

امنیت در شبکه‌های حسگر بی‌سیم

نویسندگان:
پروچ و رکو و تامارا پازینیوک

مترجم:
حمیدرضا منفرد

انتشارات بهترین نگاه
۱۳۹۹

سروشنامه: اورکو، جورج اس. Oreku, George S.

عنوان و نام پدیدآور: امنیت در شبکه‌های حسگر بی‌سیم/نویسندگان جورج ورکو و تامارا پازینیوک؛ مترجم حمیدرضا منفرد.

مشخصات نشر: کرج: بهترین نگاه، ۱۳۹۹.

مشخصات ظاهری: ۱۷۶ص.

شابک: ۹۷۸-۶۲۲-۹۷۳۱۳۰-۷

موضوع: فهرست نویسی: فیبا

یادداشت: عنوان اصلی: Security in wireless sensor networks, ۲۰۱۶.

یادداشت: کتاب حاضر نخستین بار با عنوان «امنیت در شبکه‌های حسگر بی‌سیم» در سال ۱۳۹۹ با ترجمه رامرز شای سوسهلا، سیدرضا زاهدی توسط دانشگاه افسری و تربیت پاسداری امام حسین (ع)، موسسه چاپ و انتشار، خیاگاه است.

موضوع: شبکه‌های حسگر بی‌سیم - تدابیر ایمنی

موضوع: Wireless sensor networks - Security measures

موضوع: Wireless sensor networks

شناسه افزوده: منفرد، حمیدرضا، ۱۳۷۴ - مترجم

ه‌رگز کی‌دیده‌در TK۷۸۷۲

رده‌بندی دیویی: ۰۰۴/۶۸۲۲

شماره کتابشناسی ملی: ۷۳۶۹۷۲۵

امنیت در شبکه‌های حسگر بی‌سیم

نویسنده: جورج ورکو و تامارا پازینیوک

مترجم: حمیدرضا منفرد

صفحه‌آرا و طراح جلد: مریم الهی

ناشر: بهترین نگاه

نوبت چاپ: اول / ۱۳۹۹

تیراژ: ۵۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۹۷۳۱۳۰-۷

قیمت: ۲۵۰۰۰ تومان

شماره تماس: ۰۹۱۲۷۱۷۵۸۷۳

فهرست مطالب

۹	پیش درآمد
۱۵	فصل ۱. معرفی و نمای کلی
۱۷	۱.۱ امنیت WSN
۱۸	۱.۱.۱ انواع امنیتی WSN
۲۱	۱.۱.۱.۱ ملزومات امنیتی
۲۷	۱.۱.۲ حمله‌ها
۳۴	۱.۱.۴ سبب‌ها و دفاعی
۴۵	۱.۲ انگیزه مهاجمان
۴۶	۱.۳ چالش‌های امنیتی
۵۲	۱.۴ انگیزه کتاب
۵۶	۱.۵ مسائل بحث شده در کتاب
۵۷	۱.۶ خطوط راه کتاب
۵۹	فصل ۲. QoS به عنوان یکی از راه‌ها برای امنیت در WSN
۶۳	۲.۲ QoS در شبکه‌های بی‌سیم
۶۳	۲.۲.۱ مفهوم QoS
۶۴	۲.۲.۲ معیارهای QoS
۶۵	۲.۲.۳ امنیت و QoS
۶۶	۲.۲.۴ چالش‌های QoS در شبکه‌های حسگر
۶۹	۲.۳ تاثیر امنیت بر QoS
۷۳	۲.۴ اعتمادپذیری، دسترسی و خدمت‌دهی (RAS)
۷۷	۲.۵ محاسبه دسترسی و احتمال پذیری درون WSN
۸۱	۲.۶ مدل‌های امنیتی پیشنهادی
۸۴	۲.۷ ارزیابی آزمایش
۸۶	۲.۸ خلاصه
۸۹	فصل ۳. مدل ریاضیاتی برای امنیت گره‌های حسگر بی‌سیم
۹۲	۳.۲ مانع امنیتی
۹۴	۳.۳ بیان مسئله و طراحی مدل ریاضیاتی

۳,۴	فرموله سازی	۹۵
۳,۵	اطمینان از مقاومت در برابر تهدید در گره‌های حسگر	۱۰۱
۳,۶	کاربرد مدل گره‌ها	۱۰۳
۳,۷	خلاصه	۱۰۶
فصل ۴	رمزنگارهای تقویت شده مبتنی بر فیستل، برای امنیت شبکه	۱۰۷
۴,۲	تهدیدات حمله‌ها	۱۰۹
۴,۳	اثرگذاری الگوریتم‌های WSN موجود	۱۱۲
۴,۴	تکلیف‌های روش پیشنهادی	۱۱۳
۴,۵	شماتیک فیستل	۱۱۳
۴,۶	رویکرد نظری CP	۱۱۷
۴,۷	شماتیک فیستل بهبود یافته برای تبادلات بلوکی داده	۱۱۹
۴,۸	مقایسه رمزنگارهای مبتنی بر شماتیک فیستل CPB و رمزنگارهای بدون CP	۱۲۱
۴,۹	خلاصه	۱۲۴
فصل ۵	شماتیک امضا توزیع شده (DSS) مبتنی بر RSA	۱۲۷
۵,۲	شماتیک‌های ایمن مبتنی بر RSA	۱۳۰
۵,۳	شماتیک امضای توزیع شده مبتنی بر RSA	۱۳۲
۵,۳,۱	ویژگی‌های امضای توزیع شده	۱۳۳
۵,۳,۲	رویکردهای اصلی توزیع کلید مخفی مبتنی بر RSA	۱۳۵
۵,۴	رویکرد ما در تهیه شماتیک	۱۳۷
۵,۴,۱	مقداردهی اولیه شماتیک	۱۳۹
۵,۴,۲	تولید امضای توزیع شده	۱۴۰
۵,۵	خلاصه	۱۴۲
فصل ۶	پروتکل تجمیع داده ایمن برای شبکه‌های حسگر بی‌سیم	۱۴۵
۶,۲	بیان مسئله	۱۴۹
۶,۳	پروتکل‌های تجمیع داده موجود	۱۵۰
۶,۴	پروتکل پیشنهادی	۱۵۲
۶,۵	فرضیه‌های امنیتی	۱۵۵
۶,۶	ارزیابی تجربی	۱۵۶
نتیجه‌گیری و کار آینده		۱۵۷
فهرست منابع		۱۷۶

پیش‌درآمد

شبکه‌های حسگر بی‌سیم (WSN)، حوزه مورد علاقه در بخش دانشگاهی و صنعتی است. این حوزه، دروازه‌ای به سوی تعداد بالایی از کاربردهای نظامی، صنعتی، عملی، غیر نظامی، و تجاری است. این شبکه‌ها، به‌طور خاص در کاربردهایی که مشاهدات انسانی یا حسگرهای سنتی امپدانت، ناکافی، هزینه‌بر، یا خطرناک است، امکان سنجش مفرق به سرفه را فراهم می‌کند. حسگرهای بی‌سیم دارای انرژی و قابلیت‌های دست‌یابی محدوداند، و در نتیجه به کارگیری بسیاری از روش‌های سنتی نظارتی در این شبکه‌ها، غیر ممکن خواهد بود. همچنین، این موارد اغلب در محیط‌های باز به کارگیری می‌شوند، که در معرض حمله‌های فیزیکی مانند جَمینگ یا تسخیر گره و دستکاری قرار خواهند داشت. تهدیدات متوجه WSN و سازماندهی WSN در پاسخ به این تهدیدات، به‌طور مستقیم وابسته به کاربرد WSN است. در نتیجه این موضوع باید در طراحی امنیتی WSN و تحلیل‌ها مورد توجه قرار گیرد. در غیر این صورت، ممکن است رویکردهای پیشنهادی برای سازماندهی WSN در برابر تهدیدات متناظر، در برابر مشکلات واقعی WSN برقرار نباشد؛ در نتیجه راه‌حل‌های تولید شده، مشکلات غیر واقعی را برطرف خواهند کرد.

محتوای امنیتی دارای تعریفی فنی دقیق نیست؛ این حوزه شامل

مجموعه‌ای از عامل‌های مرتبط امنیتی است که فضای طراحی WSN را به ناحیه سازگار با این دستورالعمل‌ها، تبدیل می‌کند. به طور واضح، محدودیت‌های مرسوم طراحی WSN، مانند هزینه، عامل فرم، و انرژی باید در مشخصات فنی در نظر گرفته شود.

با رشد WSN، نیاز برای مکانیزم‌های موثر امنیتی نیز افزایش یافته است. ممکن است که شبکه‌های حسگر با داده حساس در تمام باشند و یا در محیط‌های در معرض خطر و بدون مراقبت عمل کنند؛ لذا ضروری است تا این نگرانی‌های امنیتی از ابتدای طراحی میسر در نظر گرفته شود. با این حال، به دلیل منابع ذاتی و محدودیت‌های جابجایی، امنیت در شبکه‌های حسگر نسبت به امنیت سنتی شبکه یا کامپیوتر، با چالش‌های مختلفی روبه‌رو است. این شبکه‌ها نسبت به سایر شبکه‌ها، در معرض گستره وسیع‌تری از حمله قرار دارند. کیفیت رمزپسندی این حمله‌ها هر روزه در حال افزایش است. می‌بایست بین اطلاعات از طریق WSN از سواستفاده در امان باشد. روش‌های امنیتی مدرن باید نیازهای امنیتی در انتقال داده، مانند اعتمادپذیری، سلامت، و دست‌پذیری (CIA) را تضمین کنند. برقراری امنیت اطلاعات در WSN، به خصوص برای کاربردهای حساس امنیتی ضروری است. این موضوع از اصلی‌ترین نگرانی‌های است که در روش پیشنهادی با آن طرف شده است.

یکی از چالش‌های اصلی در این حوزه، طراحی این شبکه‌ها و آسیب‌پذیری آن‌ها در برابر حمله‌های امنیتی است، که منجر به تخریب شبکه و عملکرد ضعیف می‌شود. نه تنها کمیت و پیچیدگی این حمله‌ها، بلکه همچنین ظاهر و مومنتوم آن‌ها نیز هر ساله

۱۱/ امنیت در شبکه‌های حسگر بی سیم

افزایش می‌یابد. مقاومت در برابر آن‌ها پیچیده‌تر می‌شود. مأموران دشمن از آسیب‌پذیری‌های امنیتی استفاده بیشتری می‌کنند؛ به دلیل ضعف‌های امنیتی ارتباط بی‌سیم، حمله‌های متعددی در حوزه WSN انجام می‌شود.

فصل ۲. WSN به صورت روز افزون در کاربردهایی که کیفیت خدمت (QoS) و هزینه پایین محدودیت‌های اصلی هستند، مورد استفاده قرار می‌گیرند. با افزایش استفاده، باید مشکلات مربوط به اعتمادپذیری، دسترسی، و خدمت‌دهی برطرف شود. شماتک‌های مرسوم استفاده از گره‌های حسگر و ترکیب این سه ناحیه (اعتمادپذیری، دسترسی و خدمت‌دهی) برای دستیابی به QoS نه تنها اعتمادپذیری بی‌WSN را بصورت موثر بهبود می‌دهد، بلکه امنیت را نیز افزایش می‌دهد. ما در خصوص نگاه معکوس به QoS بحث خواهیم کرد و به صورت ریاضیاتی، سه عامل کیفی چشم‌گیر در توسعه خدمات کاربردی SN یعنی دسترسی، اعتمادپذیری و خدمت‌دهی امنیتی را بررسی خواهیم کرد. همچنین در خصوص مشخصه‌های معین و محدودیت‌های WSN، اما‌های QoS در زمان توسعه کاربردهای امنیتی برای چنین شبکه‌هایی بحث خواهیم کرد. امنیت WSN‌ها با ارائه مدل‌های روان و تست‌های شبیه‌سازی با استفاده از گره‌های حسگر مستقل در ازای آن‌ها بررسی می‌شود. به منظور بررسی امکان دستیابی به WSN ایمن از طریق QoS، از گره‌های Hawk برای نمایش تجربی رویکرد خود استفاده کرده ایم. مدل‌های جریان، نشان دهنده چگونگی بکارگیری QoS به منظور افزایش امنیت اپلیکیشن‌های در حال اجرا تحت WSN است.