بسمه تعالی

شبکه‌های حسگر بی‌سیم امن

(تهدیدها و راه حل‌ها)

اثر مورو کنتی

مترجم : مهندس ویدا درانی پور

انتشارات ارسطو
(چاپ و نشر ایران)
۱۳۹۶

سرشناسه : کونتی، مائورو
Conti, Mauro
عنوان و نام پدیدآور: شبکه‌های حسگر بی‌سیم امن/ اثر مورو کونتی؛ ترجمه‌ی ویدا درانی‌پور.
مشخصات نشر : مشهد: ارسطو، ۱۳۹۶.
مشخصات ظاهری : ۲۷۳ ص.: مصور.
شابک : ۱-۱۵۰-۴۳۲-۶۰۰-۹۷۸
وضعیت فهرست نویسی : فیپا
یادداشت : عنوان اصلی: .Secure wireless sensor networks : threats and solutions
موضوع : شبکه‌های حسگر بی‌سیم -- تدابیر ایمنی
موضوع : Wireless sensor networks -- Security measures
موضوع : سواد کامپیوتری
موضوع : Computer literacy
موضوع : علوم کامپیوتر
موضوع : Computer science
شناسه افزوده : درانی‌پور، ویدا، ۱۳۶۰ -، مترجم
رده بندی کنگره : ۱۳۹۶ ۹ک۲ش/ TKv۸۷۲
رده بندی دیویی : ۰۰۴/۶۸۲۲
شماره کتابشناسی ملی : ۴۶۹۵۶۰۲

نام کتاب : شبکه‌های حسگر بی‌سیم امن
نویسنده : مورو کونتی
مترجم: ویدا درانی‌پور
ناشر : ارسطو (چاپ و نشر ایران)
صفحه آرایی، تنظیم و طرح جلد : پروانه مهاجر
تیراژ : ۱۰۰۰
نوبت چاپ : اول – ۱۳۹۶
چاپ : مدیران
قیمت : ۱۹۰۰۰ تومان
شابک : ۱-۱۵۰-۴۳۲-۶۰۰-۹۷۸
تلفن های مرکز پخش : ۳۵۰۹۶۱۴۵ – ۳۵۰۹۶۱۴۶ – ۰۵۱
www.chaponashr.ir

چاپ و نشر ایران
انتشارات ارسطو

سخن اول

ایــن کتاب از دکتر مارو کانتی بر مهم‌ترین چالش‌های پیش روی شــبکه‌های حســگر بی‌ســیم تمرکز دارد و بررسی گسترده‌ای از تحقیقات پیشین در زمینهٔ تهدیدهای امنیتی انجام داده اســت. به تازگی نیز اقدامات متقابلی پیشــنهاد داده و چند روش نوین کاهشی بــرای هر حملهٔ مورد نظر ارائه کرده اســت. به علاوه، دکتــر کانتی بحث‌های دقیق نظری، تحلیلی و آزمایشی در مورد هر یک از حملات و اقدامات متقابل ارائه می‌کند. به خصوص، تهدید امنیتی ممکن اســت نتیجهٔ شرایطی خطرناک برای شبکه‌های حسگر بی‌سیم باشد، به ایــن دلیل که در اعمــال مکانیزم‌های امنیتی ســنتی محدودیت‌های ســخت‌افزاری و نرم‌افزاری ذاتی وجود دارد و این شــبکه‌ها به صورت مکرر از کاربردهای حیاتی بی‌شماری استفاده می‌کنند.

در طول این ســال‌ها، به همراه گروه تحقیقاتی‌ام در دانشکدهٔ علوم کامپیوتر از دانشگاه ســاپینزا واقع در رم[1] و چندین محقق نامدار در سراسر جهان با جنبه‌های مختلف امنیت شــبکه‌ها، مخصوصاً در شبکه‌های حسگر بی‌سیم، ســر و کار داشته‌ام. باور دارم که یکی از اهداف اصلی به‌کارگیری شبکه‌های حسگر بی‌سیم ارائه امنیت و راحتی برای انسان‌ها است. بنابراین، باید در نظر داشته باشیم که چطور این فناوری جدید اهداف طراح را بدون تهدید امنیت و حریم شخصی کاربران تضمین خواهد کرد.

دکتــر کانتی اطلاعات به روزی برای دانش‌پژوهان و محققین ارائه می‌کند که تمایل به طراحی سیســتم‌ها و کاربردهای WSN دارند. بدین ترتیب قادر خواهند بود بر چالش‌های

1. Dipartimento di Informatica della Sapienza Università di Roma

امنیتـــی موجود در این شـــبکه‌ها غلبه کننـــد. به علاوه، این کتـــاب در زمینهٔ مراحل اولیهٔ تحقیق در جنبه‌های ایجاد کلید، حملات فیزیکی، حملات تســـخیر گره، حملات کپی گره و همچنین مسائل امنیتی و حریم شخصی خدمات به‌خصوص WSN نظیر انبوهش داده‌ها شفاف‌ســـازی می‌کند. محتوای این کتاب حاصل چندین سال تلاش تحقیقاتی دکتر کانتی در زمینهٔ مسائل امنیتی و حریم شخصی شبکه‌های حسگر بی‌سیم است که مقالات و ثبت اختراعات بی‌شماری را نتیجه می‌دهد.

باعث افتخارم بود که به عنوان دانشـــجوی دکترا بر تحقیقات اولیهٔ دکتر کانتی نظارت کنم و در تمام مراحل این کار دخیل باشـــم و همچنین پس از آن با دکتر کانتی همکاری داشـــته باشـــم. باور دارم این کتاب از دکتر کانتی مرجعی کلیدی برای چالش‌های امنیتی شبکه‌های حسگر بی‌سیم قلمداد می‌شود و امیدوارم از خواندن آن *لذت* ببرید.

لوئیجی وینچنزو مانچینی دانشگاه ساپینزا رم، ایتالیا

پیش‌گفتار

پیشرفت‌های اخیر فناوری، مخصوصاً در حوزه‌های شبکه‌های کامپیوتری و کوچک‌سازی سخت‌افزار، ظهور مجموعه‌ای از محاسبات جدید وسناریوهای کاربردی را به روش‌های مختلف امکان‌پذیر می‌سازد، شامل «اینترنت اشیا»، «محاسبات همراه»، «محاسبات فراگیر»، یا «محاسبات همه جا حاضر». با وجود معنای به‌خصوص این اصطلاحات فنی و خصوصیات آن‌ها، تمام مفاهیم شامل دستگاه‌های کوچک و ریزی می‌شوند که ارتباط برقرار می‌کنند (احتمالاً به صورت بی‌سیم) و به منظور دستیابی به هدفی مشترک با یکدیگر همکاری می‌کنند. در بسیاری از این سناریوهای کاربردی نوظهور، امنیت خدمات و زیرساخت، و همچنین حریم شخصی طرفین، ویژگی اساسی به شمار می‌رود.

در این کتاب، بر فناوری نماینده در این حوزه تمرکز داریم: شبکه‌های حسگر بی‌سیم (WSN)، یعنی شبکه‌هایی که از دستگاه‌های کوچک با محدودیت منبع که دارای قابلیت‌های حسگری و ارتباط بی‌سیم هستند. به خصوص، روشی جامع برای ساخت شبکه‌های حسگر بی‌سیم ایمن ارائه می‌کنیم که با در نظر گرفتن سطوح مختلف تهدیدهای امنیتی زیر این کار را انجام می‌دهیم: نیاز پایهٔ اعتماد و محرمانگی بین گره‌ها (از طریق ایجاد کلیدهای محرمانه)، حملات فیزیکی نظیر تسخیر گره (حذف فیزیکی) یا کپی کردن گره (ایجاد فیزیکی یک گرهٔ جدید، کپی کردن اطلاعات رمزنگاری‌شده از گره‌ای قابل اعتماد)، امنیت کاربردهای به‌خصوص که در آن انبوهش به‌خصوص داده‌ها را در نظر می‌گیریم که خدماتی کلیدی در شبکه‌های حسگر بی‌سیم محسوب می‌شود و می‌تواند برای غلبه بر محدودیت‌های انرژی آن ها به کار رود. سرانجام، برای سرویس انبوهش داده‌ها به عنوان موردی نماینده جنبه‌های حریم شخصی امکانپذیر را (مثلاً حفظ حریم شخصی گره‌های

دخیل در انبوهش) نیز بررسی می‌کنیم که در سناریوهای عملی ممکن است برای کاربران نمونهٔ سنجش هوشمند یا دیگر خدمات به کار روند.

نقش‌های اصلی این کتاب به صورت خلاصه در ادامه آمده است:

- در زمینهٔ ایجاد کلیدهای محرمانهٔ جفتی بین گره‌ها، راه‌حل جدید احتمالاتی، یعنی پروتکل ایجاد کانال جمعی تقویت‌شده (ECCE)، ارائه می‌کنیم که به برخی از محدودیت‌های راه‌حل‌های موجود غلبه می‌کند. در واقع، در ECCE احتمالش بیش‌تر است جفت گره‌ها کانالی ایمن و نرخ برگشت‌پذیری بالاتر ایجاد کنند (یعنی مهاجم باید برای تخریب کانال تلاش بیش‌تری کند). در مورد این راه‌حل اطلاعات اندکی در منابع [۴۶، ۴۷] نشر یافته و توضیحاتی نیز در فصل ۲ ارائه شده است.

- در زمینهٔ حملهٔ تسخیر گره (یعنی حذف فیزیکی از شبکه)، که اولین گام برای مهاجم به منظور اجرای چند حملهٔ دیگر است (مثل حملهٔ کپی یا نقض محرمانگی) که برای شبکه‌های حسگر بی‌سیم بحرانی هستند، اولین روش را برای شناسایی تسخیر گره که از تحرک شبکه به نحو احسن بهره می‌گیرد طراحی می‌کنیم تا گره‌ها بتوانند توسط گره‌های دیگر ردیابی شوند. نتایج به دست آمده از مطالعات‌مان نشان می‌دهد که راه‌حل‌های جدید می‌تواند عملاً در شبکه‌های حسگر پیاده‌سازی شود و تحت شرایط تحرک معین (مثل میانگین سرعت معین گره) بهتر از راه‌حل‌هایی عمل می‌کنند از تحرک شبکه به نحو احسن بهره‌مند نمی‌شوند. در مورد این راه‌حل اطلاعات اندکی در منابع [۴۵، ۴۹، ۵۳] نشر یافته و توضیحاتی نیز در فصل ۳ ارائه شده است.

- در زمینهٔ حملهٔ کپی گره، ابتدا خصوصیاتی را شناسایی می‌کنیم که یک پروتکل تشخیص کپی توزیع‌شده باید در اختیار داشته باشد، سپس یک پروتکل تصادفی، کارآمد و توزیعی (RED) برای تشخیص حملهٔ همتاسازی طراحی می‌کنیم. پروتکل RED خصوصیات و عملکرد بهتری در مقایسه با فناوری‌های به‌روز نشان می‌دهد.

به خصوص، تحت تأثیر مسائل مهمی قرار نمی‌گیرد که در تحقیقات گذشته بر پروتکل‌ها تأثیرگذار بودند؛ این به معنی پیش‌بینی‌پذیری موقعیت شاهدها است. بنابراین، در سناریوهای عملی فرایند تشخیص تأثیر کم‌تری خواهد داشت. در مورد این راه‌حل اطلاعات اندکی در منابع [۵۰، ۵۲، ۵۴، ۵۵] نشر یافته و توضیحاتی نیز در فصل ۴ ارائه شده است.

- در زمینهٔ خدمات شبکه‌های حسگر بی‌سیم، بر امنیت انبوهش داده‌ها تمرکز می‌کنیم. در این جا مسئله این بود که با وجود احتمال حضور خرابکارها آیا سرویس WSN می‌تواند ایمن باشد یا خیر. با توجه به منابع محدود شبکه‌های حسگر بی‌سیم، گره‌ها نمی‌توانند داده‌های حسگری خود را به طوری مستقل به نقطهٔ جمع‌آوری ارسال کنند؛ بنابراین، استفاده از پروتکل انبوهش (و همچنین امنیت آن) ضروری است. در این سناریو اولین پروتکل امنیتی را برای ایمن‌سازی رایانش انبوهش میانگین طراحی می‌کنیم. در مورد این راه‌حل اطلاعات اندکی در منابع [۱۹۰، ۱۹۲-۱۹۴] نشر یافته و توضیحاتی نیز در فصل ۵ ارائه شده است.

- در زمینهٔ امنیت انبوهش داده‌ها، مشکل پیش رو ارائه حریم شخصی برای یک گره بود که در فرآیند انبوهش داده‌ها شرکت داشت. در بسیاری از کاربردهای شبکهٔ حسگر، داده‌ها که توسط یک گرهٔ واحد حس می‌شوند ممکن است با کاربر (یا تعدادی از کاربران) مرتبط باشند: اطلاعات در مورد سلامت بیماران در یک بیمارستان، مصرف آب در یک شهر و غیره. سپس به منظور محافظت از حریم شخصی افراد، پروتکل انبوهش داده‌ها که در این زمینه کاربرد دارد باید حریم شخصی تک‌تک گره‌ها را حفظ کند. به خصوص، مرتبط ساختن داده‌های دریافتی معین با گرهٔ حسگر معین نباید امکان‌پذیر باشد. بدین ترتیب اولین پروتکل انبوهش داده‌ها را ارائه می‌کنیم که حریم شخصی یک گره را نه تنها در مقابل گره‌های دیگر، بلکه در مقابل ایستگاه پایه (موجودیتی که در نهایت داده‌های انباشته را جمع‌آوری می‌کند) محافظت می‌کند. در مورد این راه‌حل اطلاعات اندکی در منابع [۶۰، ۲۴۰] نشر یافته و توضیحاتی نیز در فصل ۶ ارائه شده است.

قدردانی

این کتاب نسخه‌ای تجدید نظر شده از پایان‌نامهٔ دکترایم است. در این جا فرصت را غنیمت شمرده و از تمام افرادی که در تحقق این امر یاری رسانده‌اند و در طول سال‌های مطالعاتم همراهی‌ام کرده‌اند، کمال تشکر را به عمل آورم. جا دارد از استاد راهنمای دکترای خود آقای لوئیجی وینچنزو مانچینی به خاطر تشویق به تحقیق در جنبه‌های امنیتی سیستم‌ها و ارتباطات کامپیوتری؛ استاد سوشیل جاجودیا، مخصوصاً به خاطر میزبانی حضورم در دانشگاه جورج میسون؛ و تمام افرادی که در طول گذراندن دکترای خود افتخار همکاری با آن‌ها را داشته‌ام (روبرتو دی پیترو، اندریا گابریلی، الساندرو می، سانجیو ستیا، انجلو اسپوگناردی، سانکارداس روی و لی ژانگ) سپاسگزاری کنم. از استاد کریستینا پینوتی و سرجان کاپکون به خاطر نظرات ارزشمندشان نیز تشکر ویژه می‌کنم که در بهبود کیفیت این کار کمک به‌سزایی کرده‌اند. همچنین از سوزان لاگرستروم فیفه و جنیفر مالات در اسپرینگر به خاطر راهنمایی شان در طول آماده‌سازی این کتاب تشکر می‌کنم.

افزون بر این، جا دارد از تمام دانشمندان بزرگ دنیا که در مراحل اولیهٔ مسیر آکادمیک با من همکاری کردند و همچنین تمام دانشجویان پرشور و همکاران در گروه تحقیقاتی‌ام در دانشگاه پادورا سپاسگزار باشم؛ شما واقعاً باعث شدید کار تحقیقاتی‌ام هیجان‌انگیز و پر ارزش شود!

و نهایتاً در مورد آخر که البته کم اهمیت هم نیست، جا دارد از خانواده‌ام به خاطر حمایت مستمرشان و کمک به تحقق این هدف تشکر کنم.

فهرست مطالب

عنوان صفحه

عنوان | صفحه

عنوان | صفحه

عنوان | صفحه

عنوان صفحه

عنوان صفحه

۱- مقدمه

تکامل دستگاه‌های محاسباتی مسیرهای مختلفی را دنبال کرده است. با وجود نقل قولی که به غلط به توماس ج. واتسون سینیور، رئیس وقت IBM، نسبت داده شده («فکر می‌کنیم برای احتمالاً پنج کامپیوتر بازار جهانی وجود داشته باشد.»)، در طول دهۀ ۷۰ میلادی الگوی جدیدی پدیدار شد: کامپیوتر شخصی. کامپیوترها که مختص استفاده توسط یک شخص بودند آن قدر رایج شدند که بازار کامپیوترهای شخصی بر بزرگ‌رایانه‌ها[1] فائق آمدند. با معرفی شبکه‌های کامپیوتری و کوچک کردن سخت‌افزارها الگوی کاملاً جدیدی طی دهۀ گذشته پا به عرصۀ وجود نهاد: رایانش اصطلاحاً فراگیر. به بیانی دقیق‌تر، هدف این الگوی موجود ساختن کامپیوترهای زیاد در میان محیط فیزیکی به شکلی است که به طور مؤثر از دید کاربران مخفی باشند [۲۲۸]. پیشرفت‌های اخیر در ریزسیستم‌های الکترومکانیکی (MEMS)، ارتباطات بی‌سیم و دستگاه‌های الکترونیک دیجیتال، تولید دستگاه‌های کوچک، ارزان و «هوشمند» را ممکن ساخته است (که مسائل امنیت و حریم شخصی جدیدی نیز به همراه دارد [۵،۶، ۱۲، ۱۷، ۵۸، ۱۵۱، ۱۶۴]). از این دستگاه‌ها می‌توان به تلفن‌های هوشمند [۴۴، ۵۱، ۵۹، ۸۸، ۹۷، ۱۸۸، ۲۴۳]، دستیارهای شخصی دیجیتال، سیستم‌های شناسۀ فرکانس رادیویی (RFID) [۵۶، ۵۷، ۱۹۱]، شبکه‌های حسگر بی‌سیم (WSN) و بسیاری دیگر اشاره کرد.

1. mainframe

در این کتاب، بر مسائل امنیتی فناوری بازنمایانندهٔ شبکه‌های حسگر بی‌سیم تمرکز می‌کنیم که در بخش‌های بعدی معرفی شده است.

۱.۱- شبکه‌های حسگر بی‌سیم

در این کتاب دستگاه حسگر دستگاه کوچکی است که می‌تواند داده‌های محیطی را حس کند (صدا، نور، دما و غیره) و همچنین می‌تواند با گره‌های حسگر دیر در محدودهٔ ارتباطی ارتباط برقرار کند و داده‌های دریافتی را محاسبه کند. مجموعه‌ای از این دستگاه‌های حسگر که در محیطی معین پیاده‌سازی شده‌اند شبکه‌ای بدون معماریِ از پیش دایرشده تشکیل می‌دهند. کارایی این نوع شبکه از قابلیت‌های یک گرهٔ واحد (که خیلی محدود است) به دست نمی‌آید، بلکه از همکاری تعداد زیادی گره حاصل می‌شود. در یک شبکهٔ حسگر بی‌سیم، صدها یا هزاران گره معمولاً در محیطی بزرگ پیاده‌سازی می شوند که در آن می‌توانند محیط را حس کنند و داده‌های جمع‌آوری شده را به شکلی کاملاً کارآمد و توزیعی محاسبه کرده و ارتباط‌شان را برقرار نمایند. گره‌های حسگر متفاوت از دیگر دستگاه‌های بی‌سیم سنتی مستقیماً با ایستگاه پایه (BS) (دستگاهی که محدودیت‌های گرهٔ حسگر را ندارد) ارتباط برقرار نمی‌کنند، بلکه اساساً ارتباطشان با دیگر گره‌های حسگر است. بنابراین، داده‌های دریافتی به صورت محلی محاسبه شده و به ایستگاه پایه ارسال می‌شوند. نبود یک زیرساخت از پیش طراحی‌شده این موضوع را می‌رساند که هر گره نه تنها به عنوان گرهٔ حسگر بلکه همچنین به عنوان گرهٔ توسعه‌دهنده و نقطهٔ مسیریابی عمل می‌کند.

کاربردهای فعلی و آتی شبکه‌های حسگر بی‌سیم در زمینه‌های مختلف هستند [۱۲۷]: پشتیبانی از عملیات نجات، ایجاد نظارت، جلوگیری از آتش‌سوزی، نظارت بر میدان نبرد و غیره. همچنین همان طور که اغلب برای فناوری‌های جدید پیش می‌آید، مادامی که فناوری ارزان‌تر می‌شود و بیش‌تر در دسترس قرار می‌گیرد، کاربردهای بسیاری قابل طراحی و تصور هستند. توضیحات بیش‌تر دربارهٔ کاربردهای ممکن شبکه‌های حسگر بی‌سیم در بخش ۱.۱.۱ آمده است. در بسیاری از کاربردهای شبکه‌های حسگر بی‌سیم،

امنیت شـــبکه در ارتباط با محرمانگی، یکپارچگی، اصالت و دسترســـی‌پذیری مسئلهٔ اصلی محســـوب می‌شـــود. به عنوان مثال فرض کنید WSN برای امنیت یک منطقه پیاده‌سازی شـــده باشد، مثلاً برای تشخیص گازهای سمی که می‌تواند در طول کنسرت یا یک رویداد ورزشـــی بزرگ پخش شـــود. در این سناریو، اگر شبکه ایمن نباشـــد ممکن است برداشتی غلط از امنیت داشته باشیم که حتی می‌تواند از این موضوع بدتر باشد که آگاه باشیم هیچ امنیتی وجود ندارد.

۱.۱.۱- کاربردها

در این جا تعدادی از حوزه‌های کاربردی ممکن شـــبکه‌های حســـگر بی‌ســـیم را یادآور می‌شویم:

- کاربردهـــای محیطی [۳، ۳۳، ۸۶، ۲۲۶]. برخی از کاربردهای محیطی شـــبکه‌های حســـگر عبارتند از ردیابی حرکات پرندگان، حیوانات کوچک و حشرات؛ نظارت بر شرایط محیطی که بر محصولات و دام تأثیر می‌گذارد؛ آبیاری؛ ابزارهای کلان برای نظارت مقیاس بزرگ بر زمین و کاوش ســـیاره‌ای؛ تشـــخیص شیمیایی/بیولوژیکی؛ کشاورزی دقیق؛ نظارت بیولوژیکی، زمینی و محیطی در زمینه‌های دریایی، خاکی و جوی؛ تشـــخیص آتش‌ســـوزی در جنگل؛ تحقیقات هواشـــناختی یا ژئوفیزیکی؛ نگاشت بیوکمپلکسیتی محیط؛ و مطالعهٔ آلودگی.
- کاربردهای ســـلامت [۶۲]. برخی از کاربردهای ســـلامت برای شـــبکه‌های حسگر عبارتند از ارائه رابط‌هایی برای افراد معلول؛ نظارت یکپارچه بر بیماران؛ تشـــخیص بیماری؛ تجویز دارو در بیمارستان‌ها؛ نظارت مستمر داده‌های فیزیولوژیکی انسان‌ها؛ عرضهٔ دقیق ریزداروها و جراحی غیر تهاجمی؛ نظارت از راه دور افراد مسن.
- کاربردهـــای تجاری [۳، ۸۶، ۱۸۲]. برخـــی از کاربردهای تجاری عبارتند از نظارت بر فرســـودگی مواد؛ ســـاخت کیبوردهای مجازی؛ مدیریت انبار؛ نظارت بر کیفیت محصولات؛ ســـاخت فضاهای اداری هوشـــمند؛ کنترل محیطی در ســـاختمان‌های

اداری؛ کنتـــرل رباتیک و راهنمایی در محیط‌های تولید خودکار؛ اســـباب‌بازی‌های تعاملـــی؛ موزه‌هـــای تعاملی؛ کنترل و اتوماســـیون فرآیندهـــای کارخانه؛ نظارت بر نواحی روی دادن فاجعه؛ ســـاختارهای هوشـــمند با گره‌های حسگر تعبیه‌شده در آن‌ها؛ تشـــخیص ماشینی؛ حمل و نقل؛ تجهیزات کارخانه؛ کنترل محلی عملگرها؛ تشخیص و نظارت دزدی خودرو؛ ردیابی و تشخیص خودروها.

- کاربردهای نظامی [۳]. از آن جایی که شـــبکه‌های حســـگر بی‌سیم متحمل خطا، خودســـازمانده، کوچک‌شـــده، کم‌هزینه و به راحتی قابل پیاده‌سازی هستند (برای نمونه پخش شـــدن توســـط هلیکوپتر)، آن‌ها را می‌توان به عنوان منبعی ارزشمند بـــرای ارتش و امـــور نظامی در نظر گرفت. برخی از کاربردهای نظامی شـــبکه‌های حســـگر عبارتنـــد از نظارت بر منابع میدان نبرد؛ نظـــارت (مراقبت) بر میدان نبرد؛ تشخیص و شناسایی عامل‌های هسته‌ای، بیولوژیکی و شیمیایی (NBC)؛ ارتباطات تاکتیکی.

۱.۱.۲- فناوری‌های تواناسازی

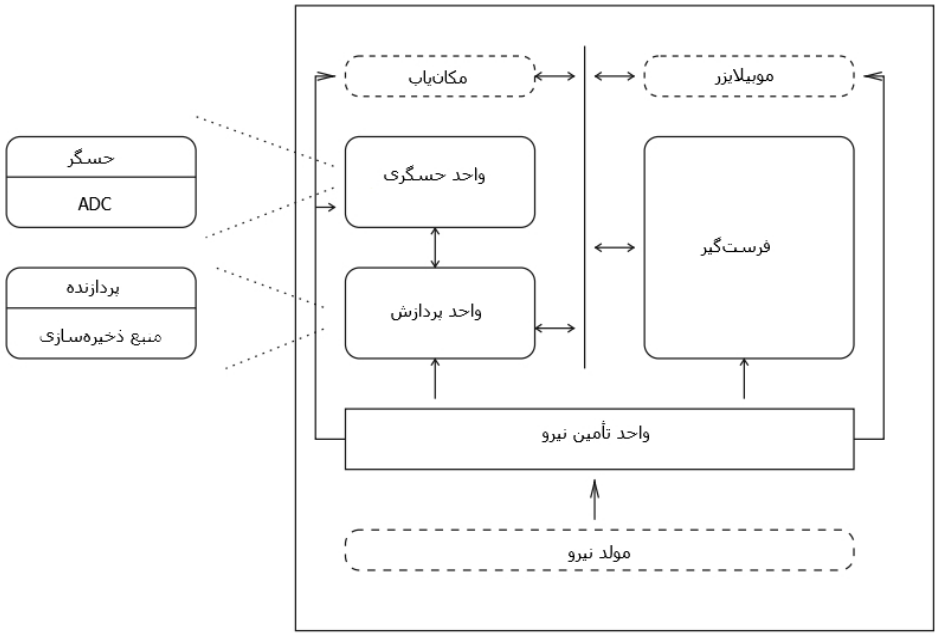
در این بخش به طور خلاصه به بررســـی فناوری‌های تواناســـازی اصلی برای شبکه‌های حسگر بی‌سیم می‌پردازیم [۱۷۴]:

- **اجزاء حســـگر.** گرهٔ حسگر از چهار جزء اصلی تشکیل شده است (شکل ۱.۱): واحد دریافـــت، واحـــد پردازش، واحد فرســـتنده و گیرنده و واحد تأمیـــن توان. گره‌های حسگر همچنین ممکن است اجزاء بسته به کاربرد دیگری نظیر سیستم مکان‌یاب، مولد نیرو و موبیلایزر داشـــته باشـــند. واحدهای حســـگری معمولاً از دو زیر واحد تشـــکیل شده‌اند: حســـگرها و مبدل‌های آنالوگ به دیجیتال (ADC). سیگنال‌های آنالوگ بر اســـاس پدیدهٔ مشاهده‌شده توســـط حسگرها ایجاد می‌شوند و به وسیلهٔ ADC به ســـیگنال‌های دیجیتال تبدیل می‌گردند، سپس به واحد پردازش خورانده می‌شـــوند. واحد پردازش که عموماً با واحد ذخیره‌ســـازی کوچکی در ارتباط است، دســـتورالعمل‌هایی را مدیریت می‌کند که باعث می‌شود گرهٔ حسگر به منظور انجام

امور حسگری اختصاص‌یافته با دیگر گره‌ها همکاری کند. واحد فرست‌گیر گره را به شبکه متصل می‌کند. یکی از مهم‌ترین اجزای گرهٔ حسگر واحد تأمین نیرو (برق) است. زیرواحدهای دیگری نیز ممکن است وجود داشته باشد که وابسته به کاربرد هستند. بسیاری از تکنیک‌های مسیریابی شبکه و وظایف حسگری مستلزم اطلاعات مکانی با دقت بالا هستند. بنابراین، در برخی کاربردها گرهٔ حسگر ممکن است به سیستم مکان‌یاب نیاز داشته باشد. در برخی موارد چنین فرض می‌شود که هر گرهٔ حسگر (یا برخی از آن‌ها) واحد سیستم موقعیت‌یابی جهانی (GPS) در اختیار دارد. برخی اوقات به منظور جابجایی گره‌های حسگر به هنگام نیاز برای انجام امور اختصاص‌یافته ممکن است متحرک سازی لازم شود. ممکن است لازم باشد تمام این زیرواحدها در یک ماژول هم‌اندازهٔ قوطی کبریت جا شوند [۱۱۳، ۱۲۵، ۱۷۳]. برق نیز به خاطر محدودیت‌های اندازه از منابع کم‌یاب قلمداد می‌شود. واحدهای تأمین نیرو ممکن است توسط واحدهای مهار نیرو[۲] مانند سلول‌های خورشیدی پشتیبانی شوند یا به قابلیت تبدیل ارتعاش به انرژی مجهز گردند [۳۹، ۱۸۹]. برای نمونه، کل انرژی ذخیره‌شده در حسگرهای کوچک[۳] smart dust تقریباً ۱ ژول است [۱۱۳، ۱۸۰]. گرچه توان پردازشی بالاتر برای پردازنده‌های کوچک‌تر و کوچک‌تر ممکن شده، واحدهای پردازش و حافظهٔ گره‌های حسگر همچنان منابعی نادر به شمار می‌روند. برای نمونه، واحد پردازش پروتوتایپ حسگر کوچک smart dust یک میکروکنترلر ۴ مگاهرتزی Atmel AVR8535 با حافظهٔ فلش ۸ کیلو بایتی، رم ۵۱۲ بایتی و EEPROM ۵۱۲ بایتی است [۱۱۳، ۱۷۳].

2. واحد مهار نیرو – *power scavenging unit / energy harvesting unit*

3. *mote*



شکل ۱.۱- اجزاء منطقی واحد حسگر

- **فناوری ارتباطات** یکی از فناوری‌های ارتباطاتی نویدبخش برای WSN فناوری بلوتوث است. این استاندارد پیکربندی موردی[۴] پیکونت‌های ارباب/برده شامل حداکثر هشت واحد فعال ارائه می‌کند. بلوتوث ارتباطات خودانگیز بین دستگاه‌ها را پشتیبانی می‌کند. این استاندارد انتقال داده بین واحدها را تا مسافت اسمی ۱۰ متر امکان‌پذیر می‌سازد. بلوتوث در اصل فناوری جایگزین کابلی تصور می‌شد و می‌تواند به خوبی در این حوزهٔ کاربردی عمل کند. بلوتوث با نرخ انتقال دادهٔ تا ۱ مگابیت در ثانیه پهنای باندی بیش از آن چه برای هدفمان نیاز داریم ارائه می‌کند. به هر حال، سناریوهایی که شامل تعداد زیادی دستگاه‌های کم‌توان هستند و از شبکهٔ موردی استفاده می‌کنند هنوز هنگام استفاده از

4. *Ad hoc*

بلوتوث به عنوان فناوری ارتباطی‌شان با تعدادی مانع مواجه می‌شوند [۱۳۰].
از دیگر فناوری‌های قابل توجه، فناوری‌ای است که از گروه کاری ZigBee [۱۲۰] به دست آمده که همچنین به نام‌های Firefly، RF-Lite، PURLnet و HomeRFLite شناخته می‌شود. زیگبی همچنان از ابتکاراتی در توسعهٔ استاندارد برای شبکه‌های بی‌سیم کم‌برد محسوب می‌شود. حوزه‌های کاربری پیش‌بینی‌شدهٔ آن شامل دستگاه‌های جانبی کامپیوتر، اسباب‌بازی‌ها، اتوماسیون خانگی (نور، هشدارهای آتش‌سوزی و غیره) و کنترل‌های از راه دور می‌شود. بسته به حوزهٔ کاربردی گره‌ها با باتری‌های AA باید بین یک ماه تا دو سال کار کنند. هدف‌گذاری برای گره‌ها این گونه است که قیمتی کم‌تر از ۵ دلار داشته باشند، در باند 2.4GHz ISM کار کنند و نرخ دادهٔ بین ۱۱۵ و ۱۰ کیلو بیت بر ثانیه در هر گره ارائه کنند. حداکثر تعداد گره‌ها ۲۵۵ است. اخیراً کارگروه IEEE 802.15 یک فعالیت استانداردسازی آغاز کرده [۱] که سعی می‌کند یک استاندارد شبکهٔ شخصی (PAN) تعریف کند. اولین نوع آن (802.15.1) مبتنی بر بلوتوث است و باید مشخصات فعلی را بهبود و گسترش دهد. هدف استاندارد 802.15.3 نرخ دادهٔ بالای 20Mbps یا بیش‌تر است. اخیراً زیگبی به صورت IEEE 802.15.4 استانداردسازی شده است. باندهای فرکانس پذیرفته‌شده برای آن 868/915MHz و 2.45GHz است. برد ارتباطی ۷۵ متر است. در این استاندارد ارتباطات می‌تواند فقط بین یک ارباب (گرهٔ اصلی) و ۲۵۰ برده (گرهٔ فرعی) برقرار گردد.

- **سیستم عامل.** سیستم عامل‌ها در ارتباطات بی‌سیم جاسازی شده باید بیش از پیش در معماری‌های نرم‌افزاری و سخت‌افزاری ناهمگن مجموعه‌ای از محدودیت‌های سخت را (نظیر تأمین نیرو و عملکرد بلادرنگ) برآورده سازند. در این حوزه مشخص است که هدف کلی مرسوم سیستم عامل‌ها کارآمد یا در بسیاری موارد کافی نیست. در میان جدیدترین سیستم‌عامل‌های گرهٔ حسگر می‌توانیم به TinyOS اشاره کنیم [۱۱۳]. TinyOS یک محیط زمان اجرای مبتنی بر مولفه است که به منظور ارائه پشتیبانی برای سیستم‌های عمیقاً جاسازی شده طراحی شده‌اند. این سیستم‌ها

مستلزم عملیات فشردهٔ همزمان هستند و در عین حال محدود به حداقل منابع سخت‌افزاری می‌شوند [۱۱۳]. مزیت اصلی TinyOS اندازهٔ کد کوچک آن است که از این رو به خوبی با گره‌های حسگر مجهز به حداقل سخت‌افزار تناسب دارد. زمان‌بند اصلی سیستم‌عامل فقط ۱۷۸ بایت حافظه را اشغال می‌کند، در انجام کپی برای گسترش رویدادها ۱.۲۵ بایت و در انجام کپی برای تغییر محتوا ۶ بایت حافظه می‌گیرد و زمان‌بندی دوسطحی را پشتیبانی می‌کند. این سیستم‌عامل برای شبکهٔ چند جهشی[5] متشکل از گره‌های ثابت طراحی شده است. سیستم عامل مورد بحث سیستمی متمرکز است؛ ایستگاه پایه دریافت داده‌ها و ارتباط بین دو گره را انجام می‌دهد. TinyOS یک سیستم عامل توان‌آگاه است. سیکل ساعتِ (چرخهٔ زمانی) به‌کارنرفته در مد خواب صرف می‌شود. مؤلفه‌های نرم‌افزاری بدین منظور نوشته می‌شوند که کار خود را انجام دهند و به مد خواب (غیر فعال) بروند. اگر داده‌ای دریافت شود، این رویداد به کامپوننت مربوطه با سیگنال خبر داده می‌شود. مؤلفه‌های نرم‌افزاری همچنین می‌توانند برای اجرای وظایف (بلوک‌های کد که برای تکمیل اجرا می‌شوند) از زمان‌بند وظایف درخواست کنند. این سیستم عامل می‌تواند نقطهٔ آغازی برای دیگر سیستم عامل‌های عمومی‌تر باشد که فرض می‌کنند: (۱) هیچ ایستگاه پایه‌ای وجود ندارد، (۲) گره‌ها سیار هستند. سیستم‌عامل‌های جایگزین دیگر شامل موارد زیر می‌شود: Microsoft Windows CE [۱۱۶]، سیستم عامل کوچک شده که به خصوص به گفتهٔ مایکروسافت برای «ابزارهای اطلاعاتی»[6] طراحی شده‌اند؛ Palm OS [۱۱۷]؛ و Redhat eCos [۱۱۸]، یک سیستم عامل منبع‌باز بلادرنگ که زیرساخت پایهٔ ران‌تایم با ردپاهای حافظه در فضای ذخیره‌سازی محدود ارائه می‌کند.

5. *Multi-hop*
6. *information appliances*

۱.۱.۳- محدودیت‌ها

شبکهٔ حسگر بی‌سیم شبکه‌ای خاص است که در مقایسه با شبکه‌های کامپیوتری سنتی محدودیت‌هـای بسـیاری دارد. به خاطر این محدودیت‌ها به‌کارگیری مسـتقیم روش‌های امنیتی موجود در حوزهٔ شـبکه‌های حسگر بی‌سیم دشوار است. بنابراین، به منظور توسعهٔ مکانیزم‌های امنیتی مفید و در عین حال بهره‌گیری از ایده‌های تکنیک‌های امنیتی موجود، لازم است ابتدا این محدودیت‌ها درک و شناخته شوند [۳۰].

۱.۱.۳.۱- منابع بسیار محدود

تمام رویکردهای امنیتی برای پیاده‌سـازی مسـتلزم مقدار معینی منابع هستند، شامل حافظهٔ داده‌ها، فضای کد، و انرژی مورد نیاز برای تأمین نیروی حسگر. به هرحال، در حال حاضر این منابع در حسگرهای بی‌سیم کوچک بسیار محدود هستند:

- یک نوع حسگر رایج (TelosB) دارای پردازندهٔ ۱۶ بیتی ۸ مگاهرتزی RISC با تنها 10K رم، 48K حافظهٔ برنامه و 1024K منبع ذخیره‌سـازی فلش اسـت [۱۱۹]. با چنین محدودیتی، نرم‌افزار ساخته‌شـده برای حسگر نیز باید کوچک باشد. فضای کد کلی TinyOS، سیسـتم عامل استاندارد بالفعل برای حسگرهای بی‌سیم، تقریباً 4K است [۱۱۳]، و زمان‌بند اصلی آن فقط ۱۷۸ بایت فضا اشغال می‌کند. بنابراین، اندازهٔ کد برای تمام کدهای امنیتی مرتبط نیز باید کوچک باشد.
- محدودیت توان. انرژی از بزرگ‌ترین محدودیت‌های حسگر بی‌سیم به شمار می‌رود. چنین فرض می‌کنیم که وقتی گره‌های حسـگر در شبکهٔ حسگر پیاده‌سازی شدند نمی‌توانند به سـادگی جایگزین (هزینهٔ عملیاتی بالا) یا شـارژ مجدد (هزینهٔ بالای حسگرها) شوند. بنابراین، شارژ باتری آن‌ها باید حفظ شود تا عمر تک‌تک گره‌های حسـگر و کل شبکهٔ حسـگر افزایش یابد. هنگام پیاده‌سازی یک قابلیت یا پروتکل رمزنگاری در گرهٔ حسگر، تأثیر انرژی کد امنیتی اضافه‌شده باید مد نظر قرار گیرد. وقتی به گرهٔ حسـگر امنیت را اضافه می‌کنیم، تأثیر آن امنیت بر طول عمر حسگر را (یعنی عمر باتری‌اش) مورد توجه قرار می‌دهیم. توان اضافی که توسـط گره‌های

حسگر به خاطر امنیت مصرف می‌شود با فرآیند مورد نیاز برای قابلیت‌های امنیتی (مثل رمزنگاری، رمزگشـــایی، امضاء داده‌ها، اعتبارسنجی امضاها)، انرژی مورد نیاز برای انتقال داده‌های مرتبط با امنیت یا سربار (مثل بردارهای اولیهٔ مورد نیاز برای رمزنگاری/رمزگشـــایی)، و انرژی مورد نیاز برای ذخیره‌سازی پارامترهای امنیتی به شکلی ایمن (مثل ذخیره‌سازی کلید رمزنگاشتی) در ارتباط است.

۱.۱.۳.۲- ارتباطات اطمینان‌ناپذیر

ارتباطات اطمینان‌ناپذیر تهدیدی دیگر در امنیت حســگر قلمداد می‌شود. امنیت شبکه شدیداً به پروتکل تعریف‌شده اتکا دارد که بدین ترتیب به ارتباطات بستگی دارد:

- **انتقال اطمینان‌ناپذیر**. به طور معمول مسیریابی مبتنی بر بسته در شبکهٔ حسگر بدون اتصال و از این رو ذاتاً اطمینان‌ناپذیر است. بسته‌ها ممکن است به خاطر خطاهای کانال آســیب ببینند یا در گره‌های بســیار فشرده کاهش یابند. در نتیجه بسته‌ها از بین می‌روند یا گم می‌شــوند. افزون بر این، کانال ارتباطی بی‌ســیم اطمینان‌ناپذیر باعث آســیب به بسته‌ها می‌شود. نرخ خطای بالاتر کانال نیز توسعه‌دهندهٔ نرم‌افزار را مجبــور می‌کند تا منابعی را برای کنتــرل خطا اختصاص دهد. از این مهم‌تر،اگر پروتکل فاقد کنترل خطای مناسب باشد، احتمال دارد بسته‌های امنیتی حیاتی از دست برود. این بسته‌ها ممکن است مثلاً شامل کلید رمزنگاری شود.
- **تداخل‌ها**. حتی در صورت قابل اطمینان بودن کانال، ممکن است ارتباط همچنان اطمینان‌ناپذیر باشــد. این امر به خاطر ماهیت همه‌پخشــی[۷] شبکهٔ حسگر بی‌سیم اســت. اگر بســته‌ها در حین انتقال با یکدیگر مواجه شوند تداخل روی خواهد داد و خود انتقال انجام نخواهد شــد. این موضوع در یک شــبکهٔ حســگر شلوغ (تراکم بالا) می‌تواند منجر به مشکلات بزرگی شود. جزئیات بیش‌تر دربارهٔ تأثیر ارتباطات بی‌سیم در منبع [۳] یافت می‌شود.

7. *broadcast* - برودکست

- **تأخیر**. مسیریابی چند جهشی، تراکم شبکه و پردازش گره می‌تواند منجر به تأخیر بیش‌تر در شـــبکه شود؛ بنابراین، باعث می‌شـــود دستیابی به همگام‌سازی در میان گره‌های حسگر دشوارتر گردد. ممکن است مسائل همگام‌سازی برای امنیت حسگر حیاتی باشـــد، چون در این حســـگر مکانیزم امنیتی بر گزارش رویدادهای حیاتی و توزیع کلید رمزنگاری اتکا دارد. مســـائل ارتباطات بلادرنگ شـــبکه‌های حسگر در منبع [۲۰۸] مورد بحث قرار گرفته‌اند.

۱.۱.۳.۳- عملیات بدون مراقبت

بســـته به کارکرد شبکهٔ حســـگر به‌خصوص، گره‌های حســـگر ممکن است مدتی بدون مراقبت رها شوند. سه هشدار اصلی در ارتباط با گره‌های حسگر بدون مراقبت وجود دارد:

- **در معرض حملات فیزیکی بودن**. حسگر ممکن است در محیطی در معرض مهاجمین، آب‌وهوای بد و غیره قرار گیرد. احتمال این که یک حســـگر در چنین محیطی در معرض حملهٔ فیزیکی قرار گیرد، خیلی بیش‌تر از کامپیوترهای شخصی است که در فضایی امن قرار گرفته‌اند و اساساً با حملاتی از شبکه مواجه می‌شوند.

- **مدیریت از راه دور**. مدیریت از راه دور شبکهٔ حسگر باعث می‌شود تشخیص مداخله و دستکاری فیزیکی (یعنی از طریق محافظ‌های دستکاری) و مسائل نگه‌داری فیزیکی (مثلاً جایگزین کردن باتری) تقریباً غیر ممکن شود. احتمالاً غیرمتعارف‌ترین مثال در این باره گرهٔ حســـگر به کار رفته برای مأموریت‌های دیده‌وری (شناسایی) پشت خطوط دشمن اســـت. در چنین مواردی، ممکن است گره پس از پیاده‌سازی هیچ تماس فیزیکی‌ای با نیروهای خودی نداشته باشد.

- **نبود نقطهٔ مدیریت مرکزی**. شـــبکهٔ حسگر می‌تواند از نوع شبکهٔ توزیعی بدون نقطهٔ مدیریت مرکزی باشد. این موضوع باعث افزایش انرژی شبکهٔ حسگر می‌شود. به هر حال، اگر به درســـتی طراحی نشـــود سازماندهی شبکه را دشوار، ناکارآمد و ضعیف می‌سازد.