۱یا ۲ سطح، با توجه به حوزه‌ی کاربردی و نیاز امنیتی در آن حوزه، طراحی شده است و قابل پیاده‌سازی می‌باشد. تمرکز این پایان‌نامه بر ایجاد و استقرار CIDS[1]ها بر روی سرخوشه‌ها[2] (سیستم تشخیص نفوذ مبتنی بر سرخوشه) و WSNIDS[3] (سیستم تشخیص نفوذ شبکه‌های حسگر بی‌سیم) بر روی سرور مرکزی یا سینک می‌باشد (بنابراین، مسأله‌ی مورد بحث در این پایان‌نامه عبارت است از: تشخیص نفوذ در شبکه‌های حسگر بی‌سیم).

۱-۳- کارهای پیشین (تجربیات گذشته)[4]

تشخیص نفوذ یک مبحث مهم در ناحیه‌ی وسیع امنیت کامپیوتر، و بطور خاص امنیت شبکه است [۶۵و۶۶] که به عنوان موضوعی مهم در شبکه‌های حسگر بی‌سیم از حساسیت و تأثیر ویژه‌ای برخوردار است. قاعده‌ی اصلی چگونگی کشف آنومالی‌های شبکه، خصوصاً بدون هیچ بازخوردی از میزبان‌های تحت تأثیر قرار گرفته، تحلیل الگوها در داده‌های شبکه و مقایسه کردن آن‌ها با داده‌های معمول است؛ سرانجام استنتاج رابطه‌های نامنظم مربوط به پروفایل یک حمله شناخته می‌شود. این رویکرد برای تشخیص نفوذ شبکه، عموماً مبتنی بر جریان اطلاعات می‌باشد. بسیاری از سیستم‌های موجود، مبتنی بر تحلیل حجم ترافیک مدلسازی شده توسط متدهای اصلی تحلیل مؤلفه،یا فقط تعداد جریان‌های متناظر با معیارهای منتخب، هر یک چشم انداز معتبر خاصی در باره‌ی ترافیک شبکه ارائه می‌دهد. تاکنون راه‌حل‌های زیادی برای شبکه‌های سنّتی پیشنهاد شده‌اند، امّا محدودیت‌های منابع شبکه‌ی حسگر بی‌سیم باعث می‌شود که آن راه‌حل‌ها برای این شبکه‌ها قابل استفاده نباشد[5] [۳و۷].

در میان انواع مختلف شبکه‌ها، شبکه‌های ادهاک تشابهاتی با شبکه‌های حسگر بی‌سیم دارند. این شبکه‌ها نیز محدودیت‌های شدید منابع دارند، هر چند که مانند شبکه‌های حسگر بی‌سیم محدودکننده نیستند. در تشخیص نفوذ برای شبکه‌های ادهاک

---

[1] Cluster-based Intrusion Detection System

[2] در شبکه‌های حسگر بی‌سیم معمولاً فرض بر آن است که سرخوشه‌ها (دقیقاً)یکی از همان نودهای معمولی حسگر در هریک از خوشه‌ها هستند؛ امّا در معماری تشخیص نفوذ پیشنهادی ما برای شبکه‌های حسگر بی‌سیم، فرض بر آن است که‌یک سیستم میزبان مجزّا تحت عنوان سرخوشه با امکانات و قابلیت‌های بالاتری نسبت به حسگرهای معمولی برای استقرار CIDS در هر خوشه وجود دارد (مانند PCیا Laptop)؛ بنابراین این سیستم‌ها به عنوان سرخوشه در نظر گرفته می شوند، که در این صورت حتّی می توان خوشه‌ها را ثابت/استاتیک در نظر گرفت و آن سیستم‌میزبان CIDS را به عنوان سرخوشه انتخاب نمود (شبکه‌ی ناهمگن).

[3] Wireless Sensor Network Intrusion Detection System

[4] Related work

[5] In-viable