امنیت در شبکه‌های حسگر بی‌سیم

Security in Wireless Sensor Networks

نویسندگان:

جورج سیلوانوس اورکو

(سازمان توسعه تحقیقات صنعتی، دارالسلام، تانزانیا)

تامارا بازینیوک

(شرکت مدیریت انرژی خاور دور، ولادی‌وستوک، روسیه)

مترجمین:

سید رضا نبوی

(باشگاه پژوهشگران جوان و نخبگان)

مهدی نجفی

(عضو هیأت علمی دانشگاه فنی و حرفه‌ای)

NAGHOOS
PUBLICATION

سرشناسه : اورکو ، جورج اس.
Oreku, George S
عنوان و نام پدیدآور : امنیت در شبکه های حسگر بی سیم/نویسندگان جورج سیلوانوس اورکو ، تامارا پازینیوک ؛ مترجمین سید رضا نبوی ، مهدی نجفی
مشخصات نشر : تهران: انتشارات ناقوس، ۱۴۰۰.
مشخصات ظاهری : ۱۳۴ ص.: مصور .
شابک : 978-600-473-382-3
وضعیت فهرست‌نویسی : فیپا
یادداشت : عنوان اصلی : Security in Wireless Sensor Networs,2016
موضوع : شبکه های حسگر بی سیم— تدابیر ایمنی
موضوع : Wireless Sensor Networs —Security Measures
موضوع : شبکه های حسگر بی سیم
موضوع : Wireless Sensor Networs
شناسه افزوده : پازینیوک، تامارا Pazynyuk , Tamara
شناسه افزوده : نبوی ، سید رضا ،۱۳۷۲- ، مترجم
شناسه افزوده : نجفی ، مهدی ، ۱۳۴۶ - ، مترجم
رده بندی کنگره : TK۷۸۷۲
رده بندی دیویی : ۰۰۳/۶۸۲۲
شمارهٔ کتابشناسی ملی : ۷۶۰۱۹۶۷

NAGHOOS PUBLICATION
انتشارات ناقوس

نام کتاب : امنیت در شبکه های حسگر بی سیم
ناشر : انتشارات ناقوس
نویسندگان : جورج سیلوانوس اورکو ، تامارا پازینیوک
مترجمین : سید رضا نبوی ، مهدی نجفی
چاپ اول : ۱۴۰۰
تیراژ : ۵۰۰جلد
چاپ و صحافی : ناژو
ناظر چاپ : یاسمن تجلی محدث
قیمت : ۳۵۰،۰۰۰ ریال
شابک : ۹۷۸-۶۰۰-۴۷۳-۳۸۲-۳
ISBN : 978-600-473-382-3

انتشارات ناقوس
بلوار کشاورز- خیابان ۱۶آذر- کوچه پارسی - پلاک ۱۰
تلفاکس : ۶۶۴۷۸۹۵۱ - ۶۶۴۷۸۹۵۴

پیشگفتار

شبکه حسگر بی‌سیم (WSN) در مراکز دانشگاهی و صنعتی بسیار مورد توجه است. این فناوری کاربردهای نظامی، صنعتی، علمی، غیرنظامی و تجاری زیادی دارد. با فناوری این شبکه‌ها می‌توان در کاربردهایی که نظارت انسانی یا حسگرهای سنتی غیر منطقی، ناکارآمد، پرهزینه یا خطرناک است، سنجش را با هزینه کمتری انجام داد. انرژی و ظرفیت محاسباتی حسگرهای بی‌سیم محدود است. به همین دلیل استفاده از روش‌های امنیتی سنتی برای آنها، مشکل یا غیر ممکن است. این حسگرها به‌طور معمول در فضای باز استفاده می‌شوند که در معرض حملات فیزیکی مانند پارازیت یا به دست آوردن و دستکاری گره است.

تهدیدات پیش‌روی شبکه حسگر بی‌سیم و سازماندهی شبکه حسگر بی‌سیم در برابر این تهدیدات، تحت تأثیر مستقیم کاربرد شبکه حسگر بی‌سیم است. در نتیجه طراحی و تحلیل امنیتی شبکه حسگر بی‌سیم باید با توجه به کاربرد آن باشد. در غیر این صورت فرضیات در مورد سازماندهی شبکه حسگر بی‌سیم و تهدیدات متناظر با آن ممکن است با دامنه مسئله سازگار نبوده و باعث شود راه‌حل‌های ارائه شده، مسائل غیر واقعی را حل کنند.

امنیت مشخصات فنی تعریف شده ای ندارد بلکه مجموعه‌ای از عوامل مرتبط است که فضای طراحی شبکه حسگر بی‌سیم را به زمینه‌ای که با آن سازگار است، محدود می‌کند. واضح است که محدودیت‌های معمولی طراحی شبکه حسگر بی‌سیم مانند هزینه، عوامل سازنده و انرژی نیز باید در مشخصات فنی در نظر گرفته شود.

با پیشرفت شبکه حسگر بی‌سیم، نیاز به مکانیزم‌های امنیتی کارآمد نیز افزایش می‌یابد. به دلیل اینکه شبکه‌های حسگر ممکن است با داده‌های حساس سروکار داشته باشند، و یا در محیط‌های خصومت آمیز بدون نظارت کار کنند، مسائل امنیتی باید از ابتدا در طراحی سیستم مد نظر قرار گیرند. اما به دلیل محدودیت منابع پردازشی، چالش‌های امنیتی شبکه‌های حسگر با امنیت در شبکه / کامپیوتر سنتی تفاوت دارد. این شبکه‌ها نسبت به شبکه‌های دیگر در معرض انواع بیشتری از حملات هستند. کیفیت و پیچیدگی این حملات هر روز بیشتر می‌شود. در زمان انتقال اطلاعات از طریق شبکه حسگر بی‌سیم باید مانع سوء استفاده از اطلاعات شویم. روش‌های امنیتی مدرن باید ایمنی انتقال داده را از نظر نیازهای امنیتی مانند محرمانگی، یکپارچگی و دسترس‌پذیری (CIA) تضمین کنند. تأمین امنیت اطلاعات در شبکه حسگر بی‌سیم نیز ضروری است، به خصوص برای کاربردهای حساس امنیتی، و یکی از مهمترین مسائلی است که در این کتاب بررسی می‌شود.

یکی از مهمترین چالش‌ها، طراحی این شبکه‌ها و آسیب‌پذیری آنها نسبت به حملات امنیتی است که منجر به تخریب شبکه و کارایی پایین آن می‌شود. هر ساله نه تنها کمیت و پیچیدگی حملات جدید افزایش می‌یابد، بلکه قدرت آنها نیز بیشتر می‌شود. مقاومت در برابر این حملات هر روز پیچیده‌تر می‌شود. عوامل مخرب با توجه به امنیت پایین بی‌سیم از این ضعف برای حمله به شبکه حسگر بی‌سیم استفاده می‌کنند.

فصل ۲. شبکه‌های حسگر بی‌سیم به‌صورت روزافزون در اموری به کار می‌روند که کیفیت خدمات (QoS) و هزینه‌ی پایین در آنها اولویت دارد. با افزایش کاربرد، قابلیت اطمینان، دسترس‌پذیری و قابلیت ارائه خدمات باید از ابتدا مدنظر قرار گیرد. روش‌های معمولی استفاده از گره‌های حسگر و ادغام این سه حوزه (قابلیت اطمینان، دسترس‌پذیری و قابلیت ارائه خدمات) برای به دست آوردن کیفیت خدمات نه تنها می‌تواند قابلیت اطمینان به شبکه‌های حسگر بی‌سیم را افزایش دهد، بلکه امنیت را نیز افزایش می‌دهد. ما کیفیت خدمات را بررسی کرده، و سه عامل مهم کیفیت را که در حال حاضر باید در توسعه خدمات و امنیت کاربردهای شبکه حسگر بی‌سیم مد نظر قرار گیرند (قابلیت اطمینان، دسترس‌پذیری و قابلیت ارائه خدمات)، به‌صورت ریاضی بیان می‌کنیم. ویژگی‌ها و محدودیت‌های شبکه حسگر بی‌سیم و عوامل کیفیت خدمات در زمان توسعه کاربردهای امنیتی برای این شبکه‌ها را نیز بررسی می‌کنیم و در آزمایشات خود امنیت شبکه‌های

حسگر بی‌سیم را با ایجاد مدل‌های جریان و آزمون‌های شبیه‌سازی با استفاده از گره‌های حسگر اختصاصی، تأمین خواهیم کرد و برای تایید روش خود و ارزیابی احتمال ایجاد شبکه حسگر بی‌سیم امن از طریق کیفیت خدمات، در آزمایشات از گره‌های Hawk استفاده می‌کنیم. مدل‌های جریان نشان می‌دهند که چگونه می‌توان از کیفیت خدمات برای افزایش امنیت کاربردهایی که در شبکه‌های حسگر بی‌سیم اجرا می‌شوند، استفاده کرد.

فصل۳. برای طراحی گره‌های حسگر بی‌سیم امن با استفاده از مفهوم مانع، یک مدل پایه ریاضی ایجاد می‌کنیم. وقتی احتمال حمله علیه گره‌های شبکه حسگر وجود داشته باشد، امنیت به یکی از نگرانی‌های اصلی تبدیل می‌شود. بنابراین امنیت پایه را به شکل دیسک طراحی کردیم تا عناصر امنیتی اصلی را که در گره‌های حسگر مختلف قابل پیاده‌سازی هستند، فراهم کنیم. مدل‌های ریاضی معرفی شده به اندازه کافی انعطاف‌پذیر هستند و می‌توان در گره‌های حسگر از آنها استفاده کرده، و در محیط‌های خصومت‌آمیز امنیت مناسبی برای گره‌ها فراهم نمود.

فصل۴. در این کتاب نشان می‌دهیم که پیچیدگی حملات مدرن در حال افزایش است. این روند نیازمند یک استراتژی دفاعی همگرا است. محدودیت توان پردازشی و باتری در گره‌های حسگر، تنوع مکانیزم‌های امنیتی را کاهش می‌دهد. فقط باید از مکانیزم‌های متناسب با شبکه حسگر بی‌سیم استفاده کرد این روش‌ها از "روش فیستل" بهبود یافته الهام گرفته شده‌اند. طراحی اصلاح شده‌ی رمز - تسریع شده از جایگشت‌های وابسته به داده استفاده می‌کند و می‌توان از آن برای سیستم‌های رمزگذاری سریع سخت افزاری، میان افزاری، نرم افزاری و شبکه حسگر بی‌سیم استفاده کرد. روش ارائه شده نشان می‌دهد رمزها با استفاده از این روش احتمال نفوذ کمتری در برابر کشف رمز تفاضلی دارند. این روش از رمزگذاری‌های رایج در شبکه حسگر بی‌سیم مانند استاندارد رمزگذاری داده‌ها (DES) و Camellia بهتر است.

فصل ۵ برخی از ویژگی‌های خاص شبکه‌های حسگر (مانند محدودیت منابع، عملی نبودن حفاظت و نظارت فیزیکی بر هر گره، و اینکه به‌طور معمول عملکرد آنها با مولفه‌های بسیاری مانند مسیریابی و تعیین مکان پشتیبانی می‌شود)، باعث می‌شود تأمین امنیت شبکه‌های حسگر مشکل باشد. ما یک روش امضای توزیع شده (DSS) برای شبکه‌های حسگر ارائه می‌کنیم که می‌تواند توزیع مجدد رمز را به‌صورت خودکار انجام دهد. هدف ما

پشتیبانی از توزیع رمز بین اعضای جدید یک شبکه حسگر، بدون دخیل کردن یک عامل مورد اعتماد یا دخالت کاربر است. تحلیل‌های ما نشان می‌دهد که روش‌های جدید در مقایسه با روش‌های قبلی، ویژگی‌های خوبی دارند. اول، این سیستم کارآمد است. دوم، توزیع خودکار کلید پس از راه‌اندازی اولیه را تضمین می‌کند. سوم، به توزیع کلید اضطراری نیاز ندارد، و به‌صورت خودکار با گره‌ها تعامل دارد.

فصل۶. پروتکل‌های مسیریابی فعلی در شبکه حسگر بی‌سیم یا حتی در شبکه‌های موردی بی‌سیم، در معرض بسیاری از حملات مانند حمله پنهانی هستند. ساده‌ترین نوع حمله این است که مهاجم اطلاعات مسیریابی مخرب را به شبکه تزریق کند. این کار منجر به ناهماهنگی در مسیریابی شده، و تأخیر انتها به انتها را افزایش می‌دهد و حتی ممکن است باعث از بین رفتن بسته‌ها در شبکه شود. در ابتدا دو پروتکل مسیریابی پایه را به‌صورت خلاصه بیان می‌کنیم. این پروتکل‌ها براساس ماهیت شبکه حسگر بی‌سیم به دو دسته گسترده تقسیم می‌شوند و نشان می‌دهیم که هیچ کدام از پروتکل‌های مسیریابی قبلی نمی‌توانند به صورت همزمان تمام نیازها را برآورده کنند.

فهرست مطالب