INSO
17520
1st.Edition
2014

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۷۵۲۰
چاپ اول
۱۳۹۳

سری X : شبکه‌های داده‌ها، امنیت و ارتباطات سامانهِ باز
خدمات و کاربردهای ایمن- امنیت شبکهِ حس‌گرِ همه‌جاگاه- الزامات امنیتی برای مسیریابیِ شبکهِ حس‌گرِ بی‌سیم

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY
Secure applications and services – Ubiquitous sensor network security – Security requirements for wireless sensor network routing

ICS: 35.110

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«سری x : شبکه‌های داده‌ها، امنیت و ارتباطات سامانه باز-خدمات و کاربردهای ایمن- امنیت شبکهِ حس‌گر همه‌جاگاه -الزامات امنیتی برای مسیریابی شبکه حس‌گر بی‌سیم»

رئیس :	**سمت و/ یا نمایندگی**
ابراهیمی آتانی، رضا (دکتری مهندسی برق، الکترونیک)	دانشکده فنی، دانشگاه گیلان
دبیر :	
فرمان آرا، شایسته (کارشناسی مهندسی کامپیوتر، نرم افزار)	سازمان ملی استاندارد ایران
اعضاء : (اسامی‌به ترتیب حروف الفبا)	
بابایی، سارا (کارشناس مهندسی کامپیوتر، نرم افزار)	کانون زبان ایران
پاکدامن، مریم (کارشناس مهندسی کامپیوتر، نرم افزار)	اداره کل استاندارد استان گیلان
جعفری، بیتا (کارشناسی ارشد مهندسی فناوری اطلاعات، شبکه های کامپیوتری)	آموزش و پرورش استان گیلان
حسنی کرباسی، امیر (کارشناس ارشد مهندسی فناوری اطلاعات، شبکه های کامپیوتری)	کارشناس
سولاری اصفهانی، ندا (کارشناس ارشد مهندسی فناوری اطلاعات، شبکه های کامپیوتری)	دانشگاه پیام نور استان تهران
طهوری، سامان (کارشناس ارشد مهندسی فناوری اطلاعات، شبکه های کامپیوتری)	کارشناس
عزیزی، زهرا (کارشناس فناوری اطلاعات)	کارشناس
فرمان آرا، نفیسه (کارشناس مهندسی برق، الکترونیک)	کارشناس

فهرست مندرجات

پیش‌گفتار

استاندارد «سری X : شبکه‌های داده‌ها، امنیت و ارتباطات سامانه باز-خدمات و کاربردهای ایمن- امنیت شبکه حس‌گر همه‌جاگاه -الزامات امنیتی برای مسیریابی شبکه حس‌گر بی‌سیم» که پیش نویس آن در کمیسیون‌های مربوط توسط سازمان ملی استاندارد تهیه و تدوین شده است و در سیصد و سی و سومین اجلاسیه کمیته ملی استاندارد رایانه و فرآوری داده مورخ۹۳/۰۱/۳۰ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی‌و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینه صنایع ، علوم و خدمات ، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین ، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد .

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

ITU-T X:1313:2012,SERIES X: DATA NETWORKS, OPEN SYSTEM-COMMUNICATIONS AND SECURITY-Secure applications and services – Ubiquitous sensor network security – Security requirements for wireless sensor network routing

مقدمه

این استاندارد الزامات امنیتی را برای مسیریابی شبکه حس‌گر بی‌سیم فراهم می‌سازد. این استاندارد هم‌بندی‌های شبکه عمومی و پروتکل‌های مسیریابی را در شبکه‌های حس‌گرِ همه‌جاگاه[1]، توضیح می‌دهد. به علاوه، این استاندارد تهدیدات امنیتی پیش روی شبکه‌های حس‌گر بی‌سیم را، تحلیل می‌کند.

در این استاندارد، عبارت «مدیریت/سرپرستی[2]» برای ایجاز و اختصار استفاده می‌شود تا هم مدیریت مخابراتی را نشان دهد و هم یک بنگاه/دفتر/نمایندگی[3] عملیاتی به رسمیت شناخته شده را،مشخص نماید.

انطباق[4] با این استاندارد داوطلبانه[5] است. اگرچه، این استاندارد مجاز است حاوی تمهیدات[6] اجباری[7] معین (به طور مثال برای تضمین هم‌کنش پذیری[8] یا قابلیت کاربری[9]) باشد و انطباق با این استاندارد زمانی حاصل می‌شود که تمامی این مقررات اجباری برآورده شوند. واژه‌های «باید[10]» یا برخی زبان‌های الزامی دیگر همچون «می‌باید[11]» و معادل‌های منفی آن برای اظهار الزامات به کار می‌روند. استفاده از این کلمات بر این نکته اشاره ندارد که انطباق با این استاندارد، توسط هر طرفی الزامی‌است[12].

1- Ubiquitous.
2 -Adminstration.
3 -Agency.
4- Compliance.
5 -Voluntary.
6 -Provision.
7- Mandatory.
8- Interoperability.
9- Applicability.
10 -Shall.
11 -Must.
12 -Is required of any party.

سری x : شبکه‌های داده‌ها، امنیت و ارتباطات سامانه باز-خدمات و کاربردهای ایمن- امنیت شبکه حس‌گر همه‌جاگاه - الزامات امنیتی برای مسیریابی شبکه حس‌گر بی‌سیم

۱ هدف و دامنه کاربرد

هدف ار تدوین این استاندارد تعیین الزامات امنیتی برای مسیریابیِ شبکهِ حس‌گرِ بی‌سیم است و موارد زیر را پوشش می‌دهد:

- هم‌بندی‌های شبکه عمومی و پروتکل‌های مسیر یابی برای شبکه‌های حس‌گر بی‌سیم (WSN)[1].
- تهدیدات امنیتی که مسیریابی WSN با آن‌ها مواجه است.
- الزامات امنیتی برای مسیریابی WSN.

۲ مراجع الزامی

مدارک الزامی‌زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آنها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن موردنظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره تاریخ تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است .

استفاده از مراجع زیر برای این استاندارد الزامی‌است :

2-1- ITU-T X.800:1991, Recommendation ITU-T X.800 (1991), Security architecture for Open Systems Interconnection for CCITT applications.

2-2- ITU-T X.805:2003, Recommendation ITU-T X.805 (2003), Security architecture for systems providing end-to-end communications.

۲-۳-استاندارد ملی ایران شماره۱۷۵۱۹سال ۱۳۹۳،[2] فناوری اطلاعات- مخابرات و تبادل اطلاعات بین سامانه‌ها – چهارچوب کاریِ امنیت برای شبکه‌های حس‌گرِ همه جاگاه

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می‌روند:

۳-۱ اصطلاحات تعریف شده در مستندات دیگر

در این استاندارد اصطلاحات و تعاریف زیر که در مستندات دیگر تعریف شده‌اند، به‌کار می‌رود:

۳-۱-۱

1 -Wireless sensor network.

۲ -بر اساس منبع استاندارد بین المللی: ISO/IEC 29180: 2012

اصالت‌سنجی[1]

به اصالت‌سنجی مبدا داده‌ها و اصالت‌سنجی هستارِ همتا[2] در ITU-T X.800 مراجعه شود.
[ITU-T X.800]

۳-۱-۲

محرمانگی[3]

خاصیتی که، اطلاعات، دردسترسِ اشخاص، هستارها یا فرآیندهایی که اصالت‌سنجی نشده‌اند، قرار نمی‌گیرد، یا برای آن‌ها آشکار نمی‌شود.
[ITU-T X.800]

۳-۱-۳

یکپارچگی[4] داده‌ها

خاصیتی که، داده‌ها به شیوه‌ای غیرمجاز[5] ، تغییر نیافته یا از بین نمی‌روند.
[ITU-T X.800]

۳-۱-۴

کلید

کلید، دنباله‌ای از نمادها که، عملیات پوشیده‌سازی[6] و واپوشیده‌سازی (پوشیده خوانی) [7]را واپایش[8] می‌کند.
[ITU-T X.800]

۳-۱-۵

حس‌گر

حس‌گر، افزاره‌ای[9] الکترونیکی است که یک شرایط فیزیکی یا ترکیب شیمیایی را حس می‌کند و یک نشانک[10](سیگنال) الکترونیکی، متناسبِ مشخصهِ مشاهده شده، آزاد می‌کند.
[b-ITU-T Y.2221]

۳-۱-۶

شبکه حس‌گر

1- Authentication.
2 -Peer-entity.
3 - confidentiality.
4- Integrity.
5 -Unuthorized.
6 -Encipherment.مغشوش کردن و درهم کردن داده‌ها یا تبدیل آنها به رمز به‌نحوی‌که معنای داده برای گیرندهٔ غیرمُجاز قابل درک نباشد
7 -Decipherment.فرایند تبدیل داده‌های درهم و پوشیده به داده‌های روشن
8 -Control.
9 -Device.
10 -Signal.

شبکه حس‌گر، شبکه‌ای است شامل گره‌های حس‌گر، که در اتصال متقابل هستند و داده‌های حس شده توسط گره‌های حس‌گر توسط ارتباط باسیم یا بی‌سیم مبادله[1] می‌شوند.

[b-ITU-T Y.2221]

۳-۱-۷

تهدید [2]

تهدید، پتانسیلِ[3] شکستن[4] امنیت است.

۳-۱-۸

شبکه حس‌گر همه‌جاگاه (USN)[5]

یک شبکه مفهومی[6] که بر روی شبکه‌های فیزیکی موجود ایجاد می‌شود و از داده‌های حس‌شده توسط حس‌گر استفاده کرده و خدماتِ دانش را برای هرکس، در هر مکان و در هر زمان، و در جایگاهی که اطلاعات، با بافت آگاهی[7] تولید می‌شود، فراهم می‌سازد.

[b-ITU-T Y.2221]

۳-۲ اصطلاحات تعریف شده در این استاندارد

این استاندارد، اصطلاحات زیر را تعریف می‌کند:

۳-۲-۱

فعال‌گر[8]

دریافت و فرستادنِ[9] داده‌های حس‌شده، است.

۳-۲-۲

بردارِ فاصله به هنگامِ تقاضای موردی (AODV)[10]

یک پروتکل مسیریابیِ به هنگام تقاضا، است که مسیرها[11] را، در شبکه‌های حس‌گر بی‌سیم و شبکه‌های موردی بی‌سیم، برپایهِ «هنگام نیاز[12]» کشف می‌کند. AODV، مسیرها را، با استفاده از چرخهِ پرسمانِ[13]

---

1 -Exchange.
2 -Threat.
3 -Potential.
4 -violation.
5 -Ubiquitous sensor network.
6 -Conceptual.
7 -Context awareness.فنّاوری توانمندساز سامانه‌های همه‌جاگاه
8 -Actuator.سازوکاری که باعث روشن یا خاموش یا تنظیم شدن یا به حرکت درآمدن یک دستگاه می‌شود
9 -Transmit.
10 -Ad hoc on-demand distance vector.
11 -Routs.
12 - As-needed
13 -Query.

درخواست مسیر (RREQ)[1] و پاسخ مسیر (RREP) [2]می‌سازد. هنگامی‌که یک گره مبدا، تمایل مسیری[3] به مقصدی را دارد، که در حال حاضر برای آن مسیری ندارد، یک بستهِ درخواست مسیر (RREQ) را در سرتاسر شبکه پخش همگانی[4] می‌کند. گره‌هایی که این بسته را دریافت می‌کنند، در در جداول مسیر، اطلاعات خود را برای گره مبدا، روزآمد[5] کرده و اشاره‌گرهای پس‌سو[6]، به سمت گره مبدا را تنظیم می‌کنند.

۳-۲-۳

یکپارچگی گره

خاصیتی که گره، به یک شیوه غیرمجاز[7] ، تغییر نیافته یا از بین نمی‌رود.

۴-۲-۳

مسیریابی

فرآیندی برای برقراری[8] پیوند[9] ارتباطی بین گره‌های حس‌گر است. مسیریابی شامل مشخص کردن مسیر و انتقال اطلاعات از طریق شبکه است.

۵-۲-۳

گرهِ شبکه حس‌گر

افزاره‌ایی با حداقل یک حس‌گر و همچنین، هیچ یا یک فعال‌گر با توانمندیِ ۱) استفاده از داده‌های حس‌گرِ داخلی برای واپایشِ هر فعال‌گرِ موجود، یا ۲) ارسال داده‌های حس‌گر و دریافت فرمان‌های[10] فعال‌گر در شبکه، است.

۶-۲-۳

هم‌بندی[11]

آرایشِ فیزیکی و منطقی عناصر یک شبکه حس‌گر است. یک شبکه حس‌گر بی‌سیم (WSN)[12]، با مجموعه‌ای از گره‌های حس‌گر و دروازه‌ها، نمایانده می‌شود که توسط پیوندهای بی‌سیم به هم متصل شده‌اند.

۷-۲-۳

شبکه حس‌گر بی‌سیم (WSN)

---

1 -route request.
2 -route response.
3 -Desires a route. بهترین مسیر بین مبدأ و مقصد
4 -Broadcast.
5 -Update.
6 -Backward.
7 -Authorized.
8 -Establishing.
9 -Association.
10- Commands.
11 -Topology.
12 -Wireless sensor network.

شبکه ای که متشکل است از یک ایستگاه پایه[1] و تعداد زیادی گره‌های حس‌گر با قابلیت انتقال بی‌سیم در دامنهِ شبکهِ حس‌گرِ USN است.

۴ کوته نوشت‌ها و سرنام‌ها

ACQUIRE	Active query forwarding In sensor networks	هدایت(پیشسوییِ) پرسمانِ فعال در شبکه‌های حس‌گر
AES	Advanced Encryption Standard	استاندارد رمزبندیِ پیشرفته
AODV	Ad hoc On-demand Distance Vector	بردارِ فاصله به هنگام تقاضایِ موردی
APTEEN	Adaptive Periodic Threshold-sensitive Energy-Efficient sensor Network protocol	پروتکل شبکه حس‌گر با کاراییِ انرژی با آستانهِ حساسیتِ متناوبِ وفقی
BS	Base Station	ایستگاه پایه
CADR	Constrained Anisotropic Diffusion Routing	مسیریابی پخشِ ناهمگرای مزاحم (متداخل)
CDMA	Code Division Multiple Access	دسترسی چندگانه ی با تقسیم کد
CH	Cluster Head	راسِ خوشه
DAG	Directed Acyclic Graph	نگاشتِ غیر مدور مستقیم
DAM	Distributed Aggregate Management	مدیریت انبوهشِ توزیع شده
DC	Data-Centric	داده محور
DODAG	Destination Oriented DAG	DAG مقصد گرا
DOS	Denial of Service	بندآوردی خدمات
EBAM	Energy-Based Activity Monitoring	پایشِ فعالیت مبتنی بر انرژی
EMLAM	Expectation-Maximization Like Activity Monitoring	بیشینه سازی انتظار مانند پایشِ فعالیت
GBR	Gradient-Based Routing	مسیر یابی مبتنی بر شیب
GPS	Global Positioning System	سامانه موقعیت یابی جهانی
ID	Identity	هویت
IDS	Intrusion Detection System	سامانه آشکارسازیِ نفوذ
IDSQ	Information-Driven Sensor Querying	پرسمان اطلاعاتی حس‌گر
IPS	Intrusion Prevention System	سامانه پیش گیری از نفوذ
LEACH	Low Energy Adaptive Clustering Hierarchy	سلسله مراتب خوشه بندی وفقی با انرژی کم
LML	Local Markov Loops	حلقه‌های مارکوف محلی
MAC	Medium Access Control	واپایشِ دسترسی محیط

1 -Base station.

MAC	Message Authentication Code	کد اصالت‌سنجی پیام
MCFA	Minimum Cost Forwarding Algorithm	الگوریتم پیشسویی(هدایت) کمینه هزینهِ
MECN	small Minimum Energy Communication Network	شبکه ارتباطی کوچک با کمینه انرژی
OS	Operating System	سامانه عامل
PEGASIS	Power-Efficient Gathering in Sensor Information Systems	جمع آوری با کاراییِ توان در سامانه‌های اطلاعاتی حس‌گر
PHY	Physical	فیزیکی
RPL	IPv6 Routing Protocol for Low-power and Lossy networks	پروتکل مسیریابی پروتکل اینترنت نسخه شش (IPV6) برای شبکه‌های با توان پایین و با اتلاف
RREP	Route Reply	پاسخ مسیر
RREQ	Route Request	درخواست مسیر
RTLS	Real-Time Locating Systems	سامانه‌های مکان یابی بی‌درنگ
SN	Sensor Network	شبکه حس‌گر
SOP	Self-Organizing Protocol	پروتکل خودسازماندهی
SPIN	Sensor Protocols for Information via Negotiation	پروتکل‌های حس‌گر برای اطلاعات از طریق مذاکره
TDMA	Time Division Multiple Access	دسترسی چندگانه با تقسیم بندی زمان
TEEN	Threshold-sensitive Energy-Efficient sensor Network protocols	پروتکل‌های شبکه حس‌گر با کاراییِ انرژی با آستانهِ حساسیت
TPM	Trusted Platform Module	پودمان سکوی قابل اعتماد
USN	Ubiquitous Sensor Network	شبکه حس‌گر همه‌جاگاه
WSN	Wireless Sensor Network	شبکه حس‌گر بی‌سیم
WPAN	Wireless Personal Area Network	شبکه بی‌سیم منطقه شخصی

۵ قراردادهها

کلمات کلیدی[1] «مستلزم این است[2]» الزامی را نشان می‌دهد که، درصورتی که انطباق با این استاندارد، مورد ادعا باشد، باید به شدت از آن پیروی شود، و هیچ انحرافی از آن مجاز نیست.

کلمات کلیدی «توصیه می‌شود[3]» الزامی را نشان می‌دهد که، توصیه می‌شود[4]، اما کاملا الزامی نیست. بنابراین این الزام برای ادعای انطباق ارایه نمی‌شود.

1 -Keywords.
2 -Is required to.
3 -Is recommended.
4 -Recommended.

کلمات کلیدی «ممنوع است[1]» الزامی را نشان می‌دهد که، درصورتی که انطباق با این استاندارد، مورد ادعا باشد، باید به شدت از آن پیروی شود، و هیچ انحرافی از آن مجاز نیست.
کلمات کلیدی «می تواند به صورت اختیاری[2]» و «مجاز است[3]» الزامی را نشان می‌دهد که، اختیاری است و بدون هیچ دلالتی بر توصیه آن، مجاز است. این اصطلاحات بر آن دلالت ندارد که پیاده‌سازی‌های فروشنده، گزینه[4] و و ویژگیی خاصی[5] را، که توسط فراهم‌کنندگان خدمت/کارور به طور اختیاری می‌تواند فعال شود را، می‌باید فراهم‌کند. بلکه به معنای آن است که فروشنده، آن ویژگی خاص را به صورت اختیاری، مجاز است فراهم کرده و همچنان خواستار انطباق با آن ویژگی[6] باشد.

۶ خصوصیاتِ هم‌بندی‌هایِ شبکه عمومی و پروتکل‌های مسیریابی در رابطه با ملاحظات امنیتی برای شبکه‌های حس‌گر بی‌سیم (WSN)

یک WSN، می‌تواند از بیش از یک ایستگاه پایه، و چندین حس‌گر تشکیل شود. ایستگاه پایه می‌تواند گره‌ای سیمی با منابع بسیار، یا گره‌ای سیار با باتری‌ها و منابع رایانشیِ کمتری باشد. حس‌گرها ممکن است از انواع ذره‌ای[7] و فقط برای حسِ داده‌ها باشند و یا ممکن است اطلاعات حس شده را، مسیردهی یا ذخیره نمایند. برای مثال، یک سر خوشه یا گره والد، منابع رایانشیِ بیشتری برای جمع‌آوری اطلاعات حس شده، و برای فعال ساختن مسیریابی، نسبت به حس‌گرهای فرزند، درهم بندیِ یک شبکه پیکربندی شده، دارد.

۶-۱ ویژگی‌های کلی مسیریابی در پیکربندیِ هم‌بندیِ شبکه

مسیریابی با یک رویهِ کشفِ همسایه آغاز می‌شود. در WSNها، ایستگاه (های) پایه و بسیاری از حس‌گرها، همسایه هستند. رویه کشف، با توجه به ارتباطِ هر گره در ساختِ هم‌بندیِ شبکه ، متفاوت است. افزونگی[8] و سیار بودنِ ایستگاه پایه نیز باید در نظر گرفته شود.

۶-۲ هم‌بندی‌های شبکه عمومی‌در WSN

گره‌های WSN به طور معمول، به صورت یکی از سه نوعِ هم‌بندیِ شبکه، سازمان‌دهی می‌شوند: هم‌بندی ستاره-ای[9]، هم‌بندی درخت[10] یا هم‌بندی توری[11]. شکل ۱ سه نوع پایهِ هم‌بندیِ شبکه را نشان می‌دهد. در هم‌بندی ستاره‌ای، هر گره، به‌طور مستقیم، به یک گره مرکزی[12]، که ایستگاه پایه نامیده می‌شود، متصل است.
در شبکه بندی ستاره‌ای، تمام حس‌گرها، در ارتباطِ با ایستگاه پایه‌شان ، هستند. بنابراین کشفِ همسایه، بین ایستگاه پایه و حس‌گرها شکل می‌گیرد. ایستگاه پایه، حضورش[13] را توسط هویتش (ID)[14] و اطلاعات موقعیت-

1 -Is prohibited from.
2 -Can optionally.
3 -May.
4 -Option.
5 - Feature.
6 -Specification.
7 -Dust types
8 -Redundancy.
9- Star.
10 -Tree.
11 -Mesh.
12 -central node.
13 - Existence.
14 -Identity.

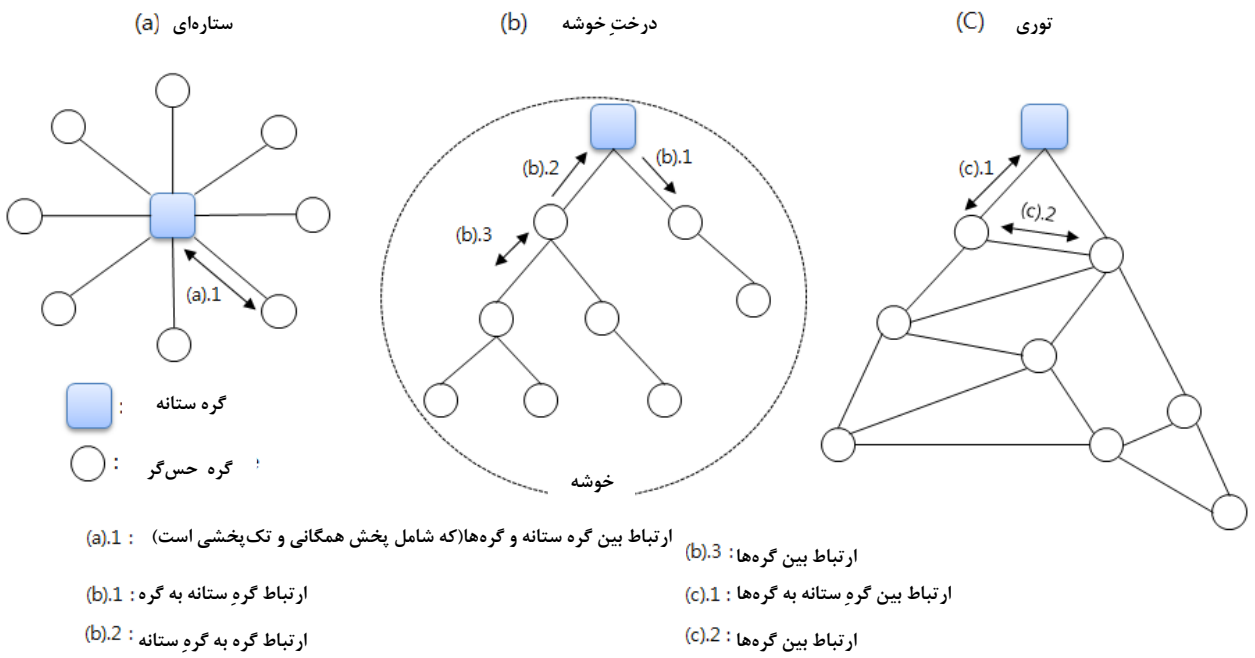
اش، اعلان[1] می‌کند، و حس‌گرها، ثبتِ پاسخشان را با هویتشان، به ایستگاه پایه می‌فرستند. برای نگاه‌داری[2] فعال وضعیت[3] شبکه، وضعیت جاری، بین ایستگاه پایه و حس‌گر مبادله می‌شود. چنانچه ایستگاه پایه یا هر حس‌گری، خراب[4] شود، متوقف شود[5] یا جابه‌جا[6] شود، کشف همسایه آغاز می‌شود. در نتیجه بهتر است برای کشف همسایه، بسته‌های واپایشی[7]، با توجه به جنبه‌های امنیتی، در نظر گرفته شوند. در یک شبکه درخت خوشه‌ای، ایستگاه پایه و حس‌گرها، حضور خود را با شناساندن خود به یکدیگر اعلان می‌کنند، به این ترتیب، شبکه درخت، پیکربندی می‌شود. در این حالت، حس‌گرهای میانی، به نسبت حس‌گرهای برگ، که مسئول حسِ داده‌ها از حس‌گرها هستند، دارای باتری‌ها و منابع رایانه‌ای بیشتری برای مسیریابی به سمت گره‌های والدشان یا به سمت ایستگاه پایه هستند.

در یک شبکه با همبندی توری، حداقل دو گره وجود دارند، که دو یا تعداد بیشتری مسیر، در بین آن‌ها وجود دارد. این نوع همبندی به بیشترِ انتقال‌ها اجازه می‌دهد که توزیع شده باشند، هرچند که ممکن است نگاه‌داریِ ارتباطات افزونه بین گره‌ها، سخت و پر هزینه باشد، اما به دلیل مسیرهای چندگانه اطمینان‌پذیر[8] است.

حس‌گرها خود را اعلان می‌کنند و درخواست همسایگانی که در فاصلهِ یک مرحله‌ایشان[9] هستند را، می‌کنند، و با سایر حس‌گرها یا ایستگاه(های) پایه به وسیلهِ انتشارِ[10] یک مرحله‌ایِ ممکنِ خود، تاحدودی یا به طور کامل، در ارتباط هستند. یک همبندیِ توری به نسبت همبندیِ درخت، به حس‌گرهایی با باتری‌ها و منابع رایانشیِ بیشتری نیاز دارد. کشف دوره‌ایِ همسایه، برای نگاه‌داریِ یک شبکه توری نیاز است.

در برخی از موارد، همبندیِ ترکیبی[11] وجود دارند که ترکیبی از حداقل دو نوع از سه نوع همبندیِ پایه به همراهِ خوشه بندی[12] هستند. در چنین مواردی، خوشه بندی به شکلِ یک یا بیش از سه همبندیِ شبکه، پیکربندی خواهد شد.

1- Advertise.
2- Maintain.
3 -Status.
4 -fail.
5 -Shut down.
6- Move.
7 -Control packet.
8-Reliable.
9 -One hop
10 -Propagation.
11 -Hybrid.
12 -Clustering.



شکل ۱- سه همبندیِ شبکه عمومی برای یک ایستگاه بر پایه WSN

۶-۳ خصوصیات پروتکل‌های مسیریابی در WSN

۶-۳-۱ ویژگی‌های کلیِ ویژگی‌های تنظیم و برپاییِ مسیریابی

در همبندیِ ستاره‌ای، نیازی به تنظیم و برپاییِ مسیریابی نیست زیرا حس‌گرها داده‌های حس‌شده را، فقط به ایستگاه پایه‌شان می‌فرستند. نشانی[1]، یک نشانیِ پروتکلِ اینترنتِ نسخه شش (IPV6) از 6lowpan ، یک نشانیِ ZigBee[2]، یا یک هویت تعریف شده توسط کاربر، برای تحویل بسته خواهد بود.

در یک همبندیِ توری و درخت، که شامل خوشه بندی است، هر حس‌گر، مسیر خود را به سمت ایستگاه پایه‌اش، برای تنظیم و برپاییِ جدول مسیریابی، پس از کشف مسیر، می‌یابد. در این قدم، اجرای عملیات پیوستن[3] و ترک کردنِ[4] درخت[5]، از یک گره والد[6]، توسط حس‌گرها[7]، با در نظر گرفتنِ ایستگاه پایه، به عنوان گره ریشه[8]، شکل می‌گیرد. به‌علاوه، گره والد، جدول مسیریابی را برای روزآمد کردنِ[9] وضعیت جاری، به طور دوره‌ای یا به هنگام تقاضا[10] واپایش می‌کند. هر گره به گره بالاتر[11] در درخت و سپس به ایستگاه پایه متصل می‌شود، و داده‌ها، از گره برگ، و از طریق چندین گره میانی، به سمت ایستگاه پایه –که همبندیِ درخت را تشکیل می‌دهند-مسیردهی می‌شوند. در شبکهِ همبندیِ درخت، یک طرح[12] مسیریابی سلسله

---

1 -Address.

۲ -به کتابنامه مراجعه شود.

3 -Join.
4 -Leave.
5 -Tree.
6 -Parent node.
7 -Sensors.
8 -Root node.
9- Update.
10-On-demand.
11 -Higher node.
12- Scheme.

مراتبی می‌تواند پیاده‌سازی شود. همچنین، نشانیی، برای تحویل بسته‌ها میانِ حس‌گرها به ایستگاه پایه، استفاده می‌شود. نشانی برای تحویل بسته‌ها استفاده می‌شود.

در این مرحله، هویت‌هایشان (ID) و مقادیر سنجهِ مسیریابی‌شان، که می‌تواند شامل وضعیت باتری، تاخیر انتشار، مکان، یا پهنای باند شبکه باشد، استفاده می‌شوند. بنابراین، بهتر است بسته‌های واپایشی، که دربرگیرنده اطلاعات مسیریابی، ID و راه مسیریابی هستند، برای امنیت در نظر گرفته شوند.
به طور خاص برای شبکه‌بندی درخت و خوشه‌بندی، یک گره والد و راس خوشه[1]، وجود دارد. که راس و والد، کارکرد انبوهشِ[2] داده‌ها و مدیریت گره‌های فرزند را انجام می‌دهند بنابراین، بهتر است امنیت آن‌ها با دقت بیشتری در نظر گرفته شود.
جدول ۱ ملاحظات امنیتی فوق را برای ویژگی‌های مسیریابی خلاصه می‌کند:

جدول ۱- ملاحضات امنیتی برای اقدامات مسیریابی

همبندی	اهداف امنیت				پروتکل‌های موجود	ملاحظات
	گره	کشف همسایه	تنظیم و برپاییِ مسیریابی	تحویل بسته		
ستاره ای	ایستگاه(های) پایه/ حس‌گرها	بسته‌های واپایش اعلان، که به صورت دوره‌ای چکانه شده و جابه‌جا می‌شوند، و دربرگیرندهِ ID و مکان، به همراه بسته‌های ثبتِ BS توسط حس‌گرها هستند.	N/A	نشانی، ID ، داده‌ها، گره بعدی	Zigbee [b-Zigbee], IEEE 802.16.4 [b-IEEE 802.1.6.4]	
درخت/ خوشه	ایستگاه(های) پایه/ حس‌گرهای والد (حس‌گرهای راس خوشه)، حس‌گرهای فرزند	بسته‌های واپایش اعلان، که به صورت دوره‌ای چکانه شده و جابه‌جا می‌شوند، و دربرگیرندهِ ID و مکان، به همراهِ BS و گره‌های والد هستند.	بسته‌های پیوستن و ترک کردن، که دربرگیرندهِ مقادیر سنجهِ مسیریابی، بین گره‌های والد و فرزند، با همراهِ یک گره ریشه، به عنوان BS، در فازِ بازسازی، آغازکردن و جابه‌جایی.	نشانی، ID ، داده‌ها، گره بعدی، جدول مسیریابی	پروتکل LEACH [b-Heinzelman] PEGASIS [b-Lindsey], TEEN and APTEEN [b-Manjeshwar-1], [b-Manjeshwar-2], MECN [b-Rodoplu], SOP[b-Subramanian], مسیریابی انبوهشی حس‌گر [b-Fang]	

1- Head cluster.
2 -Aggregation.

جدول ۱- ادامه

	SPIN [b-Chandrakasan], [b-Kulik], پخش هدایت شده (مستقیم) [b-Intanagonwiwat], مسیریابی شایعه [b-Braginsky], MCFA [b-Ye], مسیریابی برپایه شیب [b-Schurgers], ACQUIRE [b-Sadagopan], مسیریابی آگاه به از انرژی [b-Shah], پروتکل‌های مسیریابی با قدم‌زدنِ(گردش‌های) تصادفی [b-Servetto]	نشانی، هویت، داده‌ها، گره بعدی، جدول مسیریابی	بسته‌های تنظیم و برپایی مسیریابی، دبرگیرندهِ مقادیر سنجه مسیریابی، در فاز بازسازی،آغاز کردن و جابه‌جایی	بسته‌های واپایشِ اعلان، از ایستگاه‌های پایه و حس‌گرهای دربرگیرندهِ مکانِ هویت.	ایستگاه (های) پایه/ حس‌گرها	شبکه ای

۷ الزاماتی برای مسیریابی امن

در بند ۷-۱-۲ از ITU-T X.1311 تهدیدات امنیتی، و در بند ۹-۱ ابعاد امنیتیِ USN توصیف می‌شود، که شامل الزامات کارکردی در مورد اقدامات مسیریابی، همانند جدول ۱، است، و ابعاد امنیتی در بند ۹-۱ است. این این الزامات در بند ۱۱ از ITU-T X.131 نشان داده شده‌اند.

۷-۱ الزامات برای حس‌گر و ایستگاه پایه

برای مسیریابی امن، بهتر است هر گره حس‌گر و ایستگاه پایه، خود_اطمینان‌پذیر[1]باشد. هرچند ازآنجایی‌که حس‌گرها سبک[2] هستند، ملاحظات خاص اجرایی باید مورد توجه واقع شود تا ابعاد امنیتی برآورده شود. [ITU-T X.1311].

از آنجایی‌که ایستگاه پایه، از نظر اطلاعات ذخیره شده و مدیریت شبکه‌های WSN، قدرتمند تر از حس‌گرها است، بهتر است از حملات DOS و مداخله[3] فیزیکی حفظ شود، تا دسترس پذیری و اطمینان پذیری آن، تضمین شود. بنابراین، بهتر است سازوکار ضد مداخله[4] و عیبتابی[5] داشته باشد. همچنین، یک سامانه شناسایی نفوذ/پیشگیری از نفوذ (IDS/IPS)[6]یا یک دیوار آتش در شبکهِ باسیم یا بی‌سیم، به عنوان سامانه‌های جداگانه یا شکل‌های مجازی، فراهم خواهد آمد. الزامات برای هر حس‌گر و ایستگاه پایه، به شرح پیش رو خواهند بود:

1-Self-reliable.
2-Lightweight.
3-Tamper.
4-Tamper-proofing.
5 -Fault tolerance.بروز عیب باعث از کار افتادن فوری نمی‌شود
6-Intrusion Detection System/ Intrusion prevention System.

- ایستگاه پایه و حس‌گر، هرکدام، لازم است یک اصالت سنج و کلید برای شناسایی و اصالت‌سنجی یکدیگر در آغاز، داشته باشند.
- اطلاعات ذخیره شده در ایستگاه پایه و تمام حس‌گرها – به خصوص اطلاعاتِ در مورد داده‌های حس شده، ID، و مکان، مستلزمِ رمزبندی[1] و اصالت‌سنجی است.
- برای مقابله با حملات داخلی، توصیه می‌شود که ایستگاه پایه، یکپارچگی گره را ضمانت کند، همچون TPM .
- توصیه می‌شود که در ابتدا به ایستگاه‌های پایه، اجازهِ واپایشِ دسترسیِ فهرستِ گره حس‌گر، پیش از پیکربندی شبکه حس‌گر، داده شود.
- توصیه می‌شود که حس‌گر، ID را برای دسترسیِ واپایش، پیش از پیکربندی شبکه حس‌گر، احراز نماید.

توصیه می‌شود که ایستگاه پایه با توجه به دوگانگی[2] و جایگزینیِ هموار[3]، عیبتابی داشته باشد.

- توصیه می‌شود که ایستگاه پایه، دارای ساز وکار ضدِ مداخلهِ نصب شده در سخت افزارِ پشتیبانش، راه‌اندازیِ[4] امن، بهبود سامانه عامل(OS) ، و اصالت‌سنجی و اعتبار سنجی نرم افزار، به عنوان مثال با استفاده از فناوری TPM یا جعبه ایمنی باشد.
- حس‌گر می‌تواند به طور اختیاری عیبتاب و یا ضد مداخله باشد.
- از ایستگاه پایه، در صورتی که افزاره‌ای باسیم باشد، می‌توان به طور اختیاری توسط IDS/IPS و یا دیوار آتش محافظت شود.
- برای مقابله با حملات داخلی، حس‌گرها می‌توانند به طور اختیاری از یکپارچگی گره حمایت نمایند.

۲-۷ الزامات امنیتی برای رویه کشف همسایه

کشف همسایه می‌تواند از طریق پخش همگانی پیام‌ها از ایستگاه پایه، شروع شود. پس این بند، ابعاد امنیتی و تهدیدات پخش همگانی پیام‌ها از یک ایستگاه پایه به تمام گره‌های حس‌گر را در نظر می‌گیرد [ITU-T X.1311] . همچنین، حس‌گرها می‌توانند از روش پخش همگانی یک گامی[5] برای کشف همسایگانش استفاده کنند. پس از رویه، تمام ایستگاه‌های پایه و حس‌گرها، می‌توانند گروه‌های چند پخشی را برای ارتباطات کارا شکل دهند.

- لازم است ایستگاه پایه دارای یک روش مجاز با یک مقدار رازمانی[6]، برای حس‌گرها باشد. به طور مثال مقدار رازمانی اصالت سنجِ از پیش تعریف شده، محتوای کلید[7] و ID .

1- Encryption.
2 -Duplicate.
3-Smooth replacement.
4-Bootstrapping.
5 -One hop.
6 - Secrecy.
7 -Key material.

- لازم است هر حس‌گر یک سازوکار اصالت‌سنجی سبک را برای تایید یکدیگر، بپذیرد. اگر، پس از اصالت‌سنجی با ایستگاه پایه، گروه تشکیل شود، اصالت‌سنجی بر روی شناسانه[1] گروه شکل می‌گیرد و یک مقدارِ رازمانیِ عام با کلید گروهی آن‌ها، رمزبندی[2] می‌شود.
- لازم است، در زمانِ دریافت پیام‌های پخش همگانی، اصالت‌سنجی مبدا و پیام تایید شود. لازم است، یک پیامِ اعلان، در تمام گره‌های دیگر، اصالت‌سنجی شود.
- از آنجایی که این نوعی پاسخ، به پیامِ اعلان، از سوی حس‌گرها است، لازم است یک پیام تک پخشی در مبدا اصالت‌سنجی شود.
- برای ارتباط امن و به جهت حفاظت از ID، اطلاعات مکانی و منابع رایانشی، سازوکار مدیریت کلید و رمز بندی، برای اعلان و درخواست لازم است.
- حس‌گرهای میانی، می‌توانند به طور اختیاری مرجعِ استفاده از روش بازبینیِ[3] دسترسی سبکِ خود را، به همان روش اصالت سنجِ متداول گروه، بررسی کنند.

۳-۷ الزامات امنیتی برای نظیم و برقراریِ مسیریابی و تحویل بسته

الزامات امنیتی بسته به ابعاد امنیتی و تهدیدات ایجاد شده توسط حملات داخلی و خارجی، توصیف می‌شوند [ITU-T X.1311]. هنگامی‌که مسیری به ایستگاه پایه، تنظیم و برقرار می‌شود، یک سنجهِ مسیریابی مانند کوتاهترین مسیر[4] یا تاخیر می‌تواند مورد استفاده قرار گیرد، به علاوه ID والد یا راسِ خوش، می‌تواند به عنوانِ سنجهِ مسیریابی در روش و همبندیِ مسیریابیِ تعریف شده، مورد استفاده قرار گیرد. بازسازی مسیر هنگامی‌انجام می‌شود که ایستگاه پایه یا حس‌گرها جابه‌جا شوند، از بین بروند و یا تغییری در پیوستن و یا ترک کردنِ راس یا گره والد به شبکه حس‌گر، وجود دارد.

- لازم است ایستگاه پایه و تمام حس‌گرها، مجوز گره‌های همسایه شان را بازبینی کنند تا مشخص نمایند، کدام گره بعدی، برای برقراری ارتباط با ایستگاه پایه، خواهد بود. چنانچه راس خوشه‌ها یا گره‌های والد انتخاب شوند، اصالت‌سنجی گرهِ نماینده لازم است صورت گیرد تا با تغییر گره، از یک حمله چاهک ستانه (گودال)[5] ، جلوگیری شود.
- توصیه شده است در جریان اطلاعات مسیریابی، الزامی است که پیوستن و جداشدنِ پیام‌های پیکربندی مسیریابی، به هدفِ یکپارچگی و مجوز مبدا، به شیوهِ یک به یک تصدیق شوند. چنانچه طی فاز کشف همسایه، گروهی تشکیل شود، کلید اصالت‌سنجی می‌تواند کلید بزرگتری برای کارآیی بیشتر باشد.
- پیام‌هایِ پیکربندیِ شبکه، دربرگیرندهِ ID، مکان و اطلاعات سنجه . مستلزمِ حفاظت شدن، توسط روش‌های مدیریت کلید و رمز بندی هستند.

---

1 -Identifier.
2 -Encrypt.
3 -Check.
4-Shortest path.
5-Sinkhole.

- برای فراهم ساختنِ عیبتابی و اجتناب از حملات چاهک ستانه(گودال) یا کرمچاله[1] مسیرهای چندگانه برای ایستگاه پایه، می‌تواند به‌طور اختیاری، پیکربندی و با محتویات کلیدهای گوناگونی برای اصالت‌سنجی پیام و مبدا، رمزبندی، شود.
- توصیه می‌شود که، پس از کامل شدنِ تنظیم و برقراریِ مسیریابی، بسته‌ها با استفاده از سازوکارهای اصالت‌سنجی و رمزبندی و مدیریت کلید مناسب، رمزبندی و اصالت‌سنجی شوند. روش‌های رمزبندی و اصالت‌سنجی برای حس‌گرها به نسبت این روش‌ها برای ایستگاه‌های پایه، سبک تر هستند.
- هنگامی‌که رویه انبوهشِ داده‌ها توسط راسِ خوشه‌ها یا گره‌های والد صورت می‌گیرد، محتویاتِ کلید و روش‌های اصالت‌سنجی و رمزبندیِ تنظیم و برقراریِ مسیریابی یا تحویل داده‌ها، می‌توانند به طور اختیاری، در زیرگروه‌های خوشه بندی شده توسط راس‌ها یا والدها ، متفاوت باشند.

۷-۴ ابعاد و الزاماتِ امنیت برای مسیریابی امن

این بند کارکردهایی را تعریف می‌کند، که الزامات امنیتی را با ملاحظات عملکردی، برآورده می‌سازند. الزامات با طبقه بندی اهداف امنیتی در جدول ۱ توصیف می‌شوند. همچنین، این بند، به فنون امنیتی که در شبکه‌های حس‌گر همه‌جاگاه و الزامات ویژه امنیتی برای USNها که در [ITU-T X.1311]، استفاده می‌شوند، رجوع می‌کند.

۷-۴-۱ ایستگاه پایه و جنبه‌های حس‌گر

ایستگاه(های) پایه، می‌توانند، فهرستِ واپایشی دسترسی، به همراه مقدار رازمانیِ هرکدام و ID حس‌گرها را، برای بازبینیِ آغازینِ اصالت‌سنجیشان و اجازه‌شان[2]، به همراه اطلاعات کلید به اشتراک گذاشته شده، داشته باشند. کلید می‌تواند از پیش به اشتراک گذاشته شود یا توسط مقدار رازمانی یا طرفِ ثالث تولید شود. همچنین گره‌ها می‌توانند دارای قابلیت رمزبندی برای اطلاعات ذخیره شده باشند. ایستگاه(های) پایه و برخی از حس‌گرها برای انبوهش داده‌ها، بهتر است، برای حریم و محرمانگی، ذخیره سازی امن داشته باشند. ممکن است، برای اصالت‌سنجی و اجازه، مدیریت کلید، ایجاد دوباره کلید و لغو کلید گروهی، لازم باشد، مانند کلید یکتا[3] برای هر ذخیره امن. به طور خاص چنانچه، ایستگاه پایه با سیم[4] باشد، کارکردهای IPS/IDS می‌توانند فراهم شود.
ممکن است یک پودمان ضد مداخله و پودمانِ سکو برای گره‌ها برای جنبه‌های سخت افزاری مورد نیاز باشد.

1 -Wormhole.
2 -Authorization.
3 -Unique.
4 -Wire-lined.

جدول ۲- الزامات و ابعاد امنیت

ابعاد امنیتی	الزامات ویژه گره					
	رمزبندی	مدیریت کلید	ذخیره‌سازی ایمن	واپایش دسترسی آغازین، اصالت‌سنجی ، اجازه	ضد مداخله، TMP	IDS/IPS
واپایش دسترسی				Y		
اصالت سنجی	Y	Y		Y		
سلب انکار				Y		
محرمانگی	Y	Y	Y			
امنیت ارتباط	Y	Y	Y			
یکپارچگی داده‌ها	Y					
دسترس پذیری					Y	Y
حریم	Y	Y	Y			
برگشت‌پذیری در برابر حملات	Y				Y	Y

۷-۴-۲ جنبه‌های کشف همسایه

اعلانات اصالت‌سنجی‌شده، می‌باید پخش همگانی شوند. یک روش اصالت‌سنجی، برای ارسال آغازینِ اعلان فراهم می‌شود. در این جا، اطلاعاتِ ID، می‌تواند به طور گمنام، اصالت‌سنجی شود، یا در درونِ یک ID، که به طور پیوسته ،در حال تغییر است، با استفاده از یک زنجیره درهم سازی، پنهان شود. در مقابل، پیام ثبت، می‌تواند برای حفاظت از ID، مکان و اطلاعات سنجه مسیریابی، رمزبندی شود. در این جا، برای تحویل بسته، بهتر است محتویِ کلید از فاز کشف همسایه تا تنظیم و برقراریِ مسیریابی متفاوت باشد. بهتر است مدیریت کلید شامل کلید گذاریِ مجدد[1] و رویه‌های لغو باشد.

جدول ۳- الزامات و ابعاد امنیت

ابعاد امنیتی	الزامات کشف همسایه				
	رمزبندی	مدیریت کلید	اصالت‌سنجی مبدا و پیام	تازگی داده‌ها	TPM، عیبتابی
واپایش دسترسی			Y	Y	
اصالت‌سنجی		Y	Y	Y	
سلبِ انکار	Y	Y			
محرمانگی	Y	Y			
امنیت ارتباط	Y	Y			
یکپارچگی داده‌ها			Y	Y	
دسترس پذیری					Y
حریم	Y	Y	Y		
برگشت‌پذیری در برابر حملات					Y

1 -Rekeying.

۷-۴-۳ تنظیم و برقراریِ مسیریابی و جنبه‌های تحویل بسته

برای تنظیم و برقراریِ مسیریابی، با در نظر گرفتن خصوصیات ویژهِ همبندی، رویه‌هایی برای انتخاب و پیوستن/ترک‌کردنِ راس خوشه‌ها یا والدها، وجود دارند. از آنجایی که، تنظیم و برقراریِ مسیرها، ID، مکان و سنجه‌های مسیریابی، بهتر است پنهان یا رمزبندی شده و اصالت‌سنجی شده باشد، بنابراین بهتر است رویه‌های رمزبندی، ID ناشناس و مدیریت کلید، فراهم شوند. به طور خاص، مدیریت کلید، شامل ایجاد، کلید گذاریِ مجدد، و لغو، برای هر تنظیم و راه اندازیِ مسیریابی و تحویل بسته می‌شود.

جدول ۴- الزامات و ابعاد امنیت

ابعاد امنیتی	تنظیم و برقراریِ مسیریابی و الزاماتِ تحویلِ بسته					
	رمزبندی	مدیریت کلید	اصالت‌سنجی مبدا و پیام	تازگی داده‌ها	انبوهشِ ایمن داده‌ها	TPM، عیبتابی
واپایش دسترسی			Y	Y		
اصالت‌سنجی		Y	Y	Y	Y	
سلب انکار			Y			
محرمانگی	Y	Y			Y	
امنیت ارتباط	Y	Y			Y	
یکپارچگی داده‌ها			Y	Y	Y	
دسترس پذیری						Y
حریم	Y	Y	Y		Y	
برگشت‌پذیری دربرابر حملات						Y

پیوست الف

(الزامی)

مرورکلی پروتکل‌های مسیریابی حس‌گر بی‌سیم

الف- ۱ مثال‌هایی از پروتکل‌های مسیریابی موجود

سازوکارهای بسیاری برای مسیریابیِ شبکه‌های حس‌گر پیشنهاد شده‌اند. این سازوکارهای مسیریابی، خصوصیاتِ ویژهِ ذاتیِ شبکه‌های حس‌گر را درکنار الزامات کاربردی و همبندی مورد توجه قرار داده‌اند. وظیفهِ یافتن و نگاه‌داریِ مسیرها، در شبکه‌های حس‌گر، درضمنِ توجه به مصرف انرژی، اثربخشیِ[1] مسیریابی، اطمینان پذیریِ داده‌ها، و امنیت، بی اهمیت و جزیی نمی‌باشد.

موارد زیر پروتکل‌های مسیریابی موجود هستند.

-پروتکل‌های حس‌گر برای اطلاعات از طریق مذاکره (SPIN)[2] [b-Heinzelman] [b-Chandraksan] و [b-Kulik]

این پروتکل‌ها به خانواده‌ای از پروتکل‌های وفقی[3] اشاره دارد، که پروتکل‌های حس‌گر، برای اطلاعات از طریق مذاکره (SPIN) نامیده می‌شود که تمامِ اطلاعاتِ هر گره را، با فرض اینکه تمام گره‌ها در شبکه، به طور بالقوه، ایستگاه پایه هستند، به هر گره‌ای در شبکه منتشر می‌کند. این کاربر را قادر می‌سازد تا هر گره را مورد پرسمان قرار دهد و اطلاعات الزامی‌را به طور فوری بدست آورد. این پروتکل‌ها از این خاصیت که گره‌های در مجاورت نزدیک، دارای داده‌های مشابه هستند استفاده کرده، و از این رو، تنها نیاز به توزیع داده‌هایی است که گره‌های دیگر در اختیار ندارند.

-پخش هدایت شده (مستقیم) [b-Intanagonwiwat][4]

این پروتکل به یک نمونهِ[5] رایجِ انبوهشِ داده‌ها برای WSNها اشاره دارد که پخش هدایت شده (مستقیم) نامیده نامیده می‌شود. پخش هدایت شده (مستقیم) یک نمونهِ داده محور (DC) و آگاه از کاربرد است، به طوری که تمام داده‌های تولید شده توسط گره‌های حس‌گر، توسطِ جفت‌های مقدار-صفت نام گذاری می‌شود. ایده اصلیِ DC، ترکیب داده‌های آمده از منابع مختلف در مسیر (در انبوهشِ داخلِ شبکه) با حذف افزونگی و کم کردنِ تعداد انتقال‌ها است؛ از این رو انرژی شبکه حفظ و طول عمر آن افزایش می‌یابد. برخلاف مسیریابی سنتیِ انتها به انتها[6]، مسیریابی DC، مسیرها را از چندین مبدا تا یک تک مقصد می‌یابد که باعث تحکم شبکه از افزونگی داده‌ها می‌شود.

---

1 -Effectiveness.
2 -Sensor protocols for information via negotiation.
3 -Adaptive.
4 -Direct diffusion.
5 -Paradigm.
6 -End-to-end.

– مسیریابی شایعه [b-Branginsky][1]

مسیریابی شایعه گونه‌ای از پخش هدایت شده است و بیشتر برای کاربردهای که مسیریابی جغرافیایی، عملی نیست درنظر گرفته می‌شود. به طور کلی، پخش هدایت شده، زمانی که هیچ معیار جغرافیایی، برای پخشِ وظایف وجود ندارد، از به جریان انداختنِ[2] تزریقِ پرسمان، به کل شبکه استفاده می‌کند. اگرچه، در برخی موارد، فقط، میزان کمی داده‌ها، از گره‌ها درخواست شده است و از این رو استفاده از به جریان انداختن، غیرضروری است. یک رویکرد جایگزین درصورتی که تعداد رویدادها کم وتعداد پرسمان‌ها زیاد باشد، به جریان انداختنِ رویدادها است. ایده کلیدی، مسیردهی پرسمان‌ها به گره‌هایی است که یک رویداد مشخص را مشاهده می‌کنند، به جایِ، به جریان انداختنِ پرسمان‌ها در کلِ شبکه، برای بازیابی اطلاعات، درمورد رخ دادن رویداده‌ها است. به منظور به جریان انداختنِ رویدادها، در سرتاسر شبکه، الگوریتم مسیریابی شایعه، بسته‌های با طول عمر بالا، که عامل نامیده می‌شوند را، بکار می‌برد. زمانی که یک گره رویدادی را تشخیص می‌دهد، چنین رویدادی را به جدول محلی خود می‌افزاید، که جدول رویدادها نامیده می‌شود و یک عامل[3] را تولید می‌کند.

–الگوریتم پیشسوییِ (هدایتِ) کمینهِ هزینه(MCFA)[4] [b-Ye]

MCFA (الگوریتم پیشسوییِ کمینهِ هزینه) این حقیقت را بکار می‌گیرد که جهت[5] مسیریابی همیشه شناخته شده است، یعنی در جهت ایستگاهِ پایهِ ثابتِ خارجی. بنابراین یک گره حس‌گر، نیاز به داشتن یک ID یکتا یا نگاه‌داریِ یک جدول مسیریابی ندارد. در عوض، هر گره کمترین هزینه تخمین زده شده از خود به ایستگاهِ پایه را، نگاه‌داری می‌کند. هر پیامی‌که، توسطِ گره حس‌گر پیشسو (هدایت) می‌شود، برای همسایگانش نیر پخش همگانی می‌شود. زمانی که یک گره پیامی‌را دریافت می‌کند، بازبینی می‌کند که آیا خودش، در کم هزینه‌ترین مسیر میان گره حس‌گر مبدا و ایستگاهِ پایه قرار گرفته است یا نه. درصورتی که به این ترتیب باشد، پیام را برای همسایگانش دوباره پخش همگانی می‌کند. این فرآیند تا زمانی که به ایستگاه پایه برسد، تکرار می‌شود.

–مسیریابی مبتنی بر شیب (GBR)[6] [b-Schurgers]

این مسیریابی به گونه دیگری از پخش هدایت شده (مستقیم) اشاره می‌کند، که مسیریابی مبتنی بر شیب (GBR) نامیده می‌شود. ایده کلیدی، در GBR، زمانی که *توجهی*[7] در سراسر شبکه پخش شده است، به خاطر سپردنِ تعداد گام‌ها[8] است. به این صورت هر گره، می‌تواند پارامتری را که ارتفاع گره نامیده می‌شود، که کمینهِ شماره گام‌ها برای رسیدن به ایستگاه پایه (BS) است را، محاسبه می‌کند.

---

1 - Rumour routing.
2 -Flooding.
3 -Agent.
4 -Minimum cost forwarding algorithm.
5 -Direction.
6 -Gradient-based routing.
7 -Interest.
8 -Hops.

-پرسمان اطلاعاتی[1] حس‌گر (IDSQ)[2] و مسیریابی پخش ناهمگرای مزاحم(متداخل) (CADR)[3] [b-Chu]

دو فن مسیریابی، یعنی پرسمان اطلاعاتی حس‌گر (IDSQ) و مسیریابی پخش ناهمگرای مزاحم پیشنهاد شده‌اند [b-Chu]. هدفِ CDAR، شکل کلیِ پخشِ هدایت شده (مستقیم) است. ایده کلیدی، پرسمانِ حس‌گرها و مسیردهی داده‌ها در شبکه است، به طوری که در شرایطی که، تاخیر و پهنای باند کمینه است، به‌دست آوردنِ اطلاعات بیشینه باشد. CADR پرسمان‌ها ، با استفاده از مجموعه‌ای از معیارهای اطلاعاتی پخش می‌کند، تا انتخاب کند که چه حس‌گرهای می‌توانند داده‌ها را بدست آورند. که این موضوع، تنها با فعال‌سازی حس‌گرهای نزدیک به یک رویداد خاص، که به طور پویا مسیرهای داده‌ها را تنظیم می‌کنند، حاصل می‌شود. تفاوت عمده، میان این سازوکار با پخش هدایت شده (مستقیم)، مد نظر قرار دادنِ بهرهِ اطلاعاتی[4] به علاوهِ نرخ ارتباطی[5] است. در CADR، هر گره، یک هدف اطلاعات/هزینه را ارزیابی می‌کند و داده‌ها را برمبنای شیبِ اطلاعات/هزینه و الزاماتِ کاربر نهایی، مسیردهی می‌کند. در IDSQ، گره پرسمان‌گر، می‌تواند تعیین کند که کدام گره می‌تواند مفیدترین اطلاعات را با مزیتِ افزودهِ متوازن کردنِ هزینه انرژی فراهم سازد. به هر جهت، IDSQ به طور خاص نحوه چگونگیِ مسیردهیِ پرسمان و اطلاعات را، میان حس‌گرها و BS، مشخص نمی‌کند. بنابراین IDSQ می‌تواند به عنوان یک رویه بهینه سازی مکمل دیده شود. اگرچه نتایج شبیه سازی شده، نشان داده‌اند که این رویکردها نسبت به پخش هدایت شده (مستقیم)، که در آن پرسمان‌ها به روشی همگرا پخش می‌شوند و ابتدا به نزدیک ترین همسایه می‌رسند، کارایی انرژی بیشتری دارند.

-COUGRA [b-Yao]

پروتکل داده محور دیگر، پروتکل COUGAR نامیده می‌شود که براساس نویسنده آن نام گذاری شده است؛ این پروتکل شبکه را به عنوان یک سامانه دادگانِ[6] توزیع شده عظیم در نظر می‌گیرد. ایده کلیدی، استفاده از پرسمان‌های اخباری به منظور خلاصه کردن پردازش پرسمان از کارکردهای لایه شبکه است، مانند انتخاب حس‌گرهای مرتبط و غیره، COUGAR از انبوهشِ داده‌های درون شبکه‌ای، برای حصول صرفه جویی بیشتر در انرژی بهره می‌برد. خلاصه کردن، توسطِ یک لایه پرسمان افزوده، که میان لایه‌های کاربرد و شبکه قرار می‌گیرد، تامین می‌شود. COUGAR، یک معماری را برای سامانهِ دادگان حس‌گر، که در آن گره‌های حس‌گر یک گره راهنما[7] را برای اجرای انبوهش و انتقال داده‌ها به BS انتخاب می‌کنند را، دربر می‌گیرد. BS مسئول تولیدِ طرحِ پرسمان است که اطلاعات ضروری را درمورد جریان داده‌ها و رایانشِ درون شبکه، برای پرسمان وارده، مشخص می‌کند وآن را به گره‌های مرتبط، ارسال می‌کند. طرحِ پرسمان، همچنین نحوه انتخاب راهنما را برای پرسمان شرح می‌دهد. این معماری یک توانایی رایانشی درون شبکه‌ای را، که می‌تواند اثربخشیِ انرژی را، در موقعیت‌هایی

1-Information-driven.
2 -Information-driven sensor quering.
3 -Constrained anisotropiv diffusion routing.
4-Information gain.
5 -Communication rate.
6 -Database.
7 -Leader.

که داده‌های تولید شده عظیم هستند، فراهم سازد. COUGAR روش‌های مستقل از لایه‌های شبکه را برای پرسمان داده‌ها فراهم می‌کند.

-ACQUIRE [b-Sadagopan]

این پروتکل، به فنی برای پرسمانِ شبکه‌های حس‌گر اشاره دارد که پیشسوییِ (هدایتِ) پرسمان فعال[1] در شبکه‌های حس‌گر (ACQUIRE) نامیده می‌شود. همانند COUGAR، ACQUIRE شبکه را به عنوان یک دادگانِ توزیع شده می‌بیند که در آن پرسمان‌های پیچیده می‌توانند، بیشتر به چندین پرسمان فرعی تقسیم شوند. عملیات ACQUIRE، می‌تواند به صورت پیش رو شرح داده شود. گرهِ BS، یک پرسمان را ارسال می‌کند که سپس توسطِ هر گرهِ دریافت‌کنندهِ پرسمان، پیشسو (هدایت) می‌شود. طی این فرآیند هر گره سعی می‌کند، تا با استفاده از اطلاعات قبلیِ حافظهِ نهانِ[2] خود تا حدی به پرسمان پاسخ دهد و سپس آن را به گره حس‌گر دیگر پیشسو (هدایت) کند. درصورتی که اطلاعات قبلیِ حافظهِ نهان، به‌روز نباشد، گره‌ها اطلاعات را از همسایگان خود، طی یک جمع آوری سریع hopگام‌ها جمع‌آوری می‌کند. زمانی که پرسمان کاملا معین شد، یا از طریق معکوس و یا کوتاه‌ترین مسیر[3] به BS برگردانده می‌شود. بنابراین، ACQUIRE می‌تواند با امکان ارسال پاسخ‌ها توسط گره‌های بسیاری، به پرسمان‌های پیچیده بپردازد.

-مسیریابی آگاه به انرژی [b-Shah]

هدف از پروتکلِ مسیریابیِ آگاه به انرژی، پروتکلِ واکنشیِ در مقصد آغاز شده[4]، افزایشِ طولِ عمرِ شبکه است. اگرچه این پروتکل مشابه با پروتکلِ پخش هدایت شده (مستقیم) است، اما، از نظر، نگاه‌داریِ مجموعه‌ای از مسیرها ، به جای نگاه‌داری یا اعمالِ یک مسیرِ بهینه با نرخِ[5] بالاتر، متفاوت است. این مسیرها با احتمال معینی انتخاب و نگاه‌داری می‌شوند. مقدار این احتمال، به اینکه به چه مقدار، مصرفِ انرژیِ پایین، در هر مسیر، می‌توان دست یافت بستگی دارد. این موضوع، می‌تواند به طول عمر بالاتر شبکه منتج شود زیرا انرژی به طور معادل‌تری، در میان تمام گره‌ها پراکنده می‌شود.

-پروتکل‌های مسیریابی با قدم زدنِ (گردش‌های) تصادفی [b-Servetto]

هدف از فن مسیریابی مبتنی بر قدم زدن تصادفی، دست‌یابی به ایجاد تراز بار[6] در مفهوم آماری و با استفاده از مسیریابی با چند مسیر، در WSNها است. این فن تنها شبکه‌های در مقیاس بزرگ را مورد توجه قرارمی‌دهد که در آنها گره‌ها دارای سیاریت بسیار محدودی هستند. در این پروتکل، فرض می‌شود که گره‌های حس‌گر می‌توانند در زمان‌های تصادفی روشن و خاموش شوند. به علاوه هر گره دارای شناسانهِ یکتا است اما هیچ اطلاعات مکانی مورد نیاز نیست. گره‌ها به گونه‌ای مرتب شدند که هر گره به طور دقیق در یک نقطه تقاطع از یک صفحه[7] شبکه‌ای[8] هماهنگ[9] در یک سطح قرار می‌گیرد، اما همبندی می‌تواند نامنظم باشد. برای یافتن یک مسیر از مبدا به مقصدش، اطلاعات مکانی یا هماهنگی شبکه‌ای[10]، با رایانش فاصلهِ میانِ گره‌ها، با استفاده از نسخهِ (ناهمگامِ)

---

1 -Active query forwarding.
2 -Cached.
3 -Shortest path.
4 -Destination-intiated reactive protocol.
5 -Rate.
6 -Load balance.
7 -Plane.
8 -Grid.
9 -Coordination.
10 -Lattice.

غیرهمزمانِ توزیع شدهِ الگوریتمِ معروفِ بلمن-فورد [b-Bellman] بدست می‌آید. یک گره میانی، به عنوان گامِ[1] بعدی، گره همسایه را، که مطابق با یک احتمال رایانش شده، به مقصد نزدیک‌تر است را، انتخاب میکند. با دستکاری کردن دقیق بر روی این احتمال، برخی از انواع تراز بار می‌تواند در شبکه بدست آید. الگوریتم مسیریابی ساده است، چراکه گره‌ها مستلزم نگاه‌داریِ اطلاعاتِ وضعیت کمی هستند. به علاوه حتی برای جفت گره‌های مقصد و منبع یکسانی، مسیرهای مختلف، در زمان‌های مختلف، انتخاب می‌شوند.

-پروتکل LEACH[2] [b-Heinzelman]، [b-Chandrakasan]

این پروتکل یک الگوریتم خوشه بندی سلسله مراتبی را برای شبکه‌های حس‌گر معرفی می‌کند که سلسله مراتبِ خوشه‌بندیِ وفقی با انرژیِ پایین (LEACH) نامیده می‌شود. LEACH یک پروتکل برپایهِ خوشه است، که به شکلِ خوشه‌ایِ توزیع شده، است. LEACH، به صورت تصادفی، تعداد کمی‌گره حس‌گر را به عنوان راسِ خوشه‌ها (CH)[3] انتخاب می‌کند و این نقش را تا توزیع متوازن بارِ انرژی، میان حس‌گرها، در شبکه می‌چرخاند. در LEACH، گره‌های راسِ خوشه (CH)، داده‌هایِ وارد شده از گره‌هایی را که به خوشه مربوطه تعلق دارد را، فشرده می‌کنند و یک بسته انبوهش شده را، به منظور کاهش میزان اطلاعاتی که باید به ایستگاه پایه ارسال شود، به ایستگاه پایه ارسال می‌کنند. LEACH از یک TDMA[4] (دسترسی چندگانه با تقسیم بندی زمان)/ CDMA[5](دسترسی چندگانه با تقسیم کد) برای کاهش تصادم بینابینِ[6] خوشه‌ها و درون[7] خوشه استفاده می‌کند. بنابراین، این پروتکل، بیشتر زمانی که، نیاز به پایشِ دایم توسطِ شبکه حس‌گر وجود دارد، مناسب است.

-جمع آوری با کاراییِ توان در سامانه‌های اطلاعاتی حس‌گر (PEGASIS)[8] [b-Lindsey]

این پروتکل، به عنوان یشرفتی بر پروتکل LEACH پیشنهاد شد. این پروتکل که جمع آوری با کاراییِ توان، در سامانه‌های اطلاعاتی حس‌گر (PEGASIS) نامیده می‌شود یک پروتکلِ برمبنای زنجیرهِ نزدیک به بهینه است. ایده پایه این پروتکل این است که به منظور افزونگیِ طول عمر[9] شبکه، گره‌ها تنها به ارتباط با نزدیک‌ترین همسایه‌های خود نیاز خواهند داشت و برای ارتباط با ایستگاه پایه نوبت می‌گیرند. زمانی که دوره نوبت تمام گره‌های درحال ارتباط با ایستگاه پایه به پایان رسید، یک دوره جدید آغاز می‌شود و به همین ترتیب ادامه می‌یابد. این شیوه، توان مورد نیاز برای انتقال داده‌ها به ازای هر دوره را کاهش می‌دهد چراکه تخلیه توان به صورت یکسان در تمام گره‌ها گسترده می‌شود.

---

1 -Hop.
2 - Low energy adaptive clustering hirechial.
3 -Cluster head.
4 -Time division multiple access.
5 -Code division multiple access.
6 -Inter.
7 -Intra.
8- Power-efficient gathering in sensor information system.
9 -Lifetime.

-پروتکل‌های شبکه حس‌گر با کاراییِ انرژی با آستانهِ حساسیت (TEEN)[1] و پروتکل شبکه حس‌گر با کاراییِ انرژی با آستانهِ حساسیتِ متناوبِ وفقی (TEEN و APTEEN)[2] [b-Manjeshwar-1] و [b-Manjeshwar-2]

دو پروتکل مسیریابی سلسه مراتبی TEEN (پروتکل‌های شبکه حس‌گر با کارایی انرژی با آستانهِ حساسیت) و APTEEN (پروتکل شبکه حس‌گر با کارایی انرژی با آستانهِ حساسیتِ متناوبِ وفقی) به ترتیب معرفی شده‌اند. این پروتکل‌ها برای کاربردهای بحرانی به زمان پیشنهاد شده‌اند. در TEEN، گره‌های حس‌گر، محیط[3] را، به طور پیوسته حس می‌کنند، اما انتقال داده‌ها، با بسامد کمتری صورت می‌گیرد. یک حس‌گر راس خوشه، برای اعضای خود، یک آستانه قوی[4] را، که مقدار آستانه صفت حس شده است و یک آستانه ضعیف[5] را که تغییر کوچک در مقدار صفت حس شده است که موجب چکانش[6] گره برای روشن کردن[7] فرستنده و انتقال هستند را، ارسال می‌کند. بنابراین آستانه قوی، سعی می‌کند تا تعداد انتقال‌ها را، با دادنِ اجازهِ انتقال به گره‌ها، تنها در زمانی که صفت حس‌شده در گسترهِ توجه[8] قرار دارد، کاهش دهد.

-APTEEN یک پروتکل ترکیبی است که دُورِگی[9] یا مقادیر آستانه مورد استفاده در پروتکل TEEN را، بر طبق نیازهای کاربر و نوع کاربرد، تغییر می‌دهد. در APTEEN، راسِ خوشه‌ها صفت‌ها، آستانه‌ها، برنامه زمان بندی و زمان شمارش را پخش همگانی می‌کنند. گره محیط را به صورت پیوسته حس می‌کند و تنها آن گره‌هایی که مقدار داده‌ها را در آستانه قوی، یا فراتر از آن، حس کرده اند، انتقال می‌دهند.

-شبکه ارتباطیِ کوچک با کمینهِ انرژی (MECN) [b-Rodoplu]

یک پروتکل پیشنهادی است که برای یک شبکه حس‌گر معین، انرژی کارایِ یک شبکه فرعی را، با استفاده از یک سامانه موقعیت یابی جهانی با توان پایین (GPS)[10]، رایانش می‌کند و با نام شبکه ارتباطی کوچک با کمینهِ انرژی (MECN)[11]، نامیده می‌شود. MECN یک منطقه مورد اطمینان را برای هر گره شناسایی می‌کند. منطقه مورد اطمینان متشکل از گره‌هایی در یک منطقه پیرامونی است که در آن منطقه، انتقال از طریق آن گره‌ها، انرژی کاراتری نسبت به انتقال مستقیم دارد.

---

1 -Threadshold-sensetive energy efficient sensor network protocol
2 -Adaptive periodic vThreadshold-sensetive energy efficient sensor network protocol
3 -Medium.
4 -Hard thredshold.
5 -Soft thredshold.
6 -Trigger.فرایندی که در آن نشانک/ سیگنال ضعیف سبب تغییر ناگهانی مشخصه‌ها یا عملکرد مدار شود
7 -Switch on.
8 -Interest range.
9 - Periodicity.
10 -Global positioning system.
11 -Minimum energy communication network.

-پروتکل خود سازمان (SOP)[1] [b-Subramanian]

SOP یک پروتکل خود سازمان و یک طبقه بندی کاربردی را شرح می‌دهد که برای ساخت معماریِ مورد استفاده جهت پشتیبانیِ از حس‌گرهای ناهمگن، استفاده می‌شود، به‌علاوهِ این‌که، حس‌گرها می‌توانند سیار یا ثابت باشند. برخی حس‌گرها محیط را کاوش می‌کنند و داده‌ها را به یک مجموعه برگزیده[2] گره‌ها که به عنوان مسیریاب عمل می‌کنند، پیشسویی (هدایت) می‌کند. گره‌های مسیریاب ثابت هستند و ستون فقرات[3] ارتباط را شکل می‌دهند. داده‌های جمع آوری شده از طریق مسیریاب‌ها به گره‌های قدرتمندترِ BS پیشسو (هدایت) می‌شوند. هر گره حس کننده، به منظور اینکه بتواند بخشی از شبکه باشد، باید به یک مسیریاب دسترسی داشته باشد. معماری مسیریابیی، که مستلزم نشانی دهیِ هر گره حس‌گر است، ارایه شده است. گره‌های حس کننده، از طریق نشانی گره مسیریابیی که به آن متصل می‌شوند، قابل شناسایی هستند. معماری مسیریابی، سلسله مراتبی است که در آن گروه‌های گره‌ها، هنگام نیاز شکل می‌گیرند و ادغام می‌شوند. الگوریتم حلقه‌های مارکوف محلی (LML) [4]، که یک قدم زدنِ (گردشِ) تصادفی را درخت‌های پوشای یک نگاشت شکل می‌دهد، جهت پشتیبانی از عیبتابی و به عنوان ابزاری برای پخش همگانی مورد استفاده قرار می‌گیرد.

-مسیریابی انبوهشی حس‌گر [b-Fang]

مجموعه ای از الگوریتم‌ها برای ساخت و نگاه‌داریِ انبوهش‌هایِ حس‌گر پیشنهاد شده است. هدف آن پایشِ جامع فعالیت هدف در یک محیط معین (کاربردهای ردیابی هدف) است. انبوهشِ حس‌گر آن گره‌هایی در یک شبکه را دربرمی‌گیرد که دریک گروه، یک وظیفه پردازش اشتراکی را تامین می‌کنند.

سه الگوریتم پیشنهاد شده‌اند[b-Fang]. اولین الگوریتم، پروتکلی سبک، با مدیریت انبوهشیِ توزیع شده (DAM)[5]، است تا انبوهه سازیِ حس‌گر را برای یک وظیفه پایشیِ هدف شکل دهد. این پروتکل تخمین تصمیم P برای هر گره را، برای تصمیم گیری درمورد اینکه آیا باید در انبوهش شرکت کند و یا خیر و یک طرحِ مبادلهِ پیام M را، برای تعیین اینکه چگونه تخمین گروه بندی برای گره‌ها اجرا می‌شوند را، بکار می‌گیرد. یک گره تعیین می‌کند، که آیا در نتیجه اجرای تخمین درمورد داده‌های گره، و همچنین اطلاعات از دیگر گره‌ها، به یک انبوهه‌سازی تعلق دارد و یا خیر. انبوهش‌ها، زمانی که فرآیند سرانجام همگرا می‌شود، شکل می‌گیرند.

الگوریتم دوم، پایش فعالیت مبتنی بر انرژی (EBAM)[6] است که سطح انرژی را در هر گره را تخمین می‌زند. که این رویه با با رایانش محدودهِ تأثیر سیگنال و ترکیب شکلی سنگین از انرژیِ هدفِ شناسایی شده، در هر حس‌گرِ تحت تأثیر، انجام می‌شود، با فرض اینکه هر حس‌گر هدف دارای یک سطح انرژی مساوی یا ثابت است،

الگوریتم سوم، بیشینه سازی انتظارات مانندِ پایش فعالیت (EMLAM)[7]، فرض سطحِ انرژیِ هدفِ مساوی و ثابت را حذف می‌کند. EMLAM موقعیت‌های هدف و انرژی نشانک/سیگنال را، با استفاده از نشانک‌ها/سیگنال‌های دریافتی، تخمین می‌زند و تخمین‌های حاصل شده را، برای پیش بینی نحوه اینکه نشانک‌ها/سیگنال‌های اهداف،

---

1 -Self-organization.
2 -Designated.
3 -Backbone.
4 -Local Markov loop.
5 -Distributed aggregate management.
6 -Energy-based activity monitoring.
7 -Expectation-maximization like activity monitoring.

چگونه ممکن است در هر حس‌گر ترکیب شوند، مورد استفاده قرار می‌دهد. این فرآیند تا زمانی که تخمین به اندازه کافی خوب نباشد تکرار می‌شود.

پروتکل مسیریابی اینترنت نسخه شش (IPv6)[1] برای شبکه‌های با توان پایین و با اتلاف (PRL)[2]

RPL، همبندیی را به شکل یک نگاشتِ غیر مدور مستقیم (DAG)[3]، که در یک یا چند DAG مقصدگرا (DODAGها)[4] افراز شده‌اند، سازماندهی می‌کند. RPL در دو لایه مختلف کار می‌کند؛ پردازش و پشسوییِ (هدایتِ) بسته، و بهینه سازی مسیریابی. به علاوه، RPL دارای سه گزینه امنیتی است: غیر ایمن، کلید از پیش نصب شده و اصالت‌سنجی. کلیدهای از پیش نصب شده به گره‌ها اجازه می‌دهد تا پیام‌های RPL ایمن را پردازش و تولید کند. با گزینه اصالت‌سنجی شده، گره‌ها می‌توانند تنها با استفاده از کلید از پیش نصب شده، به عنوان برگ بپیوندند. پیوستن به عنوان یک مسیریاب، مستلزم بدست آوردن یک کلید، از یک مرجع اصالت‌سنج است. در حالت «غیر ایمن»، هیچ سازوکار امنیتی بکار نمی‌رود.

1 -Internet protocol.
2 -Routing protocol for low-power and lossy network.
3 -Directed acyclic graph.
4 -Destination oriented DAG.

کتابنامه

[b-ITU-T Y.2221]
Recommendation ITU-T Y.2221 (2010), Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.

[b-IEEE 802.16.2] IEEE 802.16.2™ (2004)
Recommended Practice for Local and metropolitan area networks: Coexistence of Fixed Broadband Wireless Access Systems, IEEE.

[b-IETF RFC 6650]
IETF RFC 6550 (2012), RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks.

[b-ISO/IEC 11889-1]
ISO/IEC 11889-1 (2009), Information technology – Trusted Platform Module – Part 1: Overview.

[b-Bellman]
Bellman, R. (1958), On a route problem, Quarterly of Applied Mathematics Vol. 16, pp. 87-90.

[b-Braginsky]
Braginsky, D., and Estrin, D. (2002), Rumor routing algorithm for Sensor Networks, Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA.

[b-Chandrakasan]
Heinzelman, W. R., Chandrakasan, A., and Balakrishnan, H. (2000), Energy-efficient communication protocol for wireless microsensor networks, Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS'00).

[b-Chu]
Chu, M., Haussecker, H., and Zhao, F. (2002), Scalable Information-Driven Sensor Querying and Routing for Ad Hoc Heterogeneous Sensor Networks, The International Journal of High Performance Computing Applications, Vol. 16, No. 3, pp. 293-313.

[b-Fang]
Fang, Q., Zhao, F., and Guibas, L. (2003), Lightweight sensing and communication protocols for target enumeration and aggregation, Proceedings of the 4th ACM international symposium on Mobile ad hoc networking and computing (MOBIHOC), pp. 165-176.

[b-Heinzelman]
Heinzelman, W., Kulik, J., and Balakrishnan, H. (1999), Adaptive Protocols for Information Dissemination in Wireless Sensor Networks, Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom'99), pp. 174-85, Seattle, WA.

[b-Intanagonwiwat]
Intanagonwiwat, C., Govindan, R., and Estrin, D. (2000), Directed diffusion: a scalable and robust communication paradigm for sensor networks, Proceedings of the 6th annual international conference on Mobile computing

and networkingMobiCom'00, pp. 56-67, Boston, MA.

[b-Kulik]
Kulik, J., Heinzelman, W.R., and Balakrishnan, H. (2002), Negotiation-based protocols for disseminating information in wireless sensor networks, Wireless Networks, Vol. 8, No. 2/3, pp. 169-185.

[b-Lindsey]
Lindsey, S., and Raghavendra, C. (2002), PEGASIS: Power-efficient gathering in sensor information systems, Aerospace Conference Proceedings, IEEE, Vol. 3, pp. 1125-1130.
Rec. ITU-T X.1313 (10/2012) 17

[b-Manjeshwar-1]
Manjeshwar, A., and Agarwal, D.P. (2000), TEEN: a routing protocol for enhanced efficiency in wireless sensor networks, Parallel and Distributed Processing Symposium, Proceedings 15th International, pp. 2009-2015.

[b-Manjeshwar-2]
Manjeshwar, A., and Agarwal, D.P. (2002), APTEEN:a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks, Parallel and Distributed Processing Symposium, Proceedings International, IPDPS, pp. 195-202.

[b-Rodoplu]
Rodoplu, V., and Meng, T.H. (1999), Minimum Energy Mobile Wireless Networks, IEEE Journal Selected Areas in Communications, Vol. 17, No. 8, August, pp. 1333-1344.

[b-Sadagopan]
Sadagopan, N. Krishnamachari, B., and Helmy, A. (2003), The ACQUIRE mechanism for efficient querying in sensor networks, in the Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, Alaska, May.

[b-Schurgers]
Schurgers, C., and Srivastava, M.B. (2001), Energy efficient routing in wireless sensor networks, Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE, Vol.1, pp. 357-361.

[b-Servetto]
Servetto, S., and Barrenechea, G. (2002), Constrained random walks on random graphs: routing algorithms for large scale wireless sensor networks, Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pp. 12-21, Atlanta, Georgia, USA.

[b-Shah]
Shah, R.C., and Rabaey, J. (2002), Energy aware routing for low energy ad hoc sensor networks, Wireless Communications and Networking Conference (WCNC), March, IEEE, Orlando, FL.

[b-Subramanian]
Subramanian, L., and Katz, R.H. (200), An architecture for building self-configurable systems, Proceedings of the 1st ACM international

symposium on Mobile ad hoc networking & computing, MobiHoc '00, August, Boston, MA.

[b-Yao]
Yao, Y., and Gehrke, J. (2002), The cougar approach to in-network query processing in sensor networks, ACM SIGMOD Record, Vol. 31, No. 3, pp. 9-18.

[b-Ye]
Ye, F., Chen, A., Liu, S., and Zhang, L. (2001), A scalable solution to minimum cost forwarding in large sensor networks, Proceedings of the tenth International Conference on Computer Communications and Networks (ICCCN), pp. 304-309.

[b-Zigbee]
Zigbee, <http://www.zigbee.org/Standards/Downloads.aspx>.