به نام خدا

ارائه یک معماری جهت ارتباطات امن در شبکه های حسگر بی سیم در بدن

مولف :

ساناز رضا علیزاده یکتا

انتشارات ارسطو

(سازمان چاپ و نشر ایران – ۱۴۰۳)

نسخه الکترونیکی این اثر در سایت سازمان چاپ و نشر ایران و اپلیکیشن کتاب رسان موجود می باشد

chaponashr.ir

سرشناسه : رضا علیزاده یکتا، ساناز، ۱۳۵۵
عنوان و نام پدیدآور : ارائه یک معماری جهت ارتباطات امن در شبکه های حسگر بی سیم در بدن/ مولف ساناز رضا علیزاده یکتا.
مشخصات نشر : انتشارات ارسطو (سازمان چاپ و نشر ایران)، ۱۴۰۳.
مشخصات ظاهری : ۱۲۶ ص.
شابک : ۲-۷۳۶-۴۰۸-۶۲۲-۹۷۸
وضعیت فهرست نویسی : فیپا
موضوع : شبکه های حسگر بی سیم - ارتباطات امن - معماری
رده بندی کنگره : LB۳۰۲۴
رده بندی دیویی : ۳۷۱/۱۰۳۵
شماره کتابشناسی ملی : ۹۹۰۴۳۴۶
اطلاعات رکورد کتابشناسی : فیپا

نام کتاب : ارائه یک معماری جهت ارتباطات امن در شبکه های حسگر بی سیم در بدن
مولف : ساناز رضا علیزاده یکتا
ناشر : انتشارات ارسطو (سازمان چاپ و نشر ایران)
صفحه آرایی، تنظیم و طرح جلد: پروانه مهاجر
تیراژ : ۱۰۰۰ جلد
نوبت چاپ : اول - ۱۴۰۳
چاپ : زبرجد
قیمت : ۱۲۶۰۰۰ تومان
فروش نسخه الکترونیکی - کتاب‌رسان :
https://chaponashr.ir/ketabresan
شابک : ۲-۷۳۶-۴۰۸-۶۲۲-۹۷۸
تلفن مرکز پخش : ۰۹۱۲۰۲۳۹۲۵۵
www. chaponashr. ir

انتشارات ارسطو
چاپ و نشر ایران
Chaponashr.ir

تقدیم به:

پدر و مادر عزیزم

فهرست

فصل اول:

مقدمه

مقدمه

دستگاه‌های پوشیدنی در زندگی ما روز به روز رایج تر می‌شوند. امروز به همراه داشتن دستگاه‌های محاسباتی متعدد، مانند تلفن‌های هوشمند، پخش کننده‌های موسیقی و دوربین برای مردم، امر غیر معمولی نیست؛ مردم به طور فزآینده، دستگاه‌های الکترونیکی را برای اندازه گیری فعالیت فیزیکی، برای تعامل داشتن با دستگاه‌های محبوب و یا برای نظارت کردن بر امور فیزیولوژی خود (به عنوان مثال، یک بیمار قلبی که در مورد ضربان نامنظم قلب خود نگران است و یا یک بیمار دیابتی که می‌خواهد میزان قند خون خود را مدیریت نماید) حمل و نگه داری کرده و یا می‌پوشند. ممکن است این دستگاه‌های پوشیدنی[1] غیر قابل رویت باشند، امکان پیگیری بسیاری از شرایط مرتبط با شیوه زندگی و سلامت را در سطح بی سابقه‌ای از جزئیات به طور مداوم و یا دوره‌ای فراهم آورند. اتصال بی‌سیم، تعامل با دیگر دستگاه‌های نزدیک (به عنوان مثال، سیستم‌های محبوب، سیستم‌های کنترل آب و هوا و یا دستگاه‌های پزشکی) به اشتراک گذاری خودکار داده‌های حسگر با یک سرویس شبکه‌های اجتماعی یا (در مورد نرم افزارهای سلامت) سیستم پرونده سلامت شخصی یک کاربر و یا یک سیستم پرونده الکترونیک سلامت برای بررسی توسط یک ارائه دهنده مراقبت‌های بهداشتی را امکان پذیر می‌کند.

با پیشرفت تکنولوژی در حوزه‌های سلامت انتظار می‌رود که شبکه‌های بی‌سیم ناحیه بدن مربوط به دستگاه‌های پوشیدنی، نظارت سلامت در محل، کمک‌های شخصی، شخصی سازی و اتوماسیون خانگی را در اختیارمان قرار دهد. با فراگیر شدن دستگاه‌ها، امکان

[1] Wearable devices

ارتباط با دستگاه‌های مختلف برقرار می‌شود. یعنی به جای سیستم‌های حسگر پوشیدنی اطراف بدن و انتقال آن توسط ابزارهای انتقال، استفاده از حسگرهای استانداردی است که داده‌های خود را به صورت بی‌سیم به دستگاهی مانند تلفن‌های هوشمند (در حال حاضر در دست بسیاری از مردم امروز دیده می‌شود) مخابره کند. با این حال، این حضور فراگیر حسگرهای بی‌سیم به همراه ویژگی‌هایی که آنها درک و مشاهده می‌کنند، مشکلات امنیتی و حریم خصوصی بسیاری را به ارمغان می‌آورد.

شیوه‌های زندگی بی تحرک خطرات بالقوه‌ی از قبیل فشار خون بالا، بیماریهای قلبی، دیابت و مانند آن را افزایش داده است و همچنین فقدان مراقبت‌های بهداشتی با کیفیت به افزایش خطرات کمک می‌کند. با توجه به ماهیت غیر قابل پیش‌بینی اوضاع در یک شخص، نظارت مستمر و منظم در فرد اولویت بالایی دارد.

شبکه‌های ناحیه بدن بی‌سیم یک نوع از شبکه‌های حسگر بی‌سیم هستند که یک گروه از حسگرها بر روی بدن فرد قرار می‌گیرد و پارامترهای فیزیولوژیکی خاص را اندازه می‌گیرد و بیمارستان یا مرکز پزشکی آن‌ها را نظارت می‌کنند. این نظارت توسط شبکه سلولی یا اینترنت با استفاده از دستیاران دیجیتال فردی

(PDA[1]ها) یا تلفن‌های سلولی به عنوان وسایل واسطه‌ای انجام می‌گیرد. بنابراین شبکه‌های ناحیه بدن بی‌سیم به نظر می‌رسد یک راه‌حل امیدوارکننده برای مشکل نظارت بر سلامت مستمر باشد. با این حال امنیت داده سلامت فرد بیمار بسیار مهم است. برای دستیابی به امنیت در هر شبکه‌ای پیام‌های منتقل شده باید با استفاده از طرح‌های رمزنگاری تخصصی و یک کلید رمز نگاری، رمز نگاری شوند و در قسمت دریافت کننده رمز گشایی انجام گیرد. بسیاری از راهکارهای امنیتی که برای تامین امنیت شبکه استفاده می‌شوند نمی‌توانند در شبکه‌های ناحیه بدن بی‌سیم استفاده شوند. از آنجایی که ابزارهای حسگر کوچک روی شخص قرار می‌گیرد دارای محدودیتهای قدرت سخت‌گیر و محدودیتهای منابع هستند بنابراین راهکارهای امنیتی که در محاسبات استفاده از منابع

[1] PDA: Personal Digital Assistant

ساده هستند و در عین حال به امنیت مورد نظر دست می‌یابند مهم می‌شوند. از آنجایی که اطلاعات مهم مرتبط بر روی بدن فرد برای ایستگاه‌های نظارت و تصمیم‌گیری‌های مهم براساس این داده‌ها انتقال می‌دهند، امنیت در شبکه‌های ناحیه بدن بی‌سیم یک مسئله حیاتی است.

فصل دوم :

کلیات

مقدمه

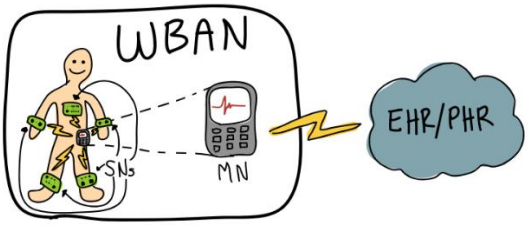
راه‌حلهای این مشکلات با دو ملاحظه در ذهن طراحی شده بودند. ملاحظه اول، اینکه شبکه‌ای از این دستگاه‌های پوشیدنی وجود دارد (یعنی، بیش از یک دستگاه وجود دارد) و ملاحظه دوم، اینکه قابلیت استفاده، نگرانی بزرگتری بود. این فصل برای درک بهتر زمینه‌ای که این راه‌حلها در آن توسعه یافتند، منظور مان از این دو ملاحظه را شرح می‌دهد و نوع خاصی از دشمن و تهدید را که ما قصد کاهش آنها را داریم، رسما اعلام می‌کند. همچنین به معرفی چند اصطلاح در مورد تکنیک‌های یادگیری ماشین که ما استفاده می‌کنیم، می‌پردازد.

درباره‌ی شبکه‌ی ناحیه بدن

ما معتقدیم که حسگرهای موجود در این دستگاه‌های پوشیدنی به وسایل مناسبی تبدیل خواهند شد. آنها با یکدیگر و با سایر دستگاه‌هایی که مردم با آنها حمل می‌کنند، مانند تلفن‌های هوشمند به درستی کار خواهند کرد. تصور می‌کنیم که در آینده، تلفن‌های هوشمند با «یک معماری سلامت تلفن همراه که امنیت قوی و تضمین حفظ حریم خصوصی را فراهم می‌آورد» جایگزین خواهند شد که ما آن را Amulet می‌نامیم [۱]. یک فرد چندین نوع مختلف حسگر (به عنوان مثال، نظارت بر فشار خون، پالس اکسی متر، گام شمار، سنجش‌گر گلوکز خون) را می‌پوشد و به دلیل نیازهای فیزیولوژیکی و یا راحتی، این حسگر لزوما در مکان‌های مختلف بدن متصل می‌شود. این حسگرها در درجه اول با یکدیگر و سایر دستگاه‌ها از طریق چند رسانه بی‌سیم ارتباط برقرار خواهند کرد.

قطب {هاب} مرکزی این شبکه همه داده‌های دریافت شده از حسگرها را ذخیره و جمع آوری خواهد کرد. در واقع، امروزه ساخت چنین سیستمی امکان پذیر است زیرا آنها حسگرهای پزشکی و تناسب اندام هستند که به صورت تجاری در دسترس بوده و قادر به برقراری ارتباط با تلفن‌های هوشمند از طریق بلوتوث هستند.

این شبکه‌ی دستگاه‌های پوشیدنی را شبکه ناحیه بدن بی‌سیم [۱] می‌نامند. شکل ۲-۱ چنین شبکه‌ای را به تصویر می‌کشد. در شبکه ناحیه بدن بی‌سیم، یک فرد یک یا چند گره حسگر [۲]، مانند یک ناظر گلوکز خون، گام شمار یا حسگر قلب نگاری الکتریکی، بر روی بدن خود می‌پوشد و یک گره منفرد موبایل مانند یک تلفن هوشمند یا Amulet به کمرش وصل می‌کند. گره موبایل [۳]و گره حسگر در محدوده نزدیک به بدن (به طور معمول، کمتر از ۲ متر) در یک شبکه‌ای با توپولوژی ستاره بطور بی‌سیم ارتباط برقرار می‌کند. اگر مطلوب باشد، این شبکه ناحیه بدن بی‌سیم می‌تواند با چند روال بک-اند [۴]که از اتصال به اینترنت گره‌های موبایل استفاده می‌کنند، ارتباط برقرار نماید. با این حال به جای اتصال به اینترنت مربوط به گره موبایل بیشتر با خود شبکه ناحیه بدن بی‌سیم در ارتباط هستیم.



شکل ۱-۰- اجزای یک شبکه بی‌سیم ناحیه - بدن.

[۱] Wireless Body Area Network :WBAN
[۲] Sensor Node :SN
[۳] Mobile Node: MN
[۴] Back-end: یک برنامه یا نرم افزار بک-اند به طور غیر مستقیم در پشتیبانی از سرویسهای فرانت-اند خدمت رسانی می‌کند.

بسیاری از SN ها بطور بی‌سیم با گره موبایل مرکزی ارتباط برقرار می‌کنند. گره موبایل قادر به ارسال اطلاعات از SNها به یک برنامه کاربردی در ابر است (مانند یک پرونده الکترونیک سلامت یا پرونده سلامت شخصی).

در شبکه ناحیه بدن بی‌سیم، فرض می‌کنیم که گره موبایل قادر به برقراری ارتباط با چند سیستم سرویس روال بک-اند (به عنوان مثال، یک پرونده‌های الکترونیک سلامت و یا پرونده سلامت شخصی) است. از سوی دیگر، گره‌های حسگر، منابع محاسباتی و انرژی محدود دارند و به این ترتیب، تنها قادر به برقراری ارتباط با گره‌های موبایل هستند. علاوه بر این، فرض می‌کنیم که گره‌های حسگر زمانی که به یک فرد متصل می‌شوند، توانایی تشخیص را دارند (اگر چه ممکن است ندانند که به چه کسی وصل شدند). برای مثال، یک گره حسگر، ممکن است حاوی مداری باشد که تکمیل شده است. به عنوان مثال، زمانی که یک فرد تسمه گره حسگر را به بدن خود می‌بندد، دو سر یک گردنبند و یا مچ بند، هم شرکت می‌کنند و مدار را تکمیل می‌نمایند.

می توان گره‌های حسگر را به یکی از دو دسته زیر تقسیم نمود: شخصی و مشترک. یک گره حسگر شخصی به طور انحصاری توسط یک فرد استفاده می‌شود (به عنوان مثال، یک ناظر گلوکز خون پوشیدنی). یک گره حسگر مشترک می‌تواند توسط چند نفر استفاده شود (به عنوان مثال، یک ناظر تناسب اندام). گره‌های حسگر می‌توانند با استفاده مورد نظر خودشان طبقه‌بندی شوند. برای مثال، گره حسگر زودگذر، حسگری است که یک فرد به صورت پراکنده و نامنظم از آن استفاده می‌کند (به عنوان مثال، ترازوی دیجیتال بی‌سیم). این نوع از گره‌های حسگر تمایل دارند که در محیط تعبیه شوند به طور معمول اجازه می‌دهند چند نفر از آنها استفاده کنند (اگر چه می‌تواند گره‌های حسگرهای شخصی، زودگذر مانند یک ناظر گلوکز خون وجود داشته باشد). از سوی دیگر، گره‌های حسگر مستمر حسگرهایی هستند که یک فرد به طور مداوم آنها را می‌پوشد (به عنوان مثال، یک

ناظر تناسب اندام). این گزارش سمینار در درجه اول مرتبط با این نوع از گره‌های حسگر است زیرا آنها به طور مداوم توسط مردم مورد استفاده قرار می‌گیرند.

ما فرض می‌کنیم گره‌های موبایل و گره‌های حسگر با موجودیت‌های زیر تعامل دارند: تولید کننده، یک کاربر و ارائه دهنده خدمات. تولید کننده موجودیتی است که به تولید حسگرها می‌پردازد و آنها را بین ارائه دهنده خدمات و کاربران توزیع می‌کند. کاربر فردی است که از گره موبایل و گره‌های حسگر برای دریافت اطلاعات در مورد سلامت خود استفاده می‌کند. به طور معمول، کاربران یک گره موبایل و گره حسگر را یا به طور مستقیم از تولید کننده و یا از یک ارائه دهنده خدمات دریافت می‌کنند. کاربران همچنین حق انتخاب دارند یا می‌توانند برای مشاوره، این اطلاعات را به یک ارائه دهنده خدمات بفرستند و یا می‌توانند داده‌های محلی را برای نظارت بر خود نگه دارند. ارائه دهنده خدمات موجودیتی است که خدماتی مانند پیکربندی حسگرها، تجزیه و تحلیل داده‌های دریافتی و ارائه مشاوره به کاربران را فراهم می‌کند. به عنوان مثال، ارائه دهنده خدمات می‌تواند یک بیمارستان، ارائه دهنده پرونده سلامت شخصی [۱]، یک سازمان خانه‌های بهداشت و یا چند کسب و کار دیگر یا سایر ارائه دهندگان خدمات باشد.

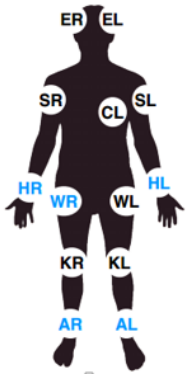
شبکه‌های بی‌سیم ناحیه بدن مدت‌های مدیدی است که توسط محققان و اغلب تحت عنوان‌های مختلف (به عنوان مثال، شبکه‌های حسگر ناحیه بدن و شبکه‌های شخصی) مورد مطالعه قرار گرفته اند [۲] [۳]. موسسه مهندسان برق و الکترونیک (IEEE) گروه مامور اجرای عملیات شش ۸۰۲. ۱۵ یک شبکه بدن-ناحیه را به صورت «یک استاندارد ارتباطی بهینه سازی شده برای دستگاه‌های کم قدرت و عمل بر روی، در داخل یا اطراف بدن انسان (اما محدود به انسانها نیست) برای اینکه انواع برنامه‌های کاربردی از جمله پزشکی، لوازم الکترونیکی مصرف کننده / سرگرمی شخصی و دیگران را ارائه نماید» به

[۱] personal health record :PHR

طور رسمی تعریف می‌کند [٤]. با این وجود، در حالی که لایه‌های فیزیکی، کنترل دسترسی متوسط و شبکه‌های زیربنایی جالب هستند، ما قدر و ارزش آنها را نمی دانیم زیرا در درجه اول معتقدیم که ارائه مکانیزم‌های امنیتی قابل استفاده برای نوع بی‌سیم شبکه‌های ناحیه بدن حائز اهمیت است.

مکان‌های مورد توجه

نقاط زیادی در بدن شما وجود دارد که می‌توانید یک SN را به آن بپوشانید. شکل ۲-۲ چند مکان احتمالی را بطور گرافیکی به تصویر می‌کشد. مکان‌های مشخص شده - دست چپ (HL)، دست راست (HR)، مچ پای چپ (AL)، مچ پای راست (AR)، کمر راست (WR) – مکانهایی را نشان می‌دهند در این گزارش سمینار بررسی کردیم. قابل ذکر است، ما نقاط واقع در قسمت بالای بدن را بررسی نکردیم. به عنوان مثال، سر شما محلی است که ممکن است یک SN را روی آن قرار دهید (به عنوان مثال، [٥]). به همین ترتیب، اگر بخواهید قلب خود [٦] و یا تعداد تنفس [٧] را نظارت کنید، ممکن است یک SN را در سمت چپ قفسه سینه (CL) قرار دهید علاوه بر این، برخی از حسگرها به گونه‌ای طراحی می‌شوند که روی بازو قرار بگیرند (به عنوان مثال، [٨]). ما این مکان‌های دیگر را به کار آینده محول می‌کنیم.



شکل ۲-۰- نقاط مجاز قرار گیری SN