



جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization



استاندارد ملی ایران

۱۷۵۱۹

چاپ اول

۱۳۹۳

INSO

17519

1st.Edition

2014

فناوری اطلاعات – مخابرات و تبادل اطلاعات
بین سامانه‌ها – چارچوب کاری امنیت برای
شبکه‌های حس‌گر همه جاگاه

Information technology—
Telecommunications and information
exchange between systems—Security
framework for ubiquitous sensor networks

ICS: 35.110

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسه استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه 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 و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانه صاحبان حق و نفع، شامل تولیدکنندگان، مصرف کنندگان، 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 می شود و پس از دریافت نظرها و پیشنهادها در کمیته 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 در کمیته ملی طرح و بررسی و در صورت 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 شماره ۵ تدوین و در کمیته ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)^۱، کمیسیون بین المللی الکتروتکنیک (IEC)^۲ و سازمان بین المللی اندازه شناسی قانونی (OIML)^۳ است و به عنوان تنها رابط^۴ کمیسیون کدکس غذایی (CAC)^۵ 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 بین المللی بهره گیری می شود.

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 درجه بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینه مشاوره، آموزش، بازرسی، ممیزی و صدور گواهی سیستم های مدیریت کیفیت و مدیریت زیست محیطی، 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، گواهینامه 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

« فناوری اطلاعات - مخابرات و تبادل اطلاعات بین سامانه‌ها - چارچوب کاری امنیت برای شبکه‌های
حس‌گر همه جاگاه »

رئیس :

ابراهیمی آتانی، رضا

(دکتری مهندسی برق، الکترونیک)

سمت و/یا نمایندگی

دانشکده فنی، دانشگاه گیلان

دبیر :

فرمان آراء، شایسته

(کارشناسی مهندسی کامپیوتر، نرم افزار)

سازمان ملی استاندارد ایران

اعضاء : (اسامی به 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

حسینی 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

طه‌پوری، سامان

(کارشناس ارشد مهندسی فناوری اطلاعات، شبکه های کامپیوتری)

کارشناس

عزیزی، زهرا

(کارشناس فناوری اطلاعات)

کارشناس

فرمان آراء، نفیسه

(کارشناس مهندسی برق، الکترونیک)

کارشناس

فهرست مندرجات

صفحه	عنوان
ب	آشنایی با سازمان ملی استاندارد ایران
د	کمیسیون فنی تدوین استاندارد
ه	پیش‌گفتار
و	مقدمه
۱	۱ هدف
۲	۲ مراجع الزامی
۳	۳ اصطلاحات و تعاریف
۷	۴ کوتاه‌نوشت‌ها
۷	۵ قراردادهای
۸	۶ مرور کلی
۱۴	۷ تهدیدات و مدل‌های امنیتی برای شبکه‌های حس‌گر همه‌جاگاه
۲۱	۸ ابعاد امنیتی کلی برای USN
۲۳	۹ تهدیدات و ابعاد امنیتی در شبکه‌های حس‌گر همه‌جاگاه
۲۸	۱۰ فنون امنیتی برای شبکه‌های حس‌گر همه‌جاگاه
۳۶	۱۱ الزامات کارکردی امنیت ویژه برای USN
۳۸	پیوست الف (الزامی) مدیریت کلید در شبکه‌های حس‌گر
۴۲	پیوست ب (اطلاعاتی) پخش همگانی اصالت سنجی شده در شبکه‌های حس‌گر: μ TPC
۴۷	پیوست پ (الزامی) سازوکار اصالت سنجی در شبکه‌های حس‌گر
۵۶	پیوست ت (الزامی) انبوهش داده‌های ایمن در شبکه‌های حس‌گر
۶۱	کتابنامه

پیش‌گفتار

استاندارد «فناوری اطلاعات- مخابرات و تبادل اطلاعات بین سامانه‌ها - چارچوب کاری امنیت برای شبکه‌های حس‌گر همه جاگاه» که پیش‌نویس 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 مورخ ۱۳۷۰/۰۱/۳۰ 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 همگامی و 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 مآخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است :

ISO/IEC 29180 : 2012, Information technology — Telecommunications and information exchange between systems — Security framework for ubiquitous sensor networks

مقدمه

ISO/IEC 29180^۱ توسط کمیته مشترک فنی ISO/IEC JTC 1^۲، فناوری اطلاعات، کمیته فرعی SC 6^۳، مخابرات و مبادله اطلاعات میان سامانه‌ها، با همکاری ITU^۴ آماده شده است. متن همسانی با عنوان Rec. ITU-T X.1311 (02/2011) منتشر شده است.

۱ - این استاندارد ملی بر اساس منبع بین‌المللی ISO/IEC 29180: 2012 که همسان با توصیه نامه ITU-T X.1311: 02/2011 است، نوشته شده است.

2-International Organization for Standardization/- International Electrotechnical Commission Joined technical Committee.

3 -Sub Committee.

4 -Internatinal Telecommunication unite.

فناوری اطلاعات – فناوری اطلاعات – مخابرات و تبادل اطلاعات بین سامانه‌ها – چارچوب کاري امنيت برای شبکه‌های حس گر همه جاگاه

۱ هدف

هدف از تدوین این استاندارد، تعیین الزامات امنیتی شبکه‌های حس گر همه جاگاه، و شرحی بر تهدیدات^۱ امنیتی در این شبکه‌ها است. همچنین، این استاندارد ملی، فناوری‌های امنیتی را، در تطابق با کارکردهای^۲ امنیتی‌ای که الزامات امنیتی مطرح را برآورده می‌کنند و در تطابق با جایگاه کاربرد فناوری‌های امنیتی در مدل امنیتی شبکه‌های حس گر همه جاگاه، رده‌بندی می‌کند. در نهایت، الزامات کارکردی امنیت و فناوری‌های امنیت، برای شبکه‌های حس گر همه جاگاه، نمایش داده می‌شوند.

پیشرفت‌های اخیر الکترونیک و فناوری ارتباطات مبتنی بر بی سیم، پیاده‌سازی^۳ یک شبکه حس گر کم هزینه^۴ و با مصرف توان پایین^۵ را آسان کرده است. بطور ابتدایی و پایه، یک شبکه حس گر همه جاگاه^۶ (USN)^۷ متشکل از سه قسمت است: یک شبکه حس گر متشکل از تعداد زیادی از گره‌های حس گر^۸، ایستگاه پایه^۹ (که به عنوان دروازه^{۱۰} نیز شناخته می‌شود) که واسطه^{۱۱} میان شبکه‌های حس گر و یک کارساز^{۱۲} کاربردی^{۱۳} است، و یک کارساز کاربردی. کارساز کاربردی، گره حس گر را در شبکه حس گر واپایش^{۱۴} می‌کند یا اطلاعات حس شده^{۱۵} را از گره‌های حس گر، در شبکه حس گر جمع‌آوری می‌کند.

USN، می‌تواند یک زیرساخت اطلاعاتی هوشمند^{۱۶} از جامعه‌ای با زندگی الکترونیکی^{۱۷} پیشرفته باشد که اطلاعات کاربر محور^{۱۸} را ارائه می‌دهد و خدمات دانش^{۱۹} را، در هر زمانی و در هر جایی که اطلاعات و دانش، با

کنش یا رویدادی که ممکن است امنیت برنامه‌ها و داده‌های رایانه را به خطر بیندازد. Threats-1

2-Functions.

3 Implementation.

4 -Low-cost.

5 -Low-power.

۶ - در هر زمان و در هر مکان.

7 -Ubiquitous sensor network.

8 -Sensor nodes.

9 -Base station.

10 -Gateway.

11 -Interface.

12 -Server.

13 -Application.

14 Control.

15 -Senced information.

16- intelligent information infrastructure.

17 - E-Life.

18 -User-oriented.

19-Knowledge.

استفاده از بافت آگاهی^۱ توسعه می‌یابند را، بوسیله آشکارسازی ذخیره، پردازش و یکپارچه‌سازی اطلاعات وضعیتی و محیطی جمع‌آوری شده توسط برچسب/دنباله^۲ حس‌گرها و/یا گره‌های حس‌گر الحاق شده به چیزی دیگر^۳، فراهم می‌سازد. از آنجایی که برای انتقال^۴ و ذخیره اطلاعات در USN، تهدیدات امنیتی و تهدیدات حریم^۵ بسیاری وجود دارند، سازوکارهای امنیتی^۶ مناسب برای حفاظت در برابر آن تهدیدات در USN لازم است.

۲ مراجع الزامی

مدارک الزامی زیر 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 مورد نظر 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 الزامی است:

۲-۱ جفت توصیه نامه ها | استانداردهای بین المللی معادل^۷ در محتوای فنی

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

۲-۱-۲- استاندارد ملی ایران شماره ۲-۱۶۲۷۴: سال ۱۳۹۱، سامانه های پردازش اطلاعات - اتصال متقابل سامانه های باز - مدل مرجع پایه - قسمت ۲- معماری امنیتی^۸

2-1-1- Recommendation ITU-T X.805 (2003), Security architecture for systems providing end-to-end communications.

۲-۱-۳- استاندارد ملی ایران شماره ۲-۱۱۲۱۰: سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی - امنیت شبکه فناوری اطلاعات قسمت ۲- معماری امنیتی شبکه^۹

۲-۲ مراجع افزوده^{۱۰}

۲-۲-۱- استاندارد ملی ایران آی تی یو تی H.235.0 شماره سال ۱۳۸۸، سامانه های دیداری و شنیداری و چند رسانه ای - زیر ساخت سرویس های دیداری و شنیداری - جنبه های سامانه ای - امنیت H.323 پشتیبانی دروازه امنیتی برای H.323

1- Context-awareness.

2- Tag.

۳ - به عنوان مثال الحاق RFID tag ها با حس‌گرها به جهت ارسال شناسانه به همراه اطلاعات حس شده توسط حس‌گر.

4 -Transferring.

5 -Privacy.

6- Mechanism.

7 -Equivalent.

۸ - بر اساس منبع استاندارد بین المللی ISO/IEC 7498-2:1989

۹ - بر اساس منبع استاندارد بین المللی ISO/IEC 18028-2:2006

10 -Additional.

2-2-2- Recommendation ITU-T X.1111 (2007), Framework of security technologies for home network.

2-2-3- Recommendation ITU-T X.1191 (2009), Functional requirements and architecture for IPTV security aspects

2-2-4- Recommendation ITU-T Y.2221 (2010), Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment.

2-2-5- Recommendation ITU-T Y.2701 (2007), Security requirements for NGN release 1.

2-2-6- FIPS PUB 140-2 (2001), Security Requirements for Cryptographic Module.

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می روند:

۳-۱ اصطلاحات تعریف شده در مستندات دیگر

اصطلاحات زیر، در مستندات دیگر تعریف شده اند.

۳-۱-۱ اصطلاحات از FIPS PUB 140-2^۱

الف) انتقال/تراپری کلید^۲

ب) آشکارسازی مداخله^۳

پ) گواه مداخله^۴

ت) رویارویی^۵ با مداخله^۶

۳-۱-۲ اصطلاحات از Rec.ITU-T Y.2221

الف) حس گر

ب) شبکه حس گر

پ) میان افزار USN

ت) شبکه حس گر همه جاگاه (USN).

۳-۱-۳ اصطلاحات از Rec.ITU-T H.235.0

الف) حمله

۳-۱-۴ اصطلاحات از Rec.ITU-T X.1191

الف) مقاوم/تاب^۷ در مقابل مداخله

1 - Federal Information Processing Standard Publication

2 -Key transport.

3 -Tamper detection.

4 -Tamper evidence.

5- Response.

6 -Tamper response,

7- Resistant.

۵-۱-۳ اصطلاحات از Rec.ITU-T X.800 | ISO/IEC 7498-2

این استاندارد از اصطلاحات زیر که در مستندات دیگر تعریف شده‌اند استفاده می‌کند:

الف) کنترل دسترسی

ب) اصالت سنجی^۱

پ) اجازه^۲

ت) محرمانگی^۳

ث) اصالت سنجی مبدا داده‌ها

ج) بندآوری خدمات^۴ (انکار خدمت)

چ) امضای رقمی^۵ (دیجیتال)

ح) یکپارچگی^۶

خ) کلید

د) مدیریت کلید

ذ) اصالت سنجی هستار همتا^۷

ر) حریم^۸

ز) انکار^۹

ژ) خط مشی^{۱۰} امنیت

س) تهدید

۲-۳ اصطلاحات تعریف شده در این استاندارد

۱-۲-۳

گره انبوهش کننده/انبوه ساز^{۱۱}

گره حس‌گری که کارکرد انبوهش/انبوه ساز داده‌ها را در یک شبکه حس‌گر شکل می‌دهد.

۲-۲-۳

-
- 1- Authentication.
 - 2- Authorization
 - 3- Confidentiality.
 - 4- Denial of service
 - 5- Digital signature.
 - 6 -Integrity.
 - 7- Peer entity authentication
 - 8 -Privacy.
 - 9 -Repudiation.
 - 10- Policy.
 - 11 -Aggregator node.

راه اندازی^۱

فرآیندی است در زمینه‌ای ایمن، که پیش از استقرار/به‌کاراندازی^۲ گره حس‌گر شکل می‌گیرد به طوری که میان گره‌های حس‌گر، یک همبستگی امن را، که مجاز است با اعتبارنامه‌ها آغاز شود، را برقرار می‌سازد^۴ و موجب فعال بودن ارتباط ایمن یک گره حس‌گر با دیگر گره‌های حس‌گر، پس از استقرار/به‌کاراندازی آنها خواهد شد.

۳-۲-۳

اعتبارنامه‌ها

مجموعه‌ای از اطلاعات امنیتی است، متشکل از کلیدها، محتویات کلیدگذاری^۵ و پارامترهای مرتبط با الگوریتم-های رمزنگاشتی^۶، که مجوز یک برهم‌کنش^۷ موفق را با یک سامانه امنیتی، امکان پذیر می‌سازد.

۴-۲-۳

انبوهش^۸ داده‌ها

فرآیندی درون شبکه‌ای است که مقدار داده‌های انبوهش شده را به گره ستانه^۹ انتقال می‌دهد و مقادیر حس شده گره‌های حس‌گر را ترکیب کرده و به خلاصه کوتاهی می‌رسد.

۵-۲-۳

کلید گروهی^{۱۰}

به کلیدی اشاره دارد که برای حفاظت ارتباطات چندپخشی میان مجموعه‌ای از گره‌های حس‌گر، در یک پیوند^{۱۱} بی سیم اشتراکی^{۱۲} استفاده می‌شود.

۶-۲-۳

آشکارسازی نفوذ^{۱۳}

فرآیند واپایش رویدادهای در جریان، در یک شبکه یا سامانه رایانه‌ای و ارزیابی آنها برای تشخیص نفوذ است.

1-Bootstap.

2- Deployment.

3 - Credential. داده‌هایی که برای اثبات صحت شناسه‌ای، ادعایی، یا تأیید شناسه سامانه، ارسال یا نمایش داده می‌شود.

4- Establish.

5 -Keying. نصب کلید در یک ابزار رمزنگاری.

6- Cryptographic.

7 -Interact.

8 -Aggregation.

9 -Sink node.

10- Group-wise -key.

11 -Link.

12 -Shared.

13 -Intrusion detection.

۷-۲-۳

توافق کلید^۱

رویه برقراری یک کلید (دستی و یا الکترونیکی) در شرایطی که کلید منتج شده، کارکردی از اطلاعات مربوط به دو یا چند شرکت کننده است، بنابراین هیچ طرفی نمی‌تواند ارزش کلید^۲ را مستقل از همکاری طرف دیگر، از پیش، تعیین کند.

۸-۲-۳

برقراری کلید^۳

فرآیندی که در آن با استفاده از رویه های تراجری^۴ کلید و/یا توافق کلید، کلیدهای رمزنگاشتی به صورت ایمن، میان گره‌های حس‌گر، برقرار می‌شوند.

۹-۲-۳

جفت کلید

به کلیدی اشاره دارد که برای حفاظت ارتباط تک پخشی بین یک زوج گره حس‌گر، در یک تک پیوند بی‌سیم، مورد استفاده قرار می‌گیرد.

۱۰-۲-۳

برگشت پذیری^۵

توانایی بازیابی^۶، پس از حمله‌ها^۷ یا شکست‌های^۸ امنیتی است.

۱۱-۲-۳

انبوهش داده‌های امن

تضمین یکپارچگی نتایج ناشی از انبوهش داده‌ها است، با بودن یک تعداد کمی از گره‌های انبوهشی بدافزار، که ممکن است برای تأثیر بر نتیجه، تلاش کنند.

۱۲-۲-۳

پودمان مقاومت/تاب^۹ در برابر مداخله

افزاره‌ای که، دسترسی^{۱۰} به اطلاعات حساسی که در پودمان قرار دارند را برای مهاجمان^{۱۱} دشوار می‌کند.

1 -Key Agreement. نوعی تبادل کلید که در آن دو یا چند کاربر با اجرای یک قرارداد به روش امن یک کلید را به اشتراک می‌گذارند.

2 -Value of the key.

3 -Key establishment. روند توزیع امن کلیدهای رمزنگاشتی بین پودمان‌ها.

4 -Transport.

5 -Resilience.

6 -Recovery.

7 -Attack.

8 -Compromises.

9 -Resistance.

10 -Access.

11 -Attackers.

۴ کوتاه نوشت‌ها

BNode	Broadcast Node	گره پخش همگانی
BS	Base Station	ایستگاه پایه
CDMA	Code Division Multiple Access	دسترسی چندگانه با تقسیم کد
DDoS	Distributed Denial of Service	بندآوری خدمات توزیع شده
DoS	Denial of Service	بندآوری خدمات (انکار خدمت)
ECDH	Elliptic Curve Diffie-Hellman	منحنی بیضوی Diffie-Hellman
FP	Feature Parameters	پارامترهای آینده
GSM	Global System for Mobile Communications	سامانه جهانی ارتباطات سیار
HSDPA	High Speed Downlink Packet Access	دسترسی بسته پیوند پایین پرسرعت
ID	Identity	هویت
MAC	Medium Access Control; Message Authentication Code	واپایش دسترسی رسانه؛ کد اصالت سنجی پیام
NGN	Next-Generation Network	شبکه نسل آینده
PHY	physical layer	لایه فیزیکی
RFID	Radio-Frequency Identification	شناسایی بسامد رادیویی
SN	Sensor Network	شبکه حس گر
TMP	Trusted Platform Module	پودمان سکوی مورد اعتماد
USN	Ubiquitous Sensor Network	شبکه حس گر همه جاگاه
WCDMA	Wideband CDMA	CDMA باندپهن
WiMAX	Worldwide Interoperability for Microwave Access	هم‌کنش‌پذیری جهانی برای دسترسی ریزموج
WLAN	Wireless Local Area Network	شبکه منطقه/ناحیه محلی بی سیم
WSN	Wireless Sensor Network	شبکه حس گر بی سیم

۵ قراردادها

در این استاندارد:

کلمات کلیدی^۱ «مستلزم این است»^۲ الزامی را نشان می‌دهد که، در صورتی 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»^۳ الزامی را نشان می‌دهد که، توصیه می‌شود^۴، اما کاملاً الزامی نیست. بنابراین این الزام برای ادعای انطباق ارایه نمی‌شود.

1 -Keywords.

2 -Is required to.

3 -Is recommended.

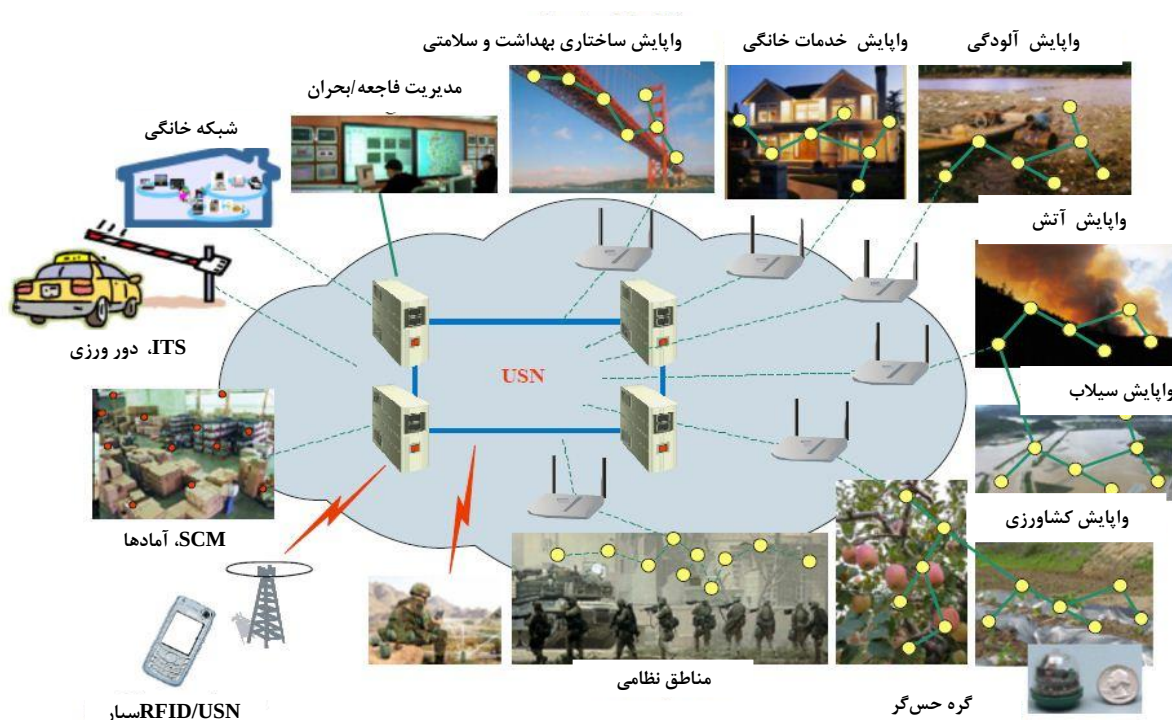
4 -Recommended.

کلمات کلیدی «ممنوع است»^۱ الزامی را نشان می‌دهد که، در صورتی که انطباق با این استاندارد، مورد ادعا باشد، باید به شدت از آن پیروی شود، و هیچ انحرافی از آن مجاز نیست.

کلمات کلیدی «می‌تواند به صورت اختیاری»^۲ و «مجاز است»^۳ 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^۴ و ویژگی‌ای خاصی^۵ را، که توسط فراهم‌سازندگان خدمت/کارور به طور اختیاری می‌تواند فعال شود را، می‌باید فراهم کند. 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^۶ باشد.

۶ مرور کلی

شکل ۱، حوزه‌های کاربردی کلی برای USN را نشان می‌دهد. شامل کاربرد شبکه خانگی، پایش آلودگی، پایش آتش، کاربردهای دورسنجی^۷ برای شرکت‌های خدماتی همگانی (برق، گاز، آب و غیره)، کاربردهای مدیریت/پایش منبع شهری (برای مثال زیرساخت شهر هوشمند) و پایش سیلاب.



شکل ۱ - مناطق کاربرد USN

1 -Is prohibited from.

2 -Can optionally.

3 -May.

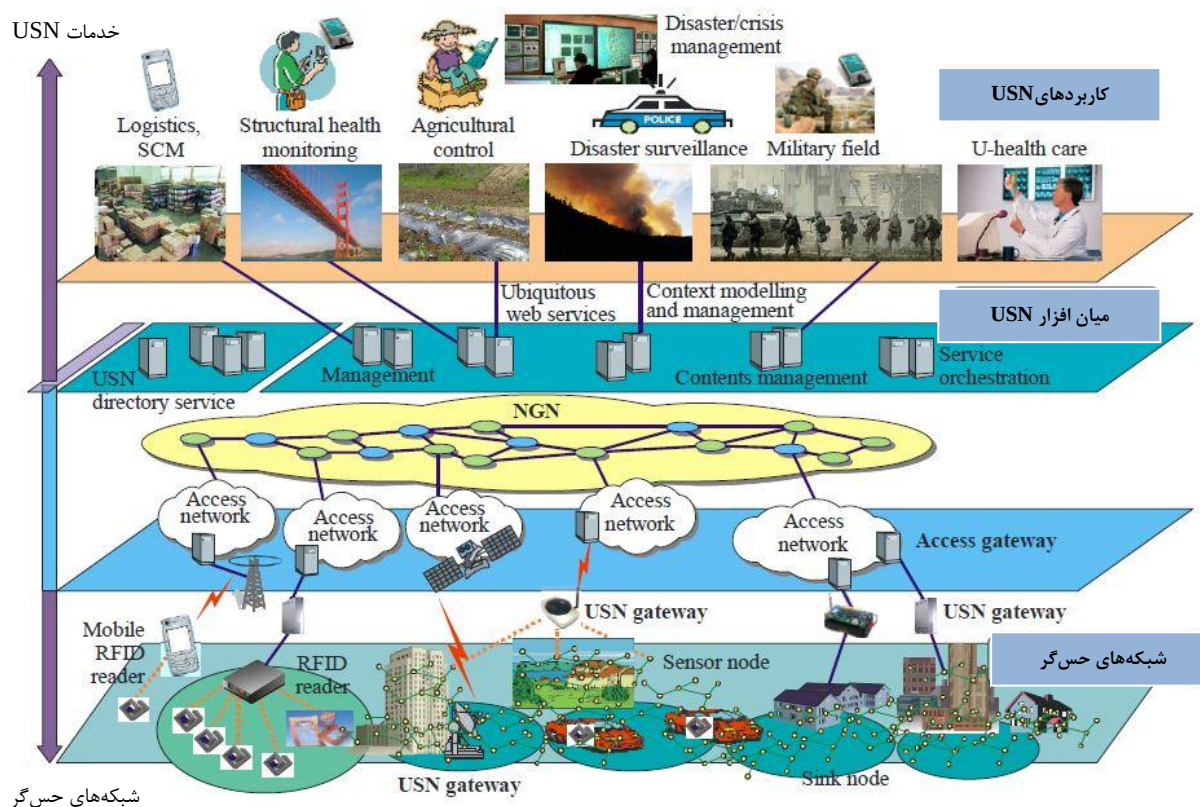
4 -Option.

5 - Feature.

6 -Specification.

7 -Telemetry. اندازه‌گیری فاصله در هر مکان و ارسال داده‌ها به مکان دیگر برای استفاده یا تحلیل.

شکل ۲ ساختار کلی USN را شرح می‌دهد. بر مبنای چنین ساختار پایه‌ای، مدل امنیتی، برای امنیت USN می‌باید تعریف شود.



شکل ۲ - مرور کلی ساختار USN

دامنه شبکه‌بندی حس گر USN به طور معمول متناظر با گره حس گر (SN) است اما شامل شبکه‌های حس گر خط سیمی نیز همچنین می‌شود. بنابراین بسیاری از انواع فناوری‌های شبکه‌بندی بی‌سیم و سیمی ممکن است برطبق مشخصات و الزامات خدمت مورد استفاده قرار گیرد. یعنی، گره‌های حس گر لایه‌های مختلف PHY/MAC (برای مثال IEEE 802.15.4) را به کار می‌گیرند یا در شبکه‌های مبتنی بر پروتکل اینترنت (IP)^۱ یا غیر IP، به گونه‌ای متفاوت عمل می‌کنند.

شبکه‌های حس گر مجزا نیستند بلکه به طور معمول، از طریق شبکه‌های دسترسی^۲ گوناگون و شبکه‌های هسته‌ای^۳، همانطور که در شکل ۲ نشان داده شده است به شبکه‌های مصرف کننده^۴ متصل می‌شوند. دامنه شبکه‌بندی دسترسی، در تناظر با بسیاری از فناوری‌های شبکه‌بندی دسترسی، برای مثال WLAN، WiMax سیار یا شبکه‌های سلولی است. شبکه‌های هسته‌ای شامل NGN، اینترنت و غیره می‌شوند. USN ممکن است مستلزم برخی الحاقات و/یا افزودن به معماری‌های شبکه هسته‌ای باشد تا بتواند الزامات قابلیت کارکردی جدید

1 -Internet protocol.
2 -Access network.
3 -Core network.
4 -Consumer network.

مورد انتظار برای خدمات و کاربردهای USN را پوشش دهد. برای مثال، کاربرد پایش امنیت خانگی، مستلزم ویژگی‌های قابلیت کارکردی ویژه کاربرد است. میان افزار^۱ USN متشکل از بسیاری از کارکردهای نرم افزاری از جمله پردازش و مدل‌های زمینه^۲، جمع‌آوری اطلاعات حسی^۳، پالایش^۴ داده‌ها، مدیریت محتوا، کارکردهای خدمات وب^۵، مدیریت نرم افزار و شبکه، مدیریت نمایه^۶ حس‌گر، خدمات راهنما^۷، دروازه‌های شبکه‌بندی و غیره است. بر مبنای تمام این کارکردها، خدمات و کاربردهای USN می‌توانند، برای مصرف کنندگان و همچنین موسسات، سازمان‌ها و دولت برقرار شده و فراهم شوند.

مدل امنیت برای USN می‌تواند به ۲ قسمت تقسیم شود: یک بخش برای شبکه IP و دیگری برای شبکه حس‌گر بی‌سیم. این استاندارد ملی به دنبال توسعه مدل امنیت برای SN و همچنین شبکه IP است. الگوهای ارتباطی در SN خود در پنج رده قرار می‌گیرد:

- ارتباط گره به ایستگاه پایه، برای مثال هشدارهای ویژه یا خواننده‌های حس‌گر.
- ارتباط ایستگاه پایه به گره، برای مثال درخواست‌های ویژه.
- ارتباط میان یک ایستگاه پایه با تمام گره‌های حس‌گر، برای مثال نشان‌فرست‌های^۸ مسیریابی، پرسمان‌ها، یا برنامه نویسی مجدد کل شبکه حس‌گر.
- ارتباطات گره به گره از جمله ارتباطات میان گره‌های حس‌گر از یک خوشه تعریف شده، برای مثال ارتباطات میان یک گره حس‌گر و تمام همسایه‌هایش.
- ارتباطات میان یک ایستگاه پایه و گروهی از گره‌ها در شرایطی که گروه، از گره‌هایی، که یک خاصیت مشترک (برای مثال، موقعیت مکانی، نسخه نرم افزاری و غیره) را به اشتراک می‌گذارند تعریف می‌شوند.

فرضیات زیر می‌توانند در نظر گرفته شوند:

- ایستگاه پایه از نظر رایانشی قدرتمند است که دارای سرعت پردازشگر، حافظه و توان لازم برای پشتیبانی از الزامات مسیریابی و رمزنگاشتی است. ایستگاه پایه، که دروازه‌ای^۹ است که شبکه‌های حس‌گر را با شبکه‌های دیگر، اتصال متقابل^{۱۰} می‌دهد، مجاز است که قسمتی از یک محیط محاسباتی مورد اعتماد باشد.
- ارتباط از ایستگاه پایه به حس‌گر، از حس‌گر به ایستگاه پایه، از حس‌گر به همسایه‌هایش، و از گره به گره است.

بنابراین، توصیه می‌شود چگونگی یکپارچگی فناوری‌های امنیتی در نظر گرفته شود.

1 -Middleware.

2 -Context model.

3 -Sensory.

4 -Filtering.

5 -Web.

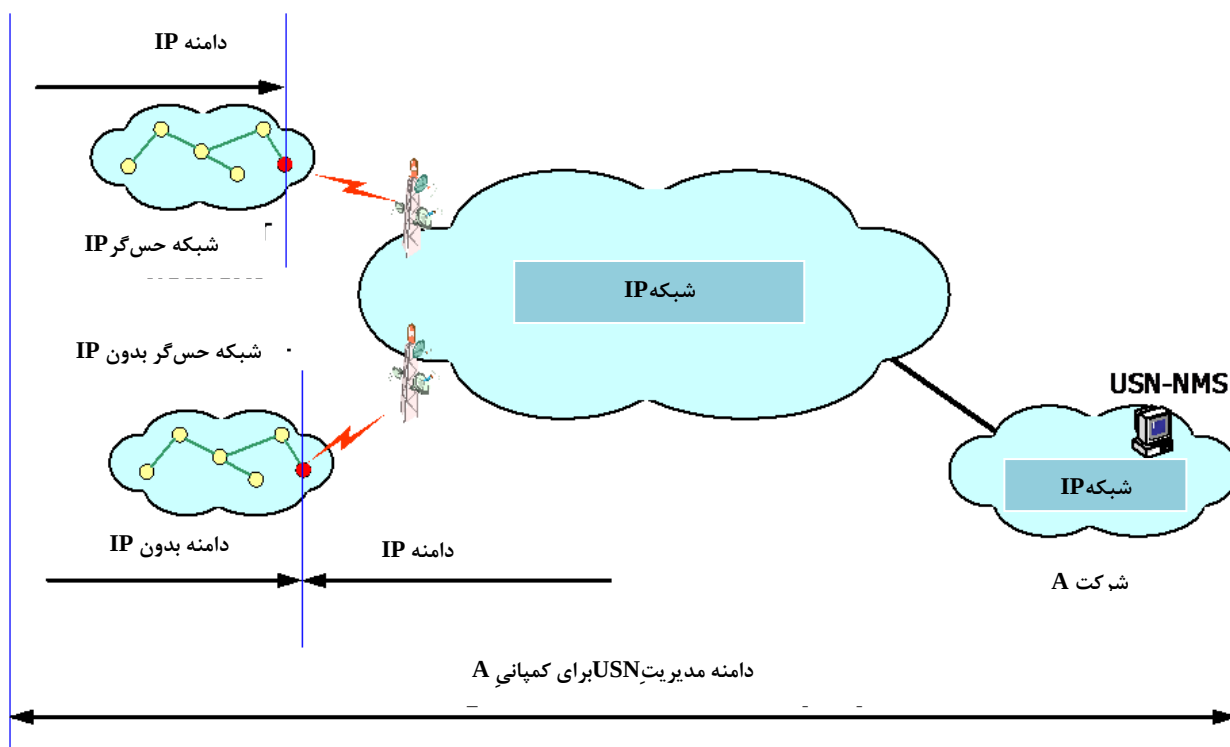
6 -Profile.

7 -Directory.

8 -Beaconده - گیرنده‌ای با بُرد کوتاه که ارتباط در مسیر را امکان‌پذیر می‌سازد.

9- Gateway.

10 -Interconnect.



شکل ۳ - پیکربندی شبکه USN

موارد زیر از مشخصات شبکه حس گر هستند:

- شبکه حس گر شامل بسیاری از گره‌های حس گر است که از طریق یک محیط بی‌سیم، در اتصال متقابل با یکدیگر هستند.
- گره‌های حس گر به طور فشرده در یک دامنه وسیع، یا در زمینه‌ای سخت و نامناسب^۱، استقرار می‌یابند.
- گره‌های حس گر در برابر خرابی^۲ آسیب پذیر^۳ هستند.
- ارتباط از ایستگاه پایه (BS) به گره حس گر از نوع پخش همگانی^۴ یا از نوع نقطه به نقطه^۵ خواهد بود.
- یک گره حس گر دارای توان، ظرفیت رایانشی و حافظه محدود است.
- یک گره حس گر ممکن است دارای شناسایی^۶ جهانی^۷ نباشد.

سه مؤلفه در SN وجود دارد: کارساز^۸ کاربردی^۹ که با گره ستانه^{۱۰} ارتباط برقرار می‌کند؛ گره ستانه، که ایستگاه پایه نامیده می‌شود که واسط بین شبکه حس گر و کارساز کاربردی است و مجموعه ای از گره‌های حس گر که از

1 -Hostile context.
2 -Failur.
3 -Vulnerable.
4 -Broadcast.
5 -Point-to-Point.
6 -Identification.
7 -Global identification.
8 -Server.
9 -Application.
10 -Sink

ارتباط بی سیم جهت ارتباط با یکدیگر استفاده می‌کنند. ستانه، ممکن است با کارساز کابردی از طریق اینترنت یا یک ماهواره ارتباط برقرار کند. معماری امنیتی در شبکه مبتنی بر IP بسیار مشابه با معماری امنیت در Rec.ITU-T X.805 | ISO/IEC 18028-2¹ است. بنابراین، این استاندارد، بر امنیت شبکه حس‌گر بی سیم (SN) متشکل از مجموعه‌ای از گره‌های حس‌گر با استفاده از انتقال بی سیم متمرکز است.

جهت ارتباط اطلاعاتی میان گره‌های حس‌گر، یک پیوند/پیوستگی² ایمن میان گره‌های حس‌گر باید، پیش از آنکه بتواند یک ارتباط ایمن میان آنها تحقق یابد، برقرار شود. توجه شود که به هر صورت، مشخصات شبکه حس‌گر در زیر، طراحی ارتباط ایمن را بسیار دشوار نشان می‌دهد:

- **دشواری در استفاده از سامانه‌های رمز³ کلید عمومی:** محدودیت توان رایانشی، اندازه حافظه و منبع تغذیه، استفاده از سامانه رمز کلید عمومی – مانند توافق کلید Diffie-Hellman، یا امضا و رمزگذاری RSA⁴ – را بسیار دشوار می‌کند. اگرچه که، یک گره حس‌گر ویژه ممکن است منابع کافی برای اجرای عملیات‌های بسیار پیچیده مورد نیاز برای سامانه رمز کلید عمومی داشته باشد، اما ممکن است در برابر حمله بندآوری خدمات که در بند ۷-۱-۱ شرح داده می‌شود، آسیب پذیر باشد.
- **آسیب پذیری گره‌های حس‌گر:** از آنجایی که گره‌های حس‌گر ممکن است در مکان‌های با شرایط نامناسب⁵ و سخت به کاراندازی شوند/استقرار یابند⁶، ایمنی آنها ممکن است شکسته شود⁷. مهاجم⁸، پس از بدست آوردن دسترسی فیزیکی به گره حس‌گر، قادر به دستیابی به اطلاعات حساس از جمله اطلاعات کلید یا اطلاعات دریافت شده، است. استفاده از یک گره حس‌گر مقاوم در برابر مداخله⁹ می‌تواند جلوی این حمله را بگیرد که متضمن هزینه بالا است. به علاوه، بکارگیری گره حس‌گر مقاوم در برابر مداخله بسیار دشوار است چراکه ممکن است منجر به یک شبکه پرهزینه شود. اگرچه برای برخی کاربردها (برای مثال کاربردهای حساس در مورد ایمنی، ارتش و غیره)، بکارگیری گره‌های حس‌گر مقاوم در برابر مداخله، و در نتیجه هزینه‌های بالاتر می‌تواند قابل قبول باشد.
- **دشواری در کسب دانش پس از بکار اندازی/استقرار:** در بسیاری از موارد، گره‌های حس‌گر به روشی به صورت تصادفی پراکنده بکار اندازی خواهند شد/استقرار خواهند یافت؛ از این رو دشواری در شناخت مکان همسایگی گره‌ها برای پروتکل امنیتی وجود دارد.
- **محدودیت در اندازه حافظه، توان انتقال و پهنای باند انتقال:** از آنجایی که حافظه در گره‌های حس‌گر محدود است، ذخیره کلیدهای یکتا¹⁰ استفاده شده توسط سایر گره‌های حس‌گر در شبکه بسیار دشوار است. به علاوه یک گره حس‌گر معمولی، دارای ظرفیت پایین از نظر پهنای باند انتقال و توان ارتباط با گره‌های همسایه است.

۱ -مجموعه استاندارد ملی ۱۱۲۱۰ قسمتهای یک و دو سال ۱۳۸۷ با منابع بین المللی ISO/IEC 18028-1:2006 و ISO/IEC 18028-2:2006 موجود است.

2 -Association.

3 -Cryptosystem.

4 -RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman.

5 -Hostile location.

6 -Deploy.

7 -Compromise.

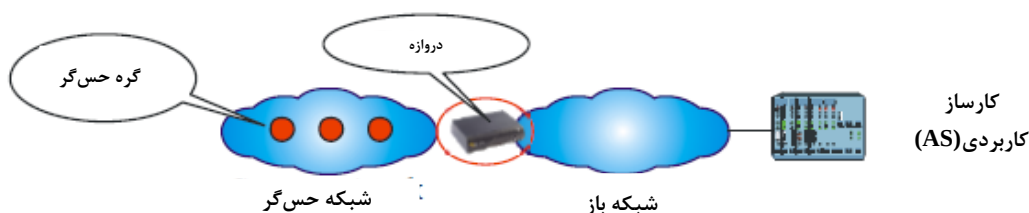
8 -Attacker.

9 -Tamper resistant.

10 -Unique.

• **تک نقطه^۱ خرابی ایستگاه مبنا:** در شبکه‌های حس گر، ایستگاه مبنا، دروازه‌ای برای ارتباط اطلاعات حس شده به یک کارساز کاربردی، از طریق شبکه هسته ای مبتنی بر IP است. امنیت شبکه حس گر بر پایه امنیت ایستگاه مبنا است. بنابراین، ایستگاه‌های مبنا می‌توانند هدفی جذاب برای انواع مختلف حمله باشند.

شکل ۴ یک مدل کلی از یک ارتباط انتها به انتها^۲ را میان یک گره حس گر در SN و یک AS نمایش می‌دهد. ممکن است مواردی وجود داشته باشند که در آن کارساز کاربردی در دروازه مستقر است.



شکل ۴ - مدل کلی یک ارتباط انتها به انتها میان یک گره حس گر در SN و AS

لایه‌های بالقوه برای پیاده‌سازی^۳ کارکرد امنیت در USNها در شکل ۵ نشان داده شده است. لایه امنیتی پایه، در تناظر با لایه پیوند^۴ یا MAC، مسئول انتقال داده‌های پیوند با پیوند^۵، میان گره‌های حس گر، یا میان گره‌های حس گر و یک دروازه است. لایه خدمت^۶، در تناظر با لایه شبکه^۷، مسئول انتقال داده‌های شبکه، میان گره‌های حس گر، و میان یک گره حس گر و یک دروازه است. مثال‌های معمول، از لایه خدمت، شامل انتقال پیام‌های پخش همگانی از دروازه به گره حس گر و برعکس می‌شود. امنیت لایه خدمت و امنیت لایه کارکرد پایه^۸، باید کارکردهای امنیتی شرح داده شده در بند ۱۰ را، در تناظر با لایه شبکه و لایه پیوند، پیاده کند. باید توجه شود که در برخی از کاربردها، کارکرد امنیتی کاربردی، به جای قرار گیری در کارساز کاربردی، در یک دروازه مستقر می‌شود.

1- Single point.

2 -End-to-end.

3 -Implement.

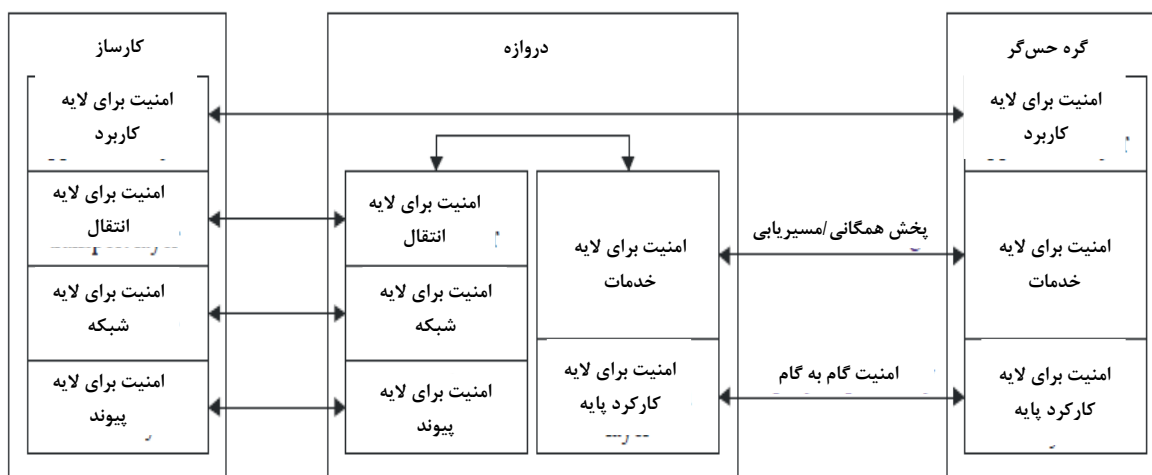
4- link layer.

5- Link-by-Link.

6- Service layer.

7 -Network layer.

8- Basic function layer.



شکل ۵ - لایه های پیاده سازی کارکردهای امنیت برای USN

۷ تهدیدات و مدل های امنیتی برای شبکه های حس گر همه جاگاه

تهدیدات برای USN ها به تهدیدات برای شبکه IP و تهدیدات برای SN طبقه بندی می شوند.

۷-۱ مدل های تهدید در شبکه های حس گر

دو نوع مهاجم در SN وجود دارد: یک مهاجم نوع خرده^۱ و یک مهاجم نوع لپ تاپ^۲. در مورد اول، مهاجم دارای قابلیت مشابه با گره حس گر است؛ این نوع می تواند به تعداد کمی از گره های حس گر دسترسی داشته باشد. یک مهاجم با افزاره نوع خرده ممکن است موجب اختلال^۳ در پیوند رادیویی نزدیکی خود شود. در مورد دوم، یک مهاجم ممکن است به افزاره های قدرتمندتر مانند رایانه های لپ تاپ دسترسی داشته باشد. یک مهاجم با یک افزاره نوع لپ تاپ می تواند ارتباط در شبکه حس گر را استراق سمع^۴ کند و دارای پهنای باند بالا، و کانال ارتباطاتی با تاخیر پایین، باشد؛ همچنین می تواند کل شبکه حس گر را با استفاده از یک فرستنده با توان بالاتر، مختل کند. دو نوع تهدید برای SN وجود دارد: تهدیدات کلی، و تهدیدات مرتبط با مسیریابی. تهدیدات در SN به ارتباط میان ایستگاه مبنا و گره حس گر، و میان گره ها، همانطور که در بند ۷-۱-۱ شرح داده می شود، اعمال می شود. تهدیدات مرتبط با مسیریابی، به تبادل پیام مسیریابی، همانطور که در بند ۷-۱-۲ شرح داده می شود، اعمال می شود.

۷-۱-۱ تهدیدات کلی در شبکه های حس گر

1- Mote-type.
2- Laptop-type.
3 -Jam.
4 -Eavesdrop.

¹ 2-7498 ISO/IEC | Rec. ITU-T X.800 و 2-18028 ISO/IEC | Rec. ITU-T X.805 به تهدیدات امنیتی زیر را برای شبکه‌ها، اشاره می‌کنند. (باید توجه شود که این موارد تهدیدات امنیتی قابل کاربرد برای SN نیز هستند):

- تخریب^۲ اطلاعات و/یا دیگر منابع
- خرابی^۳ یا تغییر^۴ اطلاعات
- سرقت^۵، برداشتن^۶ یا از دست دادن اطلاعات و/یا دیگر منابع
- افشاء^۷ اطلاعات
- قطع^۸ خدمات

علاوه بر این‌ها، تعداد زیادی تهدیدات ویژه گره حس‌گر وجود دارد همچون آسیب‌پذیری گره حس‌گر، استراق سمع، حریم داده‌های حس شده، حمله بندآوری خدمات و استفاده بدخواهانه^۹ از شبکه تجاری^{۱۰} (به چان و همکاران در کتابنامه مراجعه شود).

- آسیب‌پذیری گره‌های حس‌گر: انتظار می‌رود شبکه‌های حس‌گر متشکل از صدها یا هزاران گره حس‌گر باشند. هر گره نمایانگر یک نقطه بالقوه حمله است. پایش و حفاظت از هر حس‌گر منفرد، چه از حمله فیزیکی و چه از یک حمله منطقی، غیرعملی است. شبکه‌ها ممکن است در یک منطقه وسیع پراکنده و بیشتر آنها در معرض مهاجمانی که گره‌های حس‌گر منفرد را گیرانداخته^{۱۱} و برنامه‌نویسی مجدد می‌کنند باشند. مهاجمان همچنین می‌توانند گره‌های حس‌گر تجاری^{۱۲} خود را بگیرند و شبکه را القا^{۱۳} به پذیرش آنها به عنوان گره‌های برحق^{۱۴} کنند یا می‌توانند ادعای هویت‌های چندگانه برای یک گره تغییر یافته، نمایند. مهاجم می‌تواند با به فرمان گرفتن تعداد کمی از گره‌ها در داخل شبکه، حملات گوناگونی را همچون تحریف^{۱۵} داده‌های حس‌گر، استخراج اطلاعات حس شده خصوصی از خواندن‌های شبکه حس‌گر، و بندآوری خدمات را ایجاد کند. حل مشکل آسیب‌پذیری گره حس‌گر مستلزم راه حل‌های فناوری است. برای مثال، سخت افزار ارزان مقاوم در برابر مداخله، می‌تواند چالشی برای برنامه نویسی مجدد گره‌های حس‌گر گیرافتاده، باشد. اگرچه که، قدرتمند کردن گره‌ها در برابر مداخله، از نظر اقتصادی مناسب نیست. بنابراین باید این گونه فرض شود که یک مهاجم می‌تواند زیرمجموعه‌ای از

۱ - استاندارد ملی ایران به شماره ۱۶۲۷۴-۲ سال ۱۳۹۲ با منبع بین المللی ISO 7498-2:1989 نگارش شده است.

2- Destruction. وضعیتی که در آن قابلیت زیرساخت‌های مهم برای ارائه محصول یا خدمات در سطح مورد انتظار به مشتری از بین می‌رود.

3- Corruption. عملی که کارکرد یک سامانه را با خرابکاری در عملیات یا داده‌های آن به گونه‌ای نامطلوب تغییر می‌دهد.

4 -Modification.

5- Theft.

6- Removal.

7- Disclosure.

8 -Interruption.

9 -Malicious.

10- Commodity network.

11- Capture.

12 -Commodity sensor.

13 -Induce.

14 -Legitimate.

15- Falsification.

گره‌های حس‌گر را به خطر اندازد. از این رو، در سطح نرم افزاری، شبکه‌های حس‌گر برای تضمین عملیات ایمن، حتی با وجود تعداد کمی از گره‌های شبکه بدخواه، به قابلیت‌های جدید نیاز دارد. ^۱ *صالت* سنجی گره به گره^۱، یکی از پایه‌های تشکیل دهنده فعال ساختن گره‌های حس‌گر برای اثبات هویتشان به یکدیگر است. سپس، *ابطال*^۲ گره می‌تواند گره‌های بدخواه را جدا سازد. دستیابی به این اهداف، با در نظر گرفتن محدودیت منبع سخت افزاری، مستلزم پروتکل‌های امنیتی سبک^۳ خواهد بود. علاوه بر این، تمام ارتباطات و تمامی پروتکل‌های پردازش داده مورد استفاده در شبکه‌های حس‌گر باید برگشت‌پذیر^۴ باشد، یعنی بتواند حتی با تعداد کمی از گره‌های بدخواه، با اثربخشی بالا کار کند. برای مثال، پروتکل‌های مسیریابی باید در مقابل گره‌های به خطر افتاده‌ای^۵ که به صورت مخرب رفتار می‌کنند، برگشت‌پذیر باشند.

- **استراق سمع:** در ارتباطات شبکه حس‌گر بی‌سیم، یک مهاجم^۶ می‌تواند با پایش انتقال‌ها^۷ میان گره‌ها، دسترسی به اطلاعات خصوصی را به دست آورد. برای مثال، چند گیرنده بی‌سیم که در خارج خانه قرار داشته باشند ممکن است بتوانند خواندن‌های نور و درجه حرارت شبکه‌های حس‌گر داخل خانه را، پایش کنند، بنابراین اطلاعات تفصیلی در مورد فعالیت‌های روزانه شخصی ساکنین را فاش می‌کنند. رمزبندی کردن^۸ ارتباطات گره حس‌گر، تا اندازه‌ای مشکلات استراق سمع را حل می‌کند، اما مستلزم و طرح^۹ توزیع و مبادله کلید قوی است. اجرای این طرح باید برای مالک شبکه ساده باشد و پیاده‌سازی^{۱۰} آن با توجه به محدودیت سخت‌افزاری گره حس‌گر، امکان‌پذیر باشد. همچنین باید رازمانی^{۱۱} را، در مابقی شبکه، هنگامی که یک مهاجم، چند گره حس‌گر را به خطر می‌اندازد و کلیدهای مخفی^{۱۲} را افشاء^{۱۳} می‌کند، حفظ کند. به طور ایده آل، همچنین این الگوها، باطل شدن^{۱۴} کلیدهای افشاء شده مشخص و کلیدگذاری مجدد گره‌های حس‌گر را امکان‌پذیر می‌کنند. با توجه به تعداد زیاد گره‌های ارتباطی، رمزنگاشتی انتها به انتها^{۱۵}، از آنجایی که سخت افزار گره حس‌گر، به ندرت می‌تواند تعداد زیادی از کلیدهای رمزبندی یکتا را ذخیره کند، غیرعملی است. در عوض، طراحان شبکه حس‌گر ممکن

1- Node to node.

2- Revocation.

3- Lightweight.

4- Resilient.

5- Compromised.

6- Adversary. هستاری که به سامانه حمله می‌کند یا تهدیدی برای آن به شمار می‌آید.

7- Transmission.

8- Encrypting. تغییر دادن اطلاعات به نحوی که برای اشخاص یا طرف‌های غیرمجاز نامفهوم باشد.

9- Scheme.

10- implement.

11- Secrecy.

12- Secret key.

13- Expose.

14- Revocation.

15- End-to-end.

است رمزبندی گام به گام^۱ را انتخاب کنند که در آن هر گره حس گر، تنها کلیدهای رمزبندی را ذخیره می کند که با نزدیکترین همسایه مجاورش به اشتراک می گذارد. در این مورد، واپایش مهاجم یک گره ارتباطی، میزان اثربخشی رمزبندی را، برای هر ارتباط هدایت شده (مستقیم)^۲ از طریق آن گره به خطر افتاده را برطرف می کند. این وضعیت، می تواند در صورتی که یک مهاجم زیرساخت مسیریابی را برای ارسال بسیاری از ارتباطات از طریق یک گره مخرب تغییر دهد، تشدید کند. پروتکل های مسیریابی قوی تر به عنوان یک راه حل برای این مشکل عمل می کنند. راه حل دیگر مسیریابی چندین مسیر است، که قسمتهایی از یک پیام از طریق چندین مسیر منفصل سیر می کنند و آنها را در مقصد دوباره سرهم می کنند. مسیریابی چندین مسیر ممکن است برگشت پذیری USN را، برای حملات یا خطرات افزایش دهد. کشف کارای^۳ بهترین مسیرهای منفصل مورد استفاده در برای چنین عملیاتی، چالش تحقیقاتی دیگری را مطرح می کند. باید توجه شود که این تهدید در شبکه هسته ثابت رخ می دهد و با نقض حریم در شبکه حس گر ارتباط دارد.

● **رازمانی داده های حس شده:** شبکه های حس گر ابزارهای^۴ انبوهش اطلاعات هستند؛ مهاجم می تواند به وسیله دسترسی به داده های ذخیره شده حس گر، یا پرسرمان^۵ یا استراق سمع شبکه، به اطلاعات حساس دسترسی یابد. مهاجمان حتی می توانند، اطلاعات حساس را، با استفاده از داده های به ظاهر بی ضرر^۶، مشتق نمایند، در صورتی که بدانند چگونه دروندادهای چندین حس گر را به یکدیگر مرتبط کنند. برای مثال، یک مهاجم که دسترسی به حس گرهای درون بنا و هم خارج بنای یک خانه را بدست می آورد، ممکن است که بتواند نوفه داخلی^۷ را از نوفه خارجی^۸ مجزا^۹ کند و در نتیجه جزئیات فعالیت های خصوصی ساکنان را استخراج کند. به هر صورت، این واقعیت که شبکه های حس گر، انبوهش اطلاعات را فعال می سازد، که در صورت عدم وجود این شبکه ها، انبوهش آنها غیر ممکن خواهد بود، مشکل اصلی حریم نمی باشد. در واقع در شبکه های حس گر، به ندرت، مقدار اطلاعات زیادی از طریق مراقبت^{۱۰} مستقیم مکان، می تواند جمع آوری شود. شبکه های حس گر مشکل حریم را تشدید می کند، چراکه حجم زیادی از اطلاعات را، به راحتی با دسترسی از دور^{۱۱}، دسترس پذیر^{۱۲} می کنند. از این رو نیازی به حضور فیزیکی مهاجمان برای نگه داشت مراقبت وجود ندارد. آنها می توانند اطلاعات را به شیوه ناشناس^{۱۳}، با

1- Hop to hop

2 -Direct.

3 -Efficient.

4 -Tools.

5-Query.

6- Innocuous

7- Internal noise.

8 -External noise.

9 -Isolate.

10- Surveillance.

11- Remote access.

12- Available.

13 -Anonymous.

خطر پایین^۱ جمع‌آوری کنند. دسترسی از دور، به یک تک مهاجم اجازه می‌دهد تا چندین مکان را به صورت همزمان^۲ پایش کند. تضمین اینکه اطلاعات حس‌شده، در داخل شبکه حس‌گر باقی می‌ماند و تنها قابل دسترسی برای طرف‌های مورد اعتماد است، گامی ضروری برای تضمین حریم است. رمزبندی داده‌ها و واپایش دسترسی به عنوان یک رویکرد مورد استفاده قرار می‌گیرد. روش دیگر محدود کردن توانایی شبکه، برای جمع‌آوری تفصیلی داده‌ها، به روشی که بتواند حریم را به خطر اندازد، است. برای مثال، یک شبکه حس‌گر ممکن است داده‌ها را، فقط با گزارش درجه حرارت انبوهش شده^۳ در سرتاسر یک منطقه وسیع، یا مکان‌های تقریبی حس شده جداگانه، گمنام سازد^۴. یک سامانه، داده‌های حس شده را در یک دادگان گمنام شده^۵، با برداشتن جزئیاتی که ممکن است از نظر یک مهاجم مفید باشد، ذخیره می‌کند. رویکرد دیگر، پردازش پرسمان‌ها در شبکه حس‌گر به شیوه توزیع شده است، از این رو هیچ گره منفردی نمی‌تواند نتایج پرسمان را به تمامیت مشاهده کند. این رویکرد، از سامانه دارای پتانسیل مورد سو استفاده واقع شدن، به وسیله گره‌های بدخواه به خطر افتاده، حفاظت می‌کند.

● **حملات DoS:** با توجه به کاربرد بیشتر شبکه‌های حس‌گر در کاربردهای بحرانی ایمنی، پتانسیل آسیب ناشی از قطع عملیات، قابل توجه است. دفاع در مقابل حملات بندآوری خدمت – که با هدف تخریب کارکرد شبکه به جای خرابکاری در آن یا استفاده از اطلاعات حس شده انجام می‌شوند – به شدت دشوار است. حملات DoS می‌توانند در لایه فیزیکی رخ دهد، برای مثال از طریق اختلال رادیویی. این حملات همچنین شامل انتقال‌های بدخواهانه به شبکه برای تداخل^۶ با پروتکل های شبکه حس‌گر یا تخریب فیزیکی گره‌های شبکه مرکزی است. مهاجمان می‌توانند سبب تخلیه شارژ باتری در گره‌های حس‌گر شوند – برای مثال با ارسال مجموعه‌های متداومی از ارتباطات بی‌استفاده که گره‌های مورد هدف را مجبور به مصرف انرژی در پردازش آنها و پیش‌سویی/هدایت^۷ آنها به گره‌های دیگر می‌کند. در صورتی که مهاجمان بتوانند حریم گره‌های حس‌گر را بشکنند، حملات دسیسه‌آمیز^۸ بیشتر می‌توانند از داخل شبکه حس‌گر رخ دهند. برای مثال، می‌توانند حلقه‌های مسیریابی را ایجاد کنند که در نهایت تمام گره‌ها را در حلقه، از پای درخواهد آورد. پتانسیل دفاع در برابر حملات بندآوری خدمات به گوناگونی خود حملات است. فنونی مانند ارتباط طیف گسترده^۹ یا پرش بسامد^{۱۰} می‌تواند برای مقابله با حملات اختلالی باشد. اصالت‌سنجی مناسب می‌تواند از پذیرش پیام‌های تزریق شده به شبکه جلوگیری کند. باید توجه شود که به هر جهت، پروتکل های درگیر، باید به اندازی کارا باشند که

1 -Low-Risk

2- Simultaneously.

3- Aggregate. جمع‌آوری و گردآوری و هم‌گذاری داده‌هایی که از دو یا چند منبع مختلف گرفته می‌شوند.

4- Anonymize ناممکن سازی ردگیری فعالیت‌ها در اینترنت است.

5- Anonymized data base.

6 -Interfer.

7- Forward.

8 -Insidious.

9 -Spread-spectrum.

10-Frequency hopping. تغییر مداوم و سریع و نامنظم بسامد فرستنده ارتباطی برای جلوگیری از رهگیری یا ایجاد اختلال توسط سامانه‌های شنود یا اختلالگر دشمن.

خودشان هدف یک حمله فراگیر از پای درآمدن انرژی^۱ نشوند. برای مثال، استفاده از امضاها مبتنی بر رمزنگاری نامتقارن می‌تواند اصالت‌سنجی پیام را فراهم سازد. به هر جهت، ایجاد و درستی سنجی امضاها نامتقارن به شدت از نظر رایانشی قوی هستند و مهاجمانی که می‌توانند تعداد زیادی از این عملیات‌ها را سبب شوند می‌توانند یک حمله فراگیر از پای در آوردگی انرژی را مهیا کنند.

• **استفاده بدخواهانه از شبکه‌های تجاری:** ازدیاد^۲ شبکه‌های حس‌گر، به طور اجتناب ناپذیری^۳، موجب استفاده آنها برای مجرمانی^۴ که می‌توانند از آنها برای اهداف غیرقانونی^۵ استفاده کنند، می‌شود. برای

مثال، دزدان^۶ می‌توانند در حس‌گرهای خودکارسازی^۷ خانه رخنه^۸ کنند یا حتی به سادگی فعالیت ساکنین را، برای بدست آوردن اطلاعات خصوصی آنها درمورد حضور، موقعیت مکانی و سایر اطلاعات مالکان، استراق سمع کنند و براساس آن عمل کنند. در صورتی که حس‌گرها به اندازه کافی کوچک باشند، می‌توانند در رایانه‌ها و در تلفن‌های همراه نصب شوند تا اطلاعات شخصی و اسم رمز^۹ استخراج شوند. چنین استفاده گسترده‌ای، موانعی همچون قابلیت دسترس‌پذیری و هزینه، که چنین حملاتی را سست می‌کنند را، پایین خواهد آورد. آشکارساز^{۱۰} حس‌گر، یک نوع دفاع ممکن را، در مقابل چنین حملاتی ارائه می‌دهد. یک آشکارساز نه تنها باید بتواند حضور ارتباطات بی سیم به طور بالقوه خصمانه را، که ممکن است دارای سطوح قابل توجهی از تداخل‌های رادیویی باشند را، در یک منطقه آشکار سازد، بلکه باید بتواند میان انتقال مجاز و غیرمجاز شبکه‌های حس‌گر و افزاره‌های دیگر، تمایز قائل شوند. اگرچه چنین فناوری‌هایی ممکن است نتواند از استقرار شبکه‌های حس‌گر طرف‌های غیرمجاز، در مناطق حساس، جلوگیری کند، اما آنها را پرهزینه‌تر می‌کند و از این رو مشکل را کاهش می‌دهد.

۷-۱-۲ تهدیدات ویژه مسیریابی

Rec. ITU-T X.805 | ISO/IEC 18028-2 و Rec. ITU-T X.800 | ISO/IEC 7498-2 پنج تهدید را که برای مبادله پیام مرتبط با مسیریابی در SN به کار می‌روند را، شناسایی می‌کند. به علاوه، با توجه به پیام‌های مسیریابی مبادله‌شده میان گره‌های حس‌گر هفت تهدید شناسایی می‌شوند. (به Karlof و همکارانش در کتابنامه مراجعه شود).

• **اطلاعات مسیریابی جعل شده^{۱۱}، تغییر یافته^{۱۲} و دوباره به جریان انداخته شده^{۱۳}:** مهاجم قادر است تا اطلاعات مسیریابی را جعل کند، تغییر دهد و دوباره به جریان اندازد که ایجاد یک حلقه مسیریابی را

1 -Energy-Exhausting target.

2- Proliferation.

3- Inevitably.

4 -Criminals.

5 -Illegal.

6- Thieves.

7 -Automation.

8 -Hack.

9 -Password.

10- Detector.

11 -Spoofed.

12 -Altered.

13 -Replayed.

فعال ساخته، و موجب بالابردن ترافیک شبکه، گسترش مسیریابی و افزایش رکود/تاخیر سراسری می‌شود.

• پیشسویی (هدایت) انتخابی^۱: این مورد به حمله‌ای اشاره دارد که در آن یک گره به خطر افتاده به وسیله یک مهاجم، ممکن است پیشسویی (هدایت)^۲ پیام‌های معین را رد می‌کند و آنها را رها^۳ می‌کند که موجب توقف انتشار^۴ می‌شود.

• حمله گودال (چاهک ستانه)^۵: به حمله‌ای مربوط است که در آن مهاجم، تمام ترافیک یک منطقه معین را، از طریق یک گره به خطر افتاده، جذب می‌کند.

• حملات سایبیل^۶: به حمله‌ای اشاره دارد که در آن یک تک گره، هویت‌های چندگانه را برای گره‌های دیگر در شبکه نمایش می‌دهد که هر گره را متقاعد می‌کند که یک مهاجم، در بیش از یک محل، در یک زمان وجود دارد.

• حملات کرمچاله^۷: در یک حمله جای کرمچاله، یک مهاجم مسیر پیام‌های دریافت شده در یک قسمت را، در یک پیوند، تعیین مسیر می‌کند و آنها را در یک قسمت متفاوت برمی‌گرداند. حملات کرمچاله دو گره مجزای بدخواه را در برخواهد گرفت که برای درک فاصله خود از یک دیگر با برگرداندن بسته در راستای یک کانال خارج از باند، که تنها در اختیار مهاجمان است، با هم همکاری میکنند.

• حملات جریان HELLO^۸: به حملاتی اشاره دارد که در آن یک مهاجم از نوع لپ تاپ بسته‌های HELLO را منتشر می‌کند که هر گره در شبکه را متقاعد می‌کند که مهاجم همسایه‌اش است.

• جعل تایید: یک مهاجم می‌تواند تایید لایه پیوند را برای بسته‌ای که با هدف گره همسایه فرستاده می‌شود، جعل کند به طوری که فرستنده را متقاعد می‌کند که یک پیوند ضعیف، قوی است یا یک گره از کار افتاده یا غیرفعال، فعال است.

باید توجه شود که حملات ساده‌ای، که هریک از تهدیدات شرح داده شده در قسمت بالا را استفاده می‌کنند، ممکن است به‌طور ترکیبی، ایجاد حملات پیچیده تر (برای مثال ترکیب سایبیل و چاهک ستانه (گودال) یا کرمچاله) را نمایند.

۲-۷ مدل‌های تهدید در شبکه‌های پروتکل اینترنت (IP)^۹

مدل‌های تهدید مطرح شده در Rec.ITU-T X.805 | ISO/IEC 18028-2 می‌تواند در شبکه IP بکار رود بنابراین درمورد جزئیات این تهدیدات به Rec.ITU-T X.805 | ISO/IEC 18028-2 مراجعه شود.

۳-۷ مدل امنیت برای USNها

1- Selective forwarding.

2 -Forward.

3 -Drop.

4 -Propagation.

5 -Sinkhole.

6 - Sybil.

7 -Wormhole. لوله‌ای فرضی در خمینه فضا - زمان که ناحیه‌های بسیار دور را به هم نزدیک می‌کند.

8 -Hello flood.

9 -Internet protocol.

مدل امنیت نشان داده های شده در شکل ۶ چارچوب کاری کلی امنیت USN را مبتنی بر حوزه کاربردی USN، ساختار کلی USN و پیکر بندی شبکه USN نشان می دهد. این مدل مبتنی بر ISO/IEC 15408-1، به برقراری مفاهیم و روابط امنیتی در امنیت USN کمک می کند. زمانی که USN مورد تهدید واقع می شود، سیاست های/خط مشی های امنیتی مناسب باید برای رسیدن به اهداف امنیتی با استقرار فناوری های امنیتی مناسب و الزامات کارکردی امنیتی ویژه، انتخاب شوند.



شکل ۶ - مدل امنیت برای USN

۸ ابعاد امنیتی کلی برای USN

یک بعد امنیتی، مجموعه ای از اقدامات امنیتی طراحی شده جهت توجه به جنبه خاصی از امنیت شبکه برای حفاظت در مقابل تمام تهدیدات امنیتی مهم است؛ بعد به شبکه محدود نمی شود و به کاربردها و اطلاعات کاربر نهایی نیز بسط می یابد.

برای مقابله با تهدیدات فوق الذکر هم در شبکه IP و هم SN ابعاد امنیتی زیر در Rec. ITU-T X.805 | ISO/IEC 18028-2 کاربردپذیر است:

- **محرمانگی^۱ داده ها:** یک شبکه حس گر نباید موارد خوانده شده حس گر را، برای شبکه های همسایه نشت^۲ دهد. در بسیاری از کاربردها (برای مثال توزیع کلید) گره ها، داده های به شدت حساس را، ارتباط می دهند. رویکرد استاندارد برای محرمانه نگه داشتن داده های حساس، رمزبندی^۳ داده ها با یک کلید مخفی^۴ که تنها گیرنده های در نظر گرفته شده، دارای آن می باشند، است. از این رو محرمانگی تضمین می شود.

1 -confidentiality.

2 -Leak.

3 -Encrypt.

4 -Secret key.

- **اصالت سنجی داده‌ها^۱/شناسایی^۲ داده‌ها:** اصالت سنجی پیام برای بسیاری از کاربردها در شبکه‌های حس‌گر مهم است. در ساختار شبکه حس‌گر، اصالت سنجی، برای بسیاری از وظایف^۳ اجرایی (برای مثال، برنامه نویسی مجدد یا واپایش چرخه وظیفه گره حس‌گر) ضروری است. یک مهاجم می‌تواند به آسانی پیام‌هایی را تزریق^۴ کند؛ بنابراین گیرنده نیاز دارد تا مطمئن شود که داده‌هایی را که در هر فرآیند تصمیم‌گیری، مورد استفاده قرار می‌دهد از طرف^۵ مبدا صحیحی است. اصالت‌سنجی داده‌ها به یک گیرنده اجازه می‌دهد تا تأیید^۶ کند که داده‌ها واقعاً توسط فرستنده‌ای^۷ که مدعی^۸ آن است، ارسال شده است. شناسایی، به هدف اثبات هویت^۹ هستار یا هویت گره حس‌گر است. در مورد ارتباط دوطرفه^{۱۰}، اصالت‌سنجی داده‌ها، می‌تواند از طریق یک سازوکار کاملاً متقارن تحقق یابد: فرستنده و گیرنده یک کلید مخفی را برای رایانش کد اصالت سنجی پیام (MAC) تمام داده‌های ارتباطی به اشتراک می‌گذارند. زمانی که یک پیام با MAC صحیح می‌رسد، گیرنده می‌داند که توسط فرستنده ارسال شده است. این روش اصالت سنجی، برای تنظیمات پخش همگانی، نمی‌تواند بکار گرفته شود مگر با فرض نمودن اعتماد بیشتر به گره‌های شبکه. ارسال داده‌های اصالت سنجی شده، به گیرنده‌های غیرقابل اعتماد^{۱۱} متقابل^{۱۲}، با استفاده از یک MAC متقارن، ناامن است، چراکه هریک از گیرنده‌ها کلید MAC را می‌داند و به تبع آن، می‌تواند خود را به جای فرستنده بنمایاند^{۱۳} و پیام‌ها را به سوی گیرنده‌های دیگر جعل^{۱۴} کند. بنابراین یک سازوکار نامتقارن مورد نیاز است تا پخش همگانی اصالت‌سنجی شده، را فعال کند. یک روش، ساخت پخش همگانی اصالت‌سنجی شده، تنها از سوی نخستین‌های متقارن و معرفی عدم تقارن با افشاء تأخیر کلید و زنجیره‌های کلید کارکردی یک طرفه، است. سازوکارهای اصالت‌سنجی، به طور اساسی برای تأیید برحق بودن^{۱۵} گره، مورد استفاده قرار می‌گیرد. بنابراین حقیقی بودن و قابلیت اطمینان و اعتماد^{۱۶} گره تضمین می‌شود.
- **یکپارچگی^{۱۷} داده‌ها:** در ارتباط، یکپارچگی داده‌ها، گیرنده را مطمئن می‌کند که داده‌های دریافت شده در هنگام گذر، توسط یک مهاجم تغییر داده نشده است.

1 - Authentication. اقدامی امنیتی برای حفاظت از سامانه‌های ارتباطی در برابر شبیه‌سازی تقلبی که از طریق تشخیص اعتبار تماس گیرنده یا پیام یا سامانه انجام می‌شود.

2 - Identification. فرایند شناخته شدن هستار در شبکه.

3 - Task.

4 - Inject.

5 - Originated.

6 - Receiver.

7 - Verify.

8 - Sender.

9 - Claiming.

10 - Identity.

11 - Two-party.

12 - Mutually.

13 - Impersonate.

14 - Forge.

15 - Legitimacy.

16 - Credibility.

17 - Integrity.

- **واپایش دسترسی:** واپایش دسترسی تضمین می‌کند که تنها کاربر یا هستار مجاز، مجاز است تا دسترسی به اطلاعات، منبع، یا خدمات را، به‌دست آورد.
 - **سلب انکار^۱:** سلب انکار، تضمین می‌کند که هستار یا کاربر نمی‌تواند فعالیت‌هایی را که در شبکه انجام می‌دهد را، انکار کند.
 - **امنیت ارتباط:** امنیت ارتباط تضمین می‌کند که اطلاعات تنها از مبدا به مقصد جریان می‌یابد.
 - **دسترس پذیری^۲:** دسترس‌پذیری تضمین می‌کند که اطلاعات، خدمت و برنامه کاربردی برای کاربران مجاز در هر زمانی قابل دسترسی است.
 - **حریم:** حریم شخصی تضمین می‌کند که شناسانه^۳ کاربر یا شناسانه هستارها و استفاده از شبکه، محرمانه نگهداری می‌شوند.
- علاوه بر ابعاد امنیت که در بالا شرح داده‌ها شدند، بعد «برگشت‌پذیری در برابر حملات» از طریق طراحی مناسب پروتکل‌های مسیریابی /PHY/MAC، می‌باید تنها برای قسمت SN افزوده شود.
- **برگشت‌پذیری در برابر حملات:** این بعد، به هریک از اقدامات برای بازیابی از حملات گوناگون در USN اشاره دارد. این قابلیت تضمین می‌کند که USN می‌تواند از حملات بهبود یابد، به گونه‌ای که قادر به شناسایی/برگشت‌پذیرماندن، در برابر حملات گوناگون از طریق طراحی مناسب پروتکل‌های مسیریابی /PHY /MAC است. برگشت‌پذیری، در مقابل حملات شامل برگشت‌پذیری در مقابل گره‌های به خطر افتاده، برگشت‌پذیری در مقابل استراق سمع اطلاعات مسیریابی و غیره می‌شود.
- ۹ تهدیدات و ابعاد امنیتی در شبکه‌های حس گر همه جاگاه**
- تبادل پیام در SN می‌تواند در سه دسته طبقه بندی شود: تبادل پیام میان گره‌ها، تبادل پیام میان یک ایستگاه پایه و یک گره، و مبادله پیام برای پیام‌های مرتبط با مسیریابی.
- ۹-۱ تهدیدات و ابعاد امنیتی برای مبادله پیام در شبکه‌های حس گر همه جاگاه**
- ۹-۱-۱ تهدیدات و ابعاد امنیتی برای مبادله پیام میان گره‌های حس گر**
- جدول ۱، الزامات امنیتی را فهرست می‌کند و روابط میان ابعاد امنیتی و تهدیدات امنیتی شناسایی شده در Rec.ITU-T X.805 | ISO/IEC 18028-2 را شرح می‌دهد. حرف «Y» در یک خانه براساس فصل مشترک ستون‌ها و سطرهای جدول شکل گرفته است که نشان می‌دهد که یک تهدید امنیتی خاص با بعد امنیتی متناظر در تضاد است.

1 --Non-repudiation. خدماتی برای ارائه شواهدی به فرستنده و گیرنده پیام، تا نتوانند ارسال یا دریافت پیام را انکار کنند.

2 -Availability.

3 -Identifier.

جدول ۱- نگاشت ابعاد امنیتی به تهدیدات امنیتی

توقف خدمات	افشاء اطلاعات	تهدید امنیتی			بعد امنیتی
		سرقت، برداشتن یا از دست رفتن اطلاعات و منابع دیگر	خرابی یا تغییر اطلاعات	تخریب اطلاعات یا منابع دیگر	
	Y	Y	Y	Y	واپایش دسترسی
	Y	Y			اصالت سنجی
Y	Y	Y	Y	Y	سلب انکار
	Y	Y			محرمانگی
	Y	Y			امنیت ارتباط
			Y	Y	یکپارچگی داده‌ها
Y				Y	دسترس پذیری
	Y				حریم

جدول ۲ ابعاد امنیتی را فهرست می‌کند و روابط میان ابعاد امنیت و تهدیدات ویژه گره حس‌گر را برای مبادله پیام میان گره‌ها یا اطلاعات ذخیره شده در گره حس‌گر شرح می‌دهد. حرف «Y» در یک خانه براساس فصل مشترک ستون‌ها و سطرها جدول شکل گرفته است که نشان می‌دهد که یک تهدید امنیتی معین با بعد امنیتی متناظر در تضاد است. برای مثال، تهدید به خطر افتادن گره حس‌گر با بکارگرفتن واپایش دسترسی فیزیکی برای محدود کردن دسترسی به منبع حس‌گر برای فقط هستار یا کاربر مجاز، استفاده از اصالت سنجی گره به گره برای اثبات هویت یکی برای دیگری و بالعکس، استفاده از پردازش داده‌ها و پروتکل ارتباطی برگشت‌پذیر برای تعداد کمی از گره‌های حس‌گر به خطر افتاده، و/یا بکارگیری پروتکل‌های مسیریابی برگشت‌پذیر برای گره‌های به خطر افتاده که به طور بدخواهانه رفتار می‌کنند، می‌تواند مورد توجه قرار گیرد. تهدید حریم داده‌های حس شده، با بکارگیری واپایش دسترسی و رمزبندی داده‌ها که منتج به حفاظت داده‌های حس شده تنها قابل دسترس برای گره مجاز می‌شود، پردازش داده‌های حس شده، که به روشی توزیع شده انتقال می‌یابد به گونه‌ای که هیچ تک گره‌ای داده‌های حس شده را مشاهده نمی‌کند، و/یا انتخاب یک راه مسیریابی ایمن، برای انتقال داده‌های حس شده، می‌تواند مورد توجه قرار گیرد. تهدید حملات بند آوردن خدمت، با بکارگیری اصالت سنجی مناسب داده‌های حس شده و طراحی پروتکل امنیتی دخیل برای برگشت‌پذیری در برابر حملات DoS، و/یا فناوری ارتباطی طیف گسترده برای مقابله با هر نوع حمله اختلالی می‌تواند مورد توجه قرار گیرد.

جدول ۲ - ابعاد امنیتی برای تهدیدات ویژه گره حس گر

تهدیدات ویژه گره حس گر				بعد امنیتی
استفاده بدخواهانه از شبکه تجاری	DoS	رازماني داده‌های حس شده	به خطر افتادن گره حس گر	
Y		Y	Y	واپایش دسترسی
		Y	Y	اصلت‌سنجی
				سلب انکار
Y		Y		محرمانگی
		Y	Y	امنیت ارتباط
				یکپارچگی داده‌ها
	Y			دسترس پذیری
Y		Y		حریم
Y	Y	Y	Y	برگشت پذیری از حملات

۹-۱-۲ تهدیدات و بعد امنیتی برای پخش همگانی پیام‌ها از یک ایستگاه پایه به تمام گره‌های حس گر
جدول ۳ ابعاد امنیتی را به صورت فهرست بیان می‌کند و روابط میان ابعاد امنیت و تهدیدات امنیتی پخش همگانی پیام‌ها، از یک ایستگاه پایه به تمام گره‌های حس گر را شرح می‌دهد. حرف «Y» در یک خانه براساس فصل مشترک ستون‌ها سطرهای جدول شکل گرفته است که نشان می‌دهد که یک تهدید امنیتی مشخص با بعد امنیتی متناظر در تضاد است.

جدول ۳ - نگاهت ابعاد امنیتی به تهدیدات امنیتی در مقابل پخش همگانی پیام‌ها

تهدیدات امنیتی در مقابل پخش همگانی پیام‌ها از یک ایستگاه پایه به تمام گره‌ها					بعد امنیتی
توقیف خدمات، Dos	افشاء اطلاعات	سرقت، برداشتن یا از دست رفتن اطلاعات	خرابی یا تغییر اطلاعات	تخریب اطلاعات	
	Y	Y	Y	Y	واپایش دسترسی
	Y	Y	Y		اصلت‌سنجی
Y		Y		Y	سلب انکار
	Y	Y			محرمانگی
	Y	Y			امنیت ارتباط
			Y	Y	یکپارچگی داده‌ها
Y				Y	دسترس پذیری
	Y				حریم
Y	Y	Y	Y	Y	برگشت پذیری از حملات

۹-۱-۳ تهدیدات و بعد امنیتی برای مبادله پیام مسیریابی

تهدیدات می‌توانند به دو رده طبقه بندی شوند: حملات داخلی و حملات خارجی. حملات داخلی، می‌تواند توسط داخل شبکه صورت گیرد، یعنی مهاجم دارای اطلاعات درمورد برخی اطلاعات حساس ذخیره شده در برخی از گره‌های حس‌گر است، یعنی اطلاعات کلیدی مرتبط با مبادله پیام مسیریابی. حملات داخلی ممکن است مرتبط با حمله سایبل، حمله جریان HELLO، حمله چاهک ستانه (حمله گودال) و جای کرم خوردگی، حمله پیشسویی انتخابی و حمله DoS باشد. جدول ۴ ابعاد امنیتی را فهرست می‌کند و روابط میان ابعاد امنیت و تهدیدات امنیتی مبادله پیام مسیریابی را که توسط حمله داخلی ایجاد می‌شود را شرح می‌دهد. حرف «Y» در یک خانه براساس فصل مشترک ستون‌ها سطرهای جدول شکل گرفته است که نشان می‌دهد که یک تهدید امنیتی مشخص با بعد امنیتی متناظر در تضاد است. حمله کننده داخلی^۱، می‌تواند گره حس‌گر را به خطر اندازد، یعنی یک طرف مجاز، در گره حس‌گر، فعالیت‌های بدخواهانه را انجام می‌دهد و همچنین به حملات فعال و انفعالی اقدام می‌کند. حملات داخلی ممکن است یا از سوی گره‌های حس‌گر به خطر افتاده که کد بدخواهانه را اجرا می‌کنند یا مهاجمانی که محتویات کلید، کد و داده‌ها را از گره‌های حس‌گر برحق^۲ می‌دزدند، صورت گیرد. حمله کننده داخلی می‌تواند با جعل‌سازی یا تزریق اطلاعات مسیریابی جعلی^۳، ایجاد چاهک‌های ستانه (گودال)، پیشسویی انتخابی بسته‌ها، استفاده از حمله سایبل و پخش همگانی جریان‌های HELLO، به SN حمله کند. سازوکارهای امنیت لایه پیوند، که از یک کلید مشترک جهانی، استفاده می‌کنند ممکن است با حضور حملات داخلی یا گره‌های به خطر افتاده فاقد کارایی باشد.

برای مثال، حمله سایبل، با استفاده از رمزبندی و اصالت سنجی پیام مسیریابی که کلید منتج را به عنوان برونداد طرح^۴ توزیع کلید یک طرف سوم مانند Needham-Schroeder بکار می‌گیرد، و با محدودکردن تعداد همسایه‌هایی که یک گره مجاز به داشتن آنها است، می‌تواند مورد توجه قرار گیرد. از بیشتر حملات داخلی با استفاده از یک پودمان سکوی مورد اطمینان (TPM)، در گره حس‌گر، پیشگیری می‌شود.

1 -The insider.

2 -legitimate.

3 -Bogus.

4 -Scheme.

جدول ۴ - نگاشت ابعاد امنیتی به تهدیدات امنیتی یک حمله داخلی

بعد امنیتی	تهدید امنیتی				
	حمله سایبیل	جریان HELLO	چاهک ستانه (گودال)	پیشسویی انتخابی	کرمچاله جعل تایید
واپایش دسترسی					
اصالت سنجی	Y		Y	Y	Y
سلب انکار	Y		Y	Y	Y
محرمانگی					
امنیت ارتباط	Y		Y	Y	Y
یکپارچگی داده‌ها					
دسترس پذیری					
حریم					
برگشت پذیری از حملات					
واپایش دسترسی	Y (توزیع کلیدطرف سوم، TPM)	Y (تأیید دو جهتت بودن پیوند)	Y (چندین گذرگاه، TPM)	Y (چندین گذرگاه، TPM)	Y (همزمان سازی زمان فشرده)

جدول ۵ ابعاد امنیتی را فهرست می‌کند و روابط میان ابعاد امنیت و تهدیدات امنیتی مبادله پیام مسیریابی را که به وسیله حمله خارجی ایجاد می‌شود را، شرح می‌دهد. حرف «Y» در یک خانه براساس فصل مشترک ستون‌ها و سطرها جدول شکل گرفته است که نشان می‌دهد که یک تهدید امنیتی مشخص با بعد امنیتی متناظر در تضاد است. اگرچه حمله کننده خارجی، می‌تواند اقدام به حملات فعال و منفعل کند، اما مهاجم هیچگونه دسترسی خاصی به شبکه حس‌گر ندارد، یعنی وی نمی‌تواند گره حس‌گر را به خطر اندازد. از بیشتر حملات خارجی در مقابل پروتکل مسیریابی شبکه حس‌گر، به وسیله اصالت سنجی و رمزبندی ساده لایه پیوند، با استفاده از یک کلید مشترک جهانی، می‌تواند جلوگیری شود. حمله سایبیل دیگر ارتباطی ندارد چراکه گره‌ها، هویت تک مهاجم را نخواهند پذیرفت. بنابراین، برای مثال، حمله سایبیل، با تأیید هویت گره حس‌گر، یا با استفاده از اصالت‌سنجی پیام یا از طریق محرمانگی می‌تواند مورد توجه قرار گیرد. حملات چاهک ستانه (گودال) یا پیشسویی (هدایت) انتخابی می‌تواند غیر ممکن باشد، چراکه از پیوستن مهاجم به همبندی جلوگیری می‌شود. تایید لایه پیوند، باید با بکارگیری اصالت سنجی پیام حفاظت شود. پیام‌های مسیردهی شده در π مسیر، درمقابل حملات پیشسویی که تا n گره به خطر افتاده را درگیر می‌کند، حفظ می‌شوند.

جدول ۵ - نداشت ابعاد امنیتی برای تهدیدات امنیتی خارجی

بعد امنیتی	تهدید امنیتی				
	حمله سایبیل	جریان HELLO	چاهک (گودال)	پیشسویی (هدایت) انتخابی	کرمچاله
واپایش دسترس					
اصالت سنجی پیام	Y		Y	Y	Y
شناسایی	Y		Y	Y	Y
سلب انکار					
محرمانگی	Y		Y	Y	Y
امنیت ارتباط				Y	
یکپارچگی داده‌ها					
دسترس پذیری					
حریم			Y	Y	Y
برگشت پذیری فناوری			Y (چندین مسیر)	Y (چندین مسیر)	

۹-۱-۴ تهدیدات و بعد امنیتی برای مبادله پیام در شبکه IP

تهدیدات امنیتی و ابعاد امنیتی که در Rec. ITU-T X.805 | ISO/IEC 18028-2 مطرح شده‌اند می‌توانند به صورت مستقیم در مبادله ایمن یک پیام از طریق شبکه IP بکار گرفته شود. بنابراین برای جزییات مرتبط به Rec. ITU-T X.805 | ISO/IEC 18028-2 مراجعه شود.

۱۰ فنون امنیتی برای شبکه‌های حس گر همه جاگاه

۱۰-۱ مدیریت کلید

مدیریت کلید به تولید، توزیع، به اشتراک گذاری، کلیدگذاری مجدد و ابطال کلیدهای رمزنگاشتی^۱ برای خدمت محرمانگی داده‌ها، یکپارچگی داده‌ها، تازگی داده‌ها و اصالت سنجی داده‌ها در SN اشاره می‌کند. امنیت مدیریت کلید، بنیان امنیت خدمات امنیتی دیگر را شکل می‌دهد. در شبکه حس گر، به اشتراک گذاری یا توزیع یک

1 -cryptographic.

جفت کلید^۱، میان گره‌های حس‌گر و یک کلید گروهی^۲، میان مجموعه‌ای از گره‌های حس‌گر بسیار مهم است. که برخی مواقع طرح توافق کلید نامیده می‌شود.

به طور کلی، سه نوع توافق کلید وجود دارد: طرح کارساز مورد اعتماد، طرح خود اعمال^۳ و طرح توزیع. طرح کارساز مورد اعتماد، از کارساز مورد اعتماد مرکزی، برای به اشتراک‌گذاری جفت کلید، بین گره‌های حس‌گر یا کلید گروهی، میان گره‌های حس‌گر استفاده می‌کند. یک مثال نمونه از این طرح، کِربرس^۴ است. به هر جهت، باید یادآور شد که این نوع طرح برای شبکه حس‌گر کفایت نمی‌کند زیرا که هیچ زیرساخت مورد اعتمادی در شبکه حس‌گر وجود ندارد. طرح خود اعمال، از الگوریتم کلید عمومی برای به اشتراک‌گذاری جفت کلید یا کلید گروهی، در شبکه حس‌گر استفاده می‌کند. الگوریتم‌های نمونه از الگوریتم کلید عمومی، شامل الگوریتم توافق کلید دیف_هلمن^۵ و الگوریتم انتقال کلید RSA می‌شود. به هر جهت، باید یادآور شد که این طرح به دلیل محدودیت حافظه و پیچیدگی رایانشی گره حس‌گر، نمی‌تواند در شبکه حس‌گر بکار گرفته شود. طرح پیش توزیع کلید، اطلاعات کلید را، از پیش، میان تمام گره‌های حس‌گر، قبل از استقرار توزیع می‌کند. استقرار بیشتر گره‌های حس‌گر به صورت تصادفی است. به بیان دیگر، دانش اولیه نسبت به مکان دقیق گره حس‌گر، پیش از استقرار، ناشناخته فرض می‌شود. این طرح دارای بالاسری^۶ ارتباطی پایینی است. به علاوه، نسبت به در معرض خطر قرار گرفتن گره، برگشت‌پذیر است و به اعتماد به ایستگاه پایه، متکی نیست. بنابراین این طرح برای شبکه حس‌گر بی سیم بسیار مناسب است.

تعدادی طرح‌های پیش توزیع کلید وجود دارد، که فرض نمی‌شود که دارای دانش استقرار گره حس‌گر باشند. یک طرح ساده، پیش توزیع مبتنی بر کلید اصلی^۷ است. در این طرح، تمام گره‌ها دارای یک تک کلید اصلی مشترک^۸ هستند که برای هر گره حس‌گر، از پیش بکار انداخته شده است^۹. هر دو گره‌ای، از این کلید اصلی جهانی/سرتاسری^{۱۰}، برای بدست آوردن جفت کلید مشترک^{۱۱}، به وسیله مبادله واژه‌های^{۱۲} تصادفی استفاده می‌کنند. این طرح برگشت‌پذیری^{۱۳} مطلوب را برای گره به خطر افتاده فراهم نمی‌سازد، چراکه در صورتی که یک گره به خطر افتد، کل شبکه حس‌گر به خطر می‌افتد. طرح دوم، طرح پیش توزیع جفت کلید نامیده می‌شود. این طرح، برای این طراحی شده است که امکان داشتن N-1 جفت کلید مخفی^{۱۴} را، برای هر گره حس‌گر فراهم کند، که هریک از آن کلیدها، تنها برای این گره حس‌گر، و یکی از N-1 گره‌های حس‌گر دیگر شناخته شده

1- Pair-wise key.

2- Group-wise key.

3- Self-enforcing.

4- Kerberos

5- Diffie-Hellman

6- Overhead.

7- Master-key.

8- A single common master key.

9- Pre-deployed.

10- Global master key.

11- Common pair-wise key.

12- Nonces.

13- Resilience.

14- Secret pair-wise key.

است و N تعداد کل گره‌های حس‌گر در شبکه است. این طرح برگشت‌پذیری کامل را در مقابل گره به خطر افتاده برآورده می‌سازد، چرا که یک گره به خطر افتاده، امنیت هیچ یک از گره‌های دیگر را تحت تأثیر قرار نمی‌دهد. با این حال، از آنجایی که افزودن گره‌های جدید به گره‌های حس‌گر موجود^۱، به دلیل فقدان یک جفت کلید جدید^۲ در گره موجود^۳، غیر ممکن است، فاقد مقیاس‌پذیری^۴ می‌باشد. به علاوه، در صورتی که تعداد گره‌های حس‌گر بسیار زیاد باشد، به علت محدودیت اندازه حافظه، این طرح عملی نیست. طرح سوم طرح پیش توزیع کلید تصادفی است. در این طرح، زیر مجموعه‌ای از کلیدها از یک دسته بزرگ کلید^۵، پیش از استقرار گره حس‌گر ذخیره می‌شوند، دو گره یک کلید مشترک را می‌یابند و از آن به عنوان یک کلید نشست^۶ میان آنها استفاده می‌کنند.

در طرح‌های کلید تصادفی که تاکنون ارائه شده‌اند، اگرچه که، هر گره، می‌تواند تأیید کند که، برخی از همسایگانش دارای کلیدهای مخفی معین هستند، و اینکه، آنها در نتیجه، گره‌های برحق هستند، ولی هیچ گره‌ای نمی‌تواند هویت همسایه‌ای را که آن با ارتباط برقرار می‌کند را، اصالت سنجی کند. موارد زیر قابلیت‌های مدیریت کلید هستند که اصالت سنجی گره به گره را در یک شبکه حس‌گر پشتیبانی می‌کنند:

مدیریت کلید، اصالت سنجی گره به گره را پشتیبانی می‌کند.

- **مدیریت کلید مقیاس‌پذیر :** طرح مدیریت کلید، از یک شبکه حس‌گر بزرگ پشتیبانی می‌کند. به علاوه باید، حتی پس از استقرار گره، در زمانی که، افزایش قابل توجه در گره‌های حس‌گر ایجاد می‌شود، انعطاف‌پذیر باشد.
- **کارایی^۷ اندازه حافظه، قابلیت پردازش و بالاسری ارتباطی لازم برای مدیریت کلید:** طرح مدیریت کلید، دارای پیچیدگی ذخیره سازی کارایی است، یعنی کمینه اندازه حافظه برای ذخیره کلید در گره حس‌گر، پیچیدگی رایانشی کارایی لازم برای برقراری کلید، بالاسری ارتباطی کارا یعنی تعداد پیام‌های مبادله شده طی فرآیند تولید کلید.
- **احتمال بالای برقراری جفت کلید:** در طرح مدیریت کلید، دو گره حس‌گر دارای احتمال بالای برقراری کلید مشترک و محتویات کلید است.
- **برگشت‌پذیری در مقابل گره‌های به خطر افتاده:** طرح مدیریت کلید، دارای قابلیت مقاومت نمودن در برابر گره‌های به خطر افتاده است. یک اعتبارنامه^۸ امنیتی به خطر افتاده، نباید حتی کمینه اطلاعات درمورد امنیت سایر پیوندها، در شبکه حس‌گر را افشا کند، یعنی برگشت‌پذیری بالاتر، به معنای تعداد پایین‌تر پیوندهای به خطر افتاده است. باید توجه شود که برگشت‌پذیری، نباید به موضوع مدیریت کلید

1 -Existing sensor node.

2 -Anew pair-wise key.

3 -Existing node.

4 - Scalability.

5 -large key pool.

6 - session key.

7 -Efficiency.

8 -Credential. داده‌هایی که برای اثبات صحت شناسه‌ای ادعایی یا تأیید شناسه سامانه ارسال یا نمایش داده می‌شود

محدود شود و باید درمورد تمام گره‌های حس‌گر اعمال شود. برگشت‌پذیری در برابر استراق سمع اطلاعات مسیریابی از جمله مثال نمونه است. جزئیات مدیریت کلید در پیوست الف شرح داده شده است.

۱۰-۲ پخش همگانی اصالت سنجی شده

این مورد از اهمیت برخوردار است چراکه پخش همگانی در بسیاری از کاربردها، در شبکه حس‌گر مورد استفاده قرار می‌گیرد. برای مثال، ساختار درخت مسیریابی، پرسمان^۱ شبکه، به روزآمد کردن^۲ نرم‌افزار، همگام سازی زمان^۳ و مدیریت شبکه، همه بر پخش همگانی متکی هستند. به دلیل طبیعت ارتباط بی‌سیم در شبکه‌های حس‌گر، مهاجمان می‌توانند به آسانی داده‌های مخرب^۴ را تزریق کنند یا محتوای پیام‌های برحق^۵ را در حین پیشسویی (هدایت) طی چندین گام^۶ تغییر دهند. کاربردهای شبکه‌های حس‌گر به سازوکارهای اصالت سنجی نیاز دارند تا تضمین کنند که داده‌های یک مبدا معتبر، طی انتقال تغییر نخواهد کرد. اصالت سنجی پخش همگانی یکی از مهمترین نخستینه‌های امنیتی در شبکه‌های حس‌گر است.

هدف یک پیام پخش همگانی، تمامی گره‌های حس‌گر است. طرح اصالت سنجی پیام پخش همگانی، به هر گره مورد هدفی اجازه می‌دهد تا اعتبار پیام‌های پخش همگانی را تایید کند. دو نوع فن می‌تواند برای دستیابی به این هدف در تطابق با نوع الگوریتم رمزنگاشتی^۷ مورد استفاده قرار گیرد. درمورد رمزنگاری^۸ کلید عمومی، یک امضای رقمی (دیجیتال) می‌تواند مورد استفاده قرار گیرد. در صورت استفاده از رمزنگاری متقارن، داده‌های اصالت سنجی قابل تایید (یعنی کد اصالت سنجی پیام)، مبتنی بر چندین رمز مشترک میان ایستگاه پایه (گره ستانه) و گره حس‌گر، لازم است که به داده‌ها الحاق شود که است. در اصالت سنجی پیام پخش همگانی مبتنی بر رمزنگاری متقارن، به دلیل خواص شبکه حس‌گر، روش اصالت سنجی پخش همگانی ترجیح داده می‌شود.

یک طرح نمونه برای فراهم سازی اصالت سنجی پخش همگانی در شبکه‌های حس‌گر وجود دارد که TESLA^۹ (به IETF RFC 4082 و Adrian در کتابنامه مراجعه شود) نامیده می‌شود، که از اصالت سنجی داده‌های هر بسته تاخیر یافته و بازبینی^{۱۰} یکپارچگی پشتیبانی می‌کند. مقصود، افشای تأخیر کلیدهای متقارن است. افشای تأخیر کلید به تأخیر اصالت سنجی منجر می‌شود. TESLA دارای ویژگی‌های پیش رو است: بالاسری رایانشی پایین برای تولید و تأیید اطلاعات اصالت سنجی، بالاسری ارتباطی پایین، میانگیری^{۱۱} محدود لازم برای فرستنده و گیرنده، نیرومندی بالا نسبت به از دست رفتن بسته، مقیاس‌پذیری برای تعداد زیادی از گیرنده‌ها و حفاظت گیرنده‌ها از بند آمدن خدمت. TESLA فرضیات زیر را ایجاد می‌کند:

1 -Query

2 -Update.

3 -Time synchronization.

4 -Maliciouse data.

5 -Legitimate message.

6 -Hop.

7 -Cryptographic.

8 -Cryptography.

9 - Timed efficient stream loss-tolerant authentication.

10 -Check.

11 -Buffering.

- ایستگاه پایه و گره حس گر باید به طور آزاد همگام سازی زمانی شوند.
- TESLA باید در مرحله تنظیم و برقراری نشست^۱، از طریق یک سامانه اصالت سنجی داده‌های منظم، راه اندازی^۲ شود.

مانند نسخه ساده شده TESLA، پروتکل μ TESLA (به Perrige و همکارانش مراجعه شود) بطور اساسی از افشای تأخیر یافته کلید متقارن استفاده می‌کند. فرض می‌شود که ایستگاه پایه و گره‌های حس گر به طور آزاد همگام‌سازی زمانی شده باشند. این عملیات به صورت پیش رو است: ایستگاه پایه MAC را، با کلیدی که در آن زمان مخفی است، درون بسته، رایانش می‌کند. زمانی که یک گره بسته‌ای را دریافت می‌کند، می‌تواند تأیید کند که ایستگاه پایه، هنوز کلید MAC متناظر را، مطابق با ساعت همگام سازی شده و زمان آشکارسازی کلید، افشاء نکرده است. گره بسته را در میانگیر خود ذخیره می‌کند. زمانی که کلیدهای MAC باید آشکار شوند، ایستگاه پایه کلیدهای MAC را برای تمام گره‌های حس گر پخش همگانی می‌کند. گره حس گر می‌تواند اصالت سنجی پیام پخش همگانی را با استفاده از کلیدهای MAC آشکار شده و داده‌های MAC ذخیره شده در میانگیر تأیید کند. هر کلید MAC عضوی از یک زنجیره کلید است که به وسیله یک کارکرد یک سوپه تولید شده است. ایستگاه پایه جهت تولید این زنجیره کلید، آخرین کلید (K_n) از زنجیره کلید را به صورت تصادفی انتخاب می‌کند و تابع چکیده ساز یک سوپه H را به طور مکرر اجرا می‌کند تا تمام کلیدهای دیگر را رایانش کند: $K_i = H(K_{i+1}), i = 1, \dots, n-1$. گره حس گر که K_1 را با ایستگاه پایه به اشتراک می‌گذارد می‌تواند صحت کلید و استفاده از کلیدهای MAC آشکار شده و داده‌های MAC ذخیره شده در میانگیر را، جهت اصالت سنجی بسته ذخیره شده در میانگیر، تأیید کند. موارد زیر تفاوت‌های میان TESLA و μ TESLA هستند:

- TESLA بسته اولیه را با یک امضای رقمی اصالت سنجی می‌کند که برای گره‌های حس گر بسیار پرهزینه است. μ TESLA فقط سازوکار متقارن را استفاده می‌کند.
- آشکارسازی یک کلید در هر بسته مستلزم انرژی بسیاری برای ارسال و دریافت است. μ TESLA کلید را یک بار به ازای آغاز دوره آشکار می‌کند.
- ذخیره یک زنجیره کلید یک سوپه در گره حس گر پرهزینه است. μ TESLA تعداد ارسال کننده‌های اصالت سنجی شده را محدود می‌کند.

موارد زیر قابلیت‌های پخش همگانی اصالت سنجی شده در یک شبکه حس گر هستند:

- برگشت‌پذیری در مقابل گره‌های به خطر افتاده: از آنجایی که استقرار سخت افزار ضد مداخله در گره‌های حس گر در آینده نزدیک غیر محتمل به نظر می‌آید، پروتکل‌های شبکه حس گر ایمن لازم است که در مقابل گره‌های به خطر افتاده، برگشت‌پذیر باشند. به علاوه برگشت‌پذیری در مقابل حملات، اجتناب از نقاط منفرد خرابی را ضروری می‌کند. برای مثال، یک ایستگاه پایه یک نقطه منفرد خرابی

1 -Session setup.

2 -Bootstrap.

است. توصیه می‌شود ایستگاه‌های پایه ضد مداخله با مسیریابی چند مسیره (حتی از طریق نقاط دسترسی) ساخته شوند، از این رو خرابی‌های امنیتی ایستگاه پایه ممکن است کمتر ایجاد خطر کنند.

- **بالاسری رایانشی پایین:** گره‌های حس‌گر دارای منابع رایانشی محدود هستند؛ بنابراین یک پروتکل ایده‌آل می‌تواند دارای بالاسری رایانشی پایین برای هردوی فرستنده و گیرنده باشد.
 - **بالاسری ارتباطی پایین:** انرژی، یک منبع به شدت نایاب در گره‌های حس‌گر است. به طور خاص، ارتباط رادیویی میزان زیادی انرژی مصرف می‌کند. بنابراین تا جای امکان از پروتکل‌هایی با بالاسری ارتباطی بالا پرهیز می‌شود.
 - **نیرومندی در برابر از دست رفتن بسته:** تحویل قابل اطمینان پیام، خاصیت شبکه‌ای است که در آن پیام‌های معتبر از قلم نمی‌افتند.
 - **اصالت سنجی فوری:** تأخیر در اصالت سنجی، بسته به کاربرد، طراحی پروتکل شبکه حس‌گر را، ممکن است تحت اثر قرار دهد. برای پیام‌های بحرانی نسبت به زمان، مانند هشدار آتش نشانی، نیاز به اصالت سنجی فوری پیام از سوی گیرنده است. اگرچه باید توجه شود که تأخیر اصالت سنجی به طور معمول، برای پیام‌های غیر بحرانی نسبت به زمان، قابل قبول است.
 - **پیام‌های ارسال شده در زمان‌های نامنظم^۱:** برخی از کاربردها پیام‌های هم‌گام را در زمان‌های منظم و قابل پیش‌بینی ارسال می‌کنند، در حالی که برخی از کاربردها چنین نیستند. توصیه می‌شود در برخی موقعیت‌ها، از ارسال پیام‌های غیرهم‌گام (برای مثال آشکارساز حضور) برای پرهیز از ایجاد کانال‌های پوشیده^۲ جلوگیری شود. در موارد دیگر، توصیه می‌شود تا از فعالیت ارتباطی هم‌گام (یعنی دوره‌ای) باید اجتناب شود تا از تهدیدات امنیتی ناشی از پیش‌بینی پذیری رفتار ارتباطی شبکه جلوگیری شود.
- μ TPC نسخه بهبود یافته دیگری از TESLA است. جزئیات μ TPC برای پخش همگانی اصالت سنجی شده در شبکه‌های حس‌گر در پیوست ب شرح داده‌های شده‌اند.

۱۰-۳ انبوهش^۳ داده‌های ایمن

انبوهش داده‌ها فنی است که به طور گسترده در شبکه‌های حس‌گر بی سیم مورد استفاده قرار می‌گیرد. با توجه به استقرار شبکه حس‌گر در محیطی نامناسب و دشوار، مسائل امنیتی، محرمانگی داده‌ها و یکپارچگی در انبوهش داده‌ها حیاتی است. اعمال مرتبط بسیاری برای این مسائل امنیتی پیشنهاد شده‌اند. انبوهش ایمن داده‌ها، یک فرآیند درون شبکه‌ای و در گره انبوهش کننده، برای انتقال ایمن مقدار انبوهش شده، به گره ستانه (یعنی یک ایستگاه پایه)، است و به وسیله ترکیب مقادیر حس شده توسط تعدادی از گره‌های حس‌گر، شکل می‌گیرد. در این طرح، هر گره حس‌گر، یک مقدار حس شده رمزبندی شده را، به انبوهش کننده ارسال می‌کند، که سپس نتایج این انبوهش‌های رمزبندی شده، با استفاده از کارکردهای انبوهشی، مانند تابع جمع، تابع میانگین‌گیری، تابع میانی و مقدار بیشینه یا مقدار کمینه محاسبه می‌شود؛ گره ستانه مقدار انبوهش شده را به وسیله رمزگشایی نتیجه انبوهش‌های رمزبندی شده، بدست می‌آورد.

1-Irrigular.

2-Covert.

3-Aggregation.

بنابراین، داشتن قابلیت انبوهش داده‌ها، برای ایستگاه مبنا یا یک گره حس‌گر، نسبت به دریافت داده‌ها، از هر حس‌گر منفرد مفیدتر است. با انبوهش کردن داده‌ها، میزان داده‌هایی که باید از یک حس‌گر به حس‌گر دیگر انتقال یابد، می‌تواند کاهش یابد. انبوهش داده‌های ایمن، می‌تواند برای حس‌گرهای استقرار یافته در یک ساختار سلسله‌مراتبی بکار رود.

دو نوع روش انبوهش ایمن وجود دارد: انبوهش داده‌های رمزگذاری شده *hop* به *hop* و انبوهش داده‌های رمزگذاری شده سرتاسری.

- **انبوهش داده‌های رمزبندی شده گام به گام^۱:** این عملیات مبتنی بر رمزبندی گام به گام میان گره‌های حس‌گر همسایه است. فرض می‌شود که هر جفت از گره‌های حس‌گر همسایه، یک کلید مخفی مشترک را به اشتراک می‌گذارند. مقادیر حس شده، به وسیله تعدادی گره‌های حس‌گر رمزبندی می‌شوند. تمام مقادیر رمزگذاری شده جمع‌آوری شده، به وسیله گره‌های انبوهش‌کننده میانی، رمزگشایی می‌شوند، که سپس مقدار انبوهش شده را کسب و رمزبندی مجدد می‌کنند. این فرآیند تا گره ستانه ادامه می‌یابد. در نهایت، گره حس‌گر کل مقدار انبوهش شده را بدست می‌آورد.
- **انبوهش داده‌های رمزبندی شده سرتاسری:** این عملیات مبتنی بر رمزبندی سرتاسری میان تعدادی از گره‌های حس‌گر و یک گره ستانه است. فرض بر این است که یک رمز مشترک میان تعدادی از گره‌های حس‌گر و یک گره ستانه به اشتراک گذاشته می‌شود. گره‌های حس‌کننده، مقادیر حس شده را رمزبندی می‌کنند و آنها را به گره‌های انبوهش‌کننده میانی پیشسویی (هدایت) می‌کنند که این گره‌های میانی، مقادیر انبوهش شده را، فقط، جمع‌آوری، رمزنگاشتی، و پیشسویی (هدایت) می‌کنند، چراکه گره‌های میانی، دارای کلیدهای رمزگشایی نیستند. در نهایت گره ستانه بسیاری از نتایج انبوهش شده رمزبندی شده را، رمزگشایی می‌کند.

چهارچوب کاری انبوهش داده‌های رمزبندی شده سرتاسری هزینه‌های رایانشی بالاتری را بر گره‌های حس‌گر تحمیل می‌کند اما در مقایسه با چهارچوب انبوهش داده‌های رمزبندی شده گام به گام امنیت قدرتمندتری را کسب می‌کند.

۴-۱۰ تازگی داده‌ها

از آنجایی که تمام شبکه‌های حس‌گر، جریانی از سنج‌های گوناگون نسبت به زمان^۲ را، شکل می‌دهند، فقط، تضمین محرمانگی و اصالت سنجی کفایت نمی‌کند؛ باید تضمین شود که هر پیام تازه است. به طور عامیانه، تازگی داده‌ها، نشان دهنده این است که داده‌ها جدید است و تضمین می‌کند که هیچ مهاجمی، پیام‌های قدیمی را به جریان نینداخته است. دو نوع تازگی شناسایی می‌شود: تازگی ضعیف که ترتیب پیام جزئی را فراهم می‌کند، اما هیچ اطلاعات تأخیری را به همراه ندارد و تازگی قوی، که ترتیب کامل یک جفت درخواست-پاسخ را فراهم

1- Hop to Hop.

2- Time-varying measurement.

می‌کند و تخمین تأخیر را امکان پذیر می‌کند. تازگی ضعیف مورد نیاز سنجه‌های حس‌گر است درحالی که تازگی قدری برای همگام سازی زمانی سودمند است.

۵-۱۰ پودمان^۱ مقاوم در برابر مداخله

بهترین فن شناخته شده جهت حفاظت در برابر به خطر افتادن گره حس‌گر استفاده از پودمان مقاوم در برابر مداخله، در گره حس‌گر است. در صورتی که هر گره حس‌گر با یک پودمان مقاوم در برابر مداخله تجهیز شده باشد، محافظت از ذخیره داده‌های حساس، برای مثال داده‌های کلید، می‌تواند امکان پذیر باشد؛ در غیر این صورت، در شرایطِ گیرافتادنِ گره‌های حس‌گر، چنان‌شِ خرابی آغاز می‌شود. فن ممکن دیگر، برای حفاظت در مقابل یک گره حس‌گر به خطر افتاده، محدود کردن میزان اطلاعات بدست آمده به وسیله مهاجم، پس از خواندن داده‌های گره‌های حس‌گر گیر افتاده است. اگرچه مورد اول نسبت به مورد دوم پرهزینه تر است. بنابراین، مورد اول به کاربردهایی محدود خواهد شد که به اندازه کافی حساس هستند که مستلزم گزینه‌های پرهزینه تر باشند. در صورتی که گره‌های حس‌گر نتوانند مقاوم در برابر مداخله باشند، مورد دوم، باید برای بدست آوردن امنیت احتمالی بکارگرفته شود. پودمان رمزنگاشتی (FIPS PUB 140-2) مثالی از یک پودمان مقاوم در برابر مداخله است که داده‌های حساس را بدون خرابی ذخیره سازی تضمین می‌کند.

۶-۱۰ امنیت میان افزار USN

میزان بسیار زیادی از داده‌های جمع‌آوری شده در شبکه حس‌گر به صورت ایمن، به وسیله میان افزار USN، که داده‌های را از طریق یک کانال ایمن به کاربرد مناسب تحویل می‌دهد، ذخیره، مدیریت و تحلیل می‌شوند. از آنجایی که این میان افزار USN با شبکه‌های حس‌گر یا کاربردها از طریق شبکه IP ارتباط برقرار می‌کند، میان افزار USN، باید تهدیدات امنیتی موجود در شبکه IP را مدنظر قرار دهد. جهت تضمین ارتباطات ایمن در مقابل تهدیدات گوناگون از جمله جعل، به گوش ایستادن^۲، تغییر پیام، DoS و غیره، ابعاد امنیتی از جمله رمزبندی/رمزگشایی، اصالت سنجی، تأیید و واپایش دسترسی مدنظر قرار می‌گیرند و اجرا می‌شوند. به علاوه کارکرد رمزگذاری/رمزگشایی برای داده‌های ذخیره شده در میان افزار USN مورد نیاز است، چراکه میان افزار USN برخی مواقع داده‌های بسیار مهم و ارزشمند را، که در صورت فاش شدن موجب مشکل بزرگی می‌شود ذخیره می‌کند. فن امنیتی جهت تضمین قابل دسترس بودن میان افزار USN، همچنین مدنظر قرار می‌گیرد. پودمان رمزنگاشتی (FIPS PUB 140-2) می‌تواند به عنوان یک پودمان امنیتی برای میان افزار USN مدنظر قرار گیرد.

۷-۱۰ امنیت شبکه IP

فناوری‌های امنیت شبکه IP در Rec. ITU-T X.805 | ISO/IEC 18028-2 می‌تواند جهت ایمنی مبادله پیام از طریق شبکه IP به طور مستقیم بکار رود. بنابراین جزئیات مربوطه می‌توانند حذف شوند.

1- Module.

2 -Sniffing

۱۰-۸ اصلت سنجی گره حس گر

سازوکارها برای اصلت سنجی گره حس گر، جهت تأیید برحق بودن بودن تجهیزات در زمان ورود آنها به شبکه استفاده می شود تا تضمین کنند که تجهیزات مورد استفاده در شبکه برحق و معتبر هستند. جزئیات گره حس گر در پیوست پ شرح داده شده اند.

۱۰-۹ حفاظت حریم در شبکه های حس گر

رمزبندی داده ها و واپایش دسترسی، رویکردهای معمول برای تضمین حفاظت حریم در یک شبکه حس گر است. رویکرد دیگر محدود کردن قابلیت شبکه در جمع آوری داده های حس شده در سطحی از جزئیات است که حریم فردی مورد توجه، را می تواند به خطر اندازد. برای مثال، شبکه حس گر ممکن است درجه هوای انبوهش شده از یک منطقه بزرگ را به جای یک منطقه کوچک گزارش کند. توصیه می شود داده های حس شده، به طور ایمن با بکارگیری ساز و کار واپایش دسترسی به آنها، ذخیره شوند. رویکرد دیگر پردازش پرسمان به روشی توزیع شده است به طوری که یک گره منفرد یا تعداد کمی از گره های حس گر نتوانند به نتایج پرسمان دسترسی یابند که ممکن است به، در خطر افتادن حریم منجر شود.

۱۱ الزامات کارکردی امنیتی ویژه برای USN

این بند سطوح گوناگون الزامات امنیتی را که به صورت منفرد یا جمعی به امنیت USN وابسته است را، مشخص می کند.

۱۱-۱ الزام کارکردی الزامی

- SN مستلزم پشتیبانی از یکپارچگی داده ها و اصلت سنجی داده های حس شده است.
- طرح مدیریت کلید در SN، مستلزم پشتیبانی از طرح پیش توزیع کلید شرح داده شده در بند ۱۰-۱ است.
- مدیریت کلید، مستلزم پشتیبانی از برقراری جفت کلید و برقراری کلید گروهی است.
- SN، مستلزم اصلت سنجی پیام های پخش همگانی از یک ایستگاه پایه، به تمام گره های حس گر و بالعکس است.
- SN، مستلزم پشتیبانی از پروتکل های مسیریابی ایمن با اصلت سنجی پیام، اصلت سنجی شناسانه (ID)^۱، تازگی داده ها و یکپارچگی داده ها است.
- SN، مستلزم پشتیبانی از قابلیت برگشت پذیری در مقابل حملات گوناگون است.
- ایستگاه پایه در SN، مستلزم پشتیبانی از قابلیت تخفیف تأثیرات حملات DoS از هر دو واسط بی سیم و واسط سیمی است.
- USN، مستلزم پشتیبانی از امنیت میان افزار USN همانطور که در بند ۱۰-۶ شرح داده شده، است.
- SN، مستلزم پشتیبانی از اصلت سنجی / شناسایی گره به وسیله گره های دیگر است.

1 -Identifier.

۲-۱۱ ویژگی‌های کارکردی توصیه شده

- SN برای پشتیبانی از یک طرح انبوهش داده‌های رمزبندی شده سرتاسری ایمن، توصیه می‌شود.
- SN برای پشتیبانی از تازگی داده‌ها برای داده‌های حس شده، توصیه می‌شود.
- SN برای پشتیبانی از محرمانگی داده‌های حس شده توصیه می‌شود.
- مدیریت کلید جهت پشتیبانی از برقراری جفت کلید، مبتنی بر اصالت سنجی مبتنی بر ID توصیه می‌شود. مثال این اصالت سنجی در پیوست پ شرح داده شده است.
- USN جهت پشتیبانی از سازوکار تضمین حریم داده‌های حس شده توصیه می‌شود.
- ایستگاه پایه جهت پشتیبانی از مقاومت در برابر مداخله، برای اجتناب از یک نقطه منفرد خرابی توصیه می‌شود.

۳-۱۱ ویژگی‌های کارکردی اختیاری

- یک گره حس‌گر یا یک ایستگاه پایه می‌تواند به صورت اختیاری یک طرحی انبوهش داده‌های گام به گام را فراهم کند.
- گره حس‌گر می‌تواند به صورت اختیاری دارای یک پودمان مقاوم در برابر مداخله برای حفاظت اعتبارنامه‌ها، داده‌های حس شده یا دیگر داده‌های محرمانه باشد.
- گره حس‌گر می‌تواند به صورت اختیاری دارای آشکارسازی مداخله، گواه مداخله یا رویارویی مداخله باشد.
- SN می‌تواند به صورت اختیاری دارای قابلیت تخفیف حملات DoS در مقابل گره حس‌گر باشد.
- SN می‌تواند به صورت اختیاری دارای قابلیت دسترسی به چندین، یا به صورت تصادفی انتخاب شده‌ای از ایستگاه‌های پایه، برای تخفیف تهدیدات امنیتی در مقیاس وسیع، ناشی از نقطه منفرد تأثیرات خرابی باشد.
- SN می‌تواند به صورت اختیاری دارای قابلیت پوشاندن فعالیت غیرهمزمان به پیام‌های همزمان باشد.
- SN می‌تواند به صورت اختیاری دارای قابلیت فراهم نمودن انتخاب چندین مسیر و یا مسیر تصادفی جهت تسهیل برگشت پذیری در مقابل حملات باشد.
- ایستگاه پایه در شبکه حس‌گر می‌تواند به صورت اختیاری دارای آشکارسازی نفوذ باشد.
- SN می‌تواند به صورت اختیاری دارای قابلیت پیکربندی شدن جهت فراهم ساختن حفاظت حریم باشد.

پیوست الف

مدیریت کلید در شبکه‌های حس‌گر

(الزامی)

الف-۱ زمان تهدید

زمانی که شبکه حس‌گر استقرار یافت، گره‌ها، یک جفت کلید را در زمانی کوتاه، برای تضمین امنیت کلید برقرار می‌کنند. بنابراین، مرحله تنظیم و برپایی کلید، چه در معرض یک مهاجم قرار گیرد و یا نگیرد، تعیین کننده است چرا که اطلاعات حساس، مانند شماره تصادفی یا اطلاعات هویت گره، طی این مرحله باز^۱ است. یک مهاجم ممکن است حتی، پیش از تنظیم و برپایی کلید، از پیش، آماده حمله باشد. این مهاجم می‌تواند ارتباط میان گره‌ها را تحلیل کند یا طی تنظیم و برپایی کلید، دسترسی فیزیکی را به گره بدست آورد. این مهاجم، قوی و شدید در نظر گرفته می‌شود. این امر به این معنا است که کاربردی^۲ که نیازمند سطح بالایی از امنیت است، باید طرح^۳ کلید را، با فرض یک مهاجم آماده طراحی^۴ کند.

از سوی دیگر جهت انعطاف پذیر و سودمندتر کردن یک کاربرد، یک طرح مدیریت کلید با سطح پایینی از امنیت می‌تواند در نظر گرفته شود. در این مورد، احتمال حمله، پس از برقراری کلید، وجود دارد. برای مهاجمی که زمان استقرار را نمی‌داند و قادر به دسترسی به مکان استقرار نیست، که تا حمله‌ای را، طی تنظیم و برپایی کلید ترتیب دهد، احتمال حمله، دشوار است. وجود حمله سست^۵، در این مورد بسیار حقیقی است. در کاربردی که، طی تنظیم و برپا شدن کلید، حملات سست، اجرا می‌شود و یا حمله‌ای اجرا نمی‌شود، طراحی طرح کلید، برای بهبود کارایی^۶ و مقیاس پذیری، تنها با امنیت سست، معقول است.

الف-۲ طبقات مدیریت کلید

مبتنی بر دو معیار بالا، یعنی تهدیدات و زمان تهدید، ۴ طبقه مدیریت کلید تعریف می‌شوند.

الف-۲-۱ طبقه ۱

این طبقه فرض می‌کند که یک مهاجم می‌تواند پس از تنظیم و برپایی کلید، استراق سمع کند. هیچ تهدید دیگری مانند گیراندازی گره، در سراسر عمر شبکه وجود ندارد. بنابراین این طبقه ضعیف ترین مهاجم را در نظر می‌گیرد.

الف-۲-۲ طبقه ۲

1 -Open.
2 -Application.
3 -Scheme.
4 -Design.
5- Losse.
6 -Efficiency.

این طبقه فرض می‌کند که یک مهاجم می‌تواند پس از تنظیم و برپایی کلید، گره‌ها را استراق سمع، گیراندازی و برنامه ریزی مجدد کند یا گره‌ها را به خطر اندازد. به بیان دیگر، طی تنظیم و برپایی کلید، هیچ تهدیدی وجود ندارد و استراق سمع کمتر وجود دارد. پس از برپاشدن کلید، یک مهاجم قادر به استراق سمع یا بدست آوردن اطلاعات مخفی از طریق گیراندازی گره است.

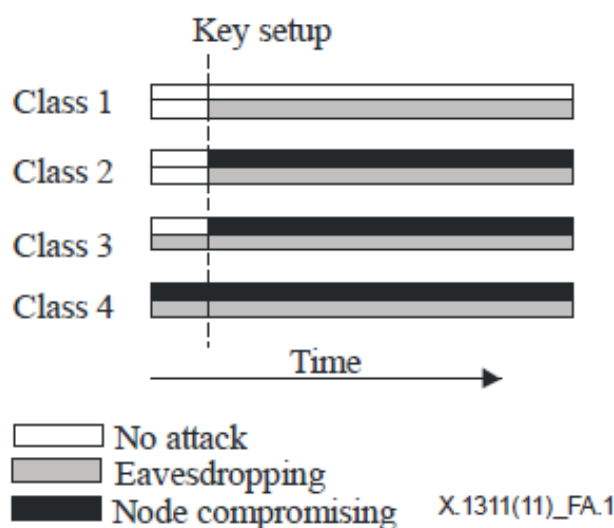
الف-۲-۳ طبقه ۳

این طبقه فرض می‌کند که یک مهاجم می‌تواند ارتباطات را زمانی که گره‌ها استقرار می‌یابند استراق سمع کند؛ پس از برپاسازی کلید، مهاجم می‌تواند برای تمام حملات از جمله گیرانداختن گره آماده باشد.

الف-۲-۴ طبقه ۴

یک مهاجم فعال همیشه در انتظار استقرار گره باقی می‌ماند. این امر به این معنا است که استراق سمع و گیرانداختن گره، در مرحله‌ای که در آن گره‌ها استقرار می‌یابند، روی داده است. با در نظر گرفتن قدرتمندترین مهاجم‌ها، این طبقه یک فرضیه کلی است اما موجب هزینه^۱ بالایی می‌شود.

به صورت کلی، یک مهاجم که قادر به اجرای حملاتی از جمله گیرانداختن گره است، دارای توانایی کافی برای استراق سمع داده‌های انتقال یافته، نیز می‌باشد. براین اساس، نیازی به در نظر گرفتن طبقات دیگر نیست: موردی که در آن به خطر افتادن یک گره همیشه ممکن است اما، استراق سمع تنها پس از تنظیم و برپایی کلید عملی است، و موردی که در آن تمام حملات به جز استراق سمع، تنها پس از برپا شدن کلید ممکن است. به علاوه هرچه سطح طبقه بالاتر باشد، مهاجم قوی‌تر است. در صورتی که یک طرح کلید در طبقه بالاتری ایمن باشد، همچنین در طبقه پایین‌تر نیز، ایمن است. طبقات طرح کلید در شکل الف-۱ نشان داده شده‌اند.



شکل الف ۱ - طبقات مدیریت کلید

1 -Cost.

الف-۳ طرحهای کلید

الف-۳-۱ سازوکارهای مدیریت کلید

الف-۳-۱-۱ پیش توزیع جفت کلید

یک جفت کلید، میان یک جفت گره به صورت مستقیم ذخیره می‌شود و در هر گره، پیش از استقرار گره پیش توزیع می‌شود («طرح جفت کلید»). از آنجایی که هر گره در این طرح، جفت کلیدهای خود را ذخیره می‌کند، دارای برگشت‌پذیری کامل درمقابل به گیرافتادن گره است؛ به بیان دیگر، حتی اگر یک گره به گیر افتد، کلیدهای گره‌های تصرف نشده هیچگاه به خطر نمی‌افتند. اگرچه باید توجه شود که مقیاس پذیری محدود می‌شود چراکه مقیاس شبکه به حافظه گره که کلیدهای بالقوه در آن ذخیره شده اند بستگی دارد.

الف-۳-۱-۲ پیش توزیع مبتنی بر کلید اصلی^۱

یک جفت کلید، از یک عدد تصادفی مبادله شده میان هر گره و یک کلید اصلی تک، که به هر گره پیش توزیع شده است، مشتق می‌شود («طرح کلید اصلی»). این امر به اتصال کلید منجر می‌شود و مستلزم حافظه کم است. با این حال، برگشت‌پذیری بسیار پایین است چرا که زمانی که کلید اصلی در معرض یک مهاجم قرار گیرد، تمام جفت کلیدها می‌توانند به خطر بیفتند. برخلاف طرح کلید اصلی، که پس از تنظیم و برپایی کلید، کلید اصلی را پاک نمی‌کند، یک کلید اصلی، کاملاً پس از برقراری یک جفت کلید پاک می‌شود. اگرچه برگشت‌پذیری با پاک شدن کلید اصلی گره‌های استقرار یافته بهبود می‌یابد، خطر به به خطر افتادن کلید اصلی، طی افزوده شدن گره، با ذخیره شدن کلید اصلی، توسط گره‌های افزوده شده، باقی می‌ماند.

الف-۳-۱-۳ مشارکت ایستگاه مبنا

«SPINS» تحت این سازوکار قرار می‌گیرد (به Perrig و همکارانش در کتابنامه مراجعه شود). در SPINS به هر گره، کلید مشترک با ایستگاه پایه داده می‌شود که به عنوان دروازه شناخته می‌شود. ایستگاه پایه به صورت مستقیم، یک جفت کلید را، که با کلید مشترک هر گره، رمزبندی شده است، را انتقال می‌دهد. به بیان دیگر، ایستگاه پایه در تنظیم و برپاشدن کلید به عنوان میانجی قرار می‌گیرد. این طرح نه تنها از اتصال کامل پشتیبانی می‌کند، بلکه از برگشت‌پذیری کامل نیز پشتیبانی می‌کند. در عین حال به دلیل میزان ترافیک وسیع، که از میانجی‌گری ناشی می‌شود، مقیاس پذیر نیست.

الف-۳-۱-۴ پیش توزیع کلید احتمالاتی

در شبکه‌های بزرگ، روش احتمالاتی نسبت به روش جبری بسیار کارتر است. برای مثال این سازوکار، مبتنی بر مفهومی است که تمام گره‌ها در تمام شبکه‌ها، با احتمال ۰,۹۹۹۷ متصل می‌شوند - تقریباً کاملاً متصل - اگر احتمال اینکه، هر گره بتواند یک جفت کلید را، با گره‌های همسایه خود برقرار کند، ۰,۳۳ باشد. یک حلقه کلید پیش از استقرار، در هر گره ذخیره می‌شود (حلقه کلید k به صورت تصادفی از مخزن^۲ کلید P ، (که به صورت تصادفی از یک فضای عظیم کلید انتخاب شده است). یک کلید مشترک، در هر دو حلقه کلید یک جفت از

1 -Master key.

2 - pool.

گره‌ها، به عنوان جفت کلید آنها مورد استفاده قرار می‌گیرد. این کلید برگشت‌پذیری کافی را ضمانت می‌کند - یک برگشت‌پذیری ناقص - به دلیل اینکه احتمال شکست پیوند ارتباطی k/P است. به علاوه از شبکه‌های با مقیاس بزرگ پشتیبانی می‌کند.

الف-۳-۱-۵ پیش توزیع بدون کلید

این سازوکار این واقعیت شبکه‌های حس‌گر را مد نظر قرار می‌دهد که در صورتی که یک مهاجم، از این که در کجا و چه زمانی گره‌ها استقرار می‌یابند، اطلاعی نداشته باشد، اجرای یک حمله فعال، در یک مرحله ابتدایی دشوار است. بهبود کارایی، به جای انتخاب^۱ کمینه زیان گره، می‌تواند جایگزین مناسبی برای حملات، طی تنظیم و برپایی کلید باشد. در این طرح، تنظیم و برپایی کلید، در یک زمان به نسبت کوتاه و از طریق تنها چند انتقال تکمیل می‌شود. به عنوان مزیت این سازوکار، ایستگاه پایه در تنظیم و برپایی کلید شرکت نمی‌کند؛ بنابراین انرژی به نسبت کمی مصرف می‌شود. برخلاف طرح‌های پیش توزیع بالا، نیازی به بارگذاری کلیدهای بالقوه در یک گره ندارد، در نتیجه موجب هزینه پایین از نظر سازمان شبکه می‌شود. باید توجه شود که اگرچه این شیوه، تنها زمانی که یک مهاجم، ارتباط را طی تنظیم و برپایی کلید مشاهده نمی‌کند، قدرتمند است؛ نمی‌تواند با توجه به برقراری جفت کلید، از طریق داده‌های تبادل شده طی تنظیم و برپایی کلید، گره‌ها را بیافزاید.

الف-۳-۱-۶ پیش توزیع جفت کلید مرتبط احتمالاتی

فرض شود که شبکه حس‌گر دارای بیشینه n گره است. یک راه حل ساده، برای مشکل پیش توزیع کلید، طرح جفت کلیدهایی است، که در آن هر گره حاوی $n-1$ کلید ارتباطی است که هریک جفت کلید، به صورت خصوصی، با یک گره دیگر در شبکه، به اشتراک گذاشته شده است. طرح جفت کلیدهایی احتمالاتی، اصلاح طرح جفت کلید است، مبتنی بر مشاهده اینکه، نیاز به ذخیره شدن تمام $n-1$ کلید، در حلقه کلید گره، برای داشتن یک نمودار تصادفی پیوسته، با احتمال بالا، نمی‌باشد. فرمول Erdos و Renyi به ما اجازه می‌دهد تا کوچکترین احتمال p هر دو گره‌ای را که به گونه‌ای به یکدیگر متصل هستند، که کل نمودار با احتمال بالای c پیوسته است، محاسبه کنیم. که در آن c سطح مطلوب اطمینان (احتمال) است که، شبکه حس‌گر پس از تکمیل پروتکل اتصال، متصل می‌شود (به Spencer مراجعه شود). برای رسیدن به احتمال p در یک شبکه با n گره، هر گره تنها به ذخیره یک مجموعه تصادفی، از np جفت کلیدهای، به جای ذخیره کامل تمام $n-1$ کلید، نیاز دارد. استفاده از جفت کلید، به جای کلید کاملاً تصادفی، که از یک مخزن معین انتخاب می‌شود، می‌تواند، در صورتی که هر گره دربرگیرنده کلید k ، شناسانه (ID) گره دیگر را، که آن گره نیز k را در بر می‌گیرد، ذخیره کند، خصوصیات اصالت سنجی گره به گره را در اختیار قرار می‌دهد. بنابراین، در صورتی که k برای ایجاد یک پیوند ایمن با گره دیگر مورد استفاده قرار گیرد، هر دو گره از هویت یکدیگر مطمئن هستند چراکه هیچ گره دیگری نمی‌تواند k را در برگیرد.

1 -Opting.

پیوست ب

پخش همگانی اصالت سنجی شده در شبکه‌های حس‌گر: μTPC

(اطلاعاتی)

ب-1 ساخت μTPC

مشکل اصلی در مقیاس‌پذیری μTESLA نحوه توزیع و اصالت سنجی پارامترهای اولیه μTESLA (μTP) از جمله الزام‌های زنجیره کلید، زمان آغاز، طول هر فاصله زمانی و غیره است. μTESLA چندسطحی، از نمونه‌های μTESLA سطح بالا، جهت اصالت سنجی پارامترهای موارد سطح پایین استفاده می‌کند؛ که تأخیر اصالت سنجی معرفی شده به وسیله μTESLA ، طی توزیع آن پارامترها، را به ارث می‌برد. در نتیجه چنین تأخیر اصالت سنجی، یک مهاجم می‌تواند حملات DoS را اجرا کند تا توزیع پارامترهای اولیه μTESLA را قطع کند. به علاوه، یک μTESLA چند سطحی نمی‌تواند تعداد زیادی از ارسال کنندگان را ساماندهی کند. پروتکل μTESLA مبتنی بر درخت، از سازوکار درخت مرکب جهت توزیع μTP استفاده می‌کند. با استفاده از گواهی درخت مرکب، گره‌های گیرنده می‌توانند فوراً μTP را اصالت سنجی کنند؛ از این رو در برابر حملات DoS مقاومت می‌کنند. اگرچه باید توجه شود که هزینه μTESLA مبتنی بر درخت، بسیار بالا است. پروتکل اصالت سنجی پخش همگانی مبتنی بر μTPCT جهت توزیع و اصالت سنجی μTP ، μTPC (زنجیره یک طرفه μTP) را می‌سازد. μTPC می‌تواند در برابر حملات DoS مقاومت کند اما هزینه پائینی را دربر دارد.

در شبکه‌های حس‌گر دارای چندین گره پخش همگانی (BNode)¹، BNode ممکن است دارای خصوصیات متفاوت با در نظر گرفتن وظایفی که می‌باید انجام دهد، باشد. چرخه حیات، فراوانی پخش همگانی و الزام بی‌درنگ BNode، ویژگی خاص پارامترها (FP)² هستند. BS بر مبنای FP، BNode، μTP را خواهد ساخت. برای مثال برای BNode بی با چرخه حیات کوتاه، فراوانی بالای پخش همگانی و الزام بی‌درنگ، BS یک μTP خاص را خواهد ساخت که حاوی تأخیر کوتاه آشکارسازی کلید و نمونه‌های μTESLA کمتر با فاصله‌های زمانی کوتاه است. FP در صورت لزوم می‌تواند بسط یابد.

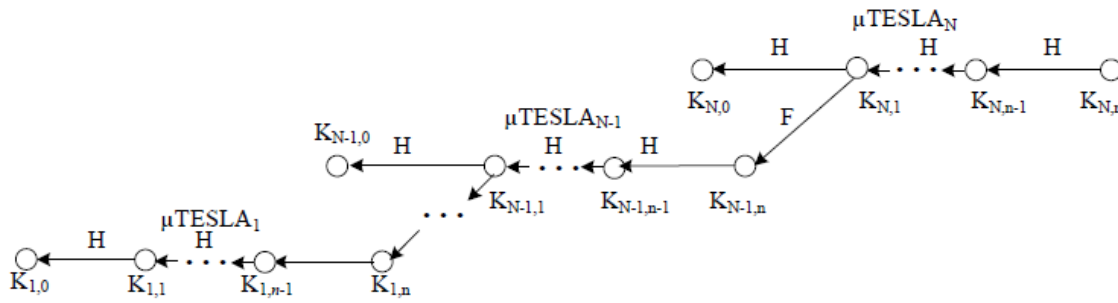
μTPC متشکل از μTP و زنجیره یک طرفه است. پس از تعیین شدن FP، BS ابتدا طول عمر BNode را به N فاصله زمانی با طول T_N تقسیم می‌کند، به گونه ای که مدت T_N (برای مثال سی دقیقه)، برای اجرای یک نمونه μTESLA در BNode و گره‌های حس‌گر به صورت کارآمد، مناسب است. بر مبنای فراوانی پخش همگانی و الزام بی‌درنگ BNode، BS، T_N را به n فاصله زمانی با طول T_n تقسیم خواهد کرد. بر مبنای N و n ، BS از تابع شبه تصادفی F جهت تولید N زنجیره کلید μTESLA که به یکدیگر پیوند خورده اند استفاده می‌کند. ابتدا BS آخرین کلید $K_{N,n}$ از N مین زنجیره کلید μTESLA را، به صورت تصادفی تولید می‌کند. پس از آن با استفاده از تابع چکیده ساز H (برای مثال SHA-1)، BS، مابقی کلیدهای N مین زنجیره کلید μTESLA را مطابق با

1 -Broadcast node.

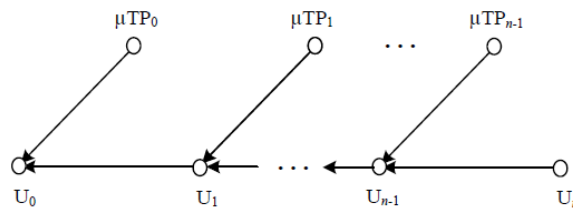
2 -Feature parameter.

$K_{N,i} = H(K_{N,i+1})$ تولید می‌کند. برای $(i-1)$ امین زنجیره کلید μTESLA ، BS آخرین کلید را با اجرای یک تابع شبه تصادفی بر روی اولین کلید (کلید نزدیک به التزام) امین زنجیره کلید μTESLA تولید می‌کند و سپس مابقی کلیدهای $(i-1)$ امین زنجیره کلید μTESLA را با اجرای H بر روی آخرین کلید آن تولید می‌کند. با این روش، BS تمام زنجیره‌های کلید μTESLA را تا آخرین آنها تولید می‌کند. شکل ب-۱ ساخت زنجیره‌های کلید μTESLA را نشان می‌دهد.

پس از اینکه تمام زنجیره‌های کلید μTESLA تولید شدند، برای j BNode، BS کلیدهای متفاوت را به فاصله‌های زمانی T_n متفاوت تخصیص خواهد داد. براین است که N نمونه μTESLA وجود خواهد داشت. از آنجایی که پارامتر اولیه امین نمونه μTESLA ، $\mu\text{TP}_i = \{T_s \| K_{i,0} \| T_i \| T_{int} \| d\}$ است که در آن T_s مشخص کننده زمان جاری، $K_{i,0}$ مشخص کننده التزام، T_i به زمان آغاز اشاره دارد، T_{int} مشخص کننده فاصله همگام سازی و d به تأخیر افشای کلید اشاره دارد. پس از اینکه تمام μTP ها تعیین شدند، BS یک مقدار U_N را به طور تصادفی تولید می‌کند و سپس هر مقدار U را تا U_0 براساس $U_{i-1} = H(U_i \| \mu\text{TP}_{i-1})$ رایانش می‌کند که در آن $\|$ مشخص کننده الحاق پیام است. در نهایت، BS، μTPC را می‌سازد که حاوی N μTP است. شکل ب-۲ مثالی از ساخت یک μTPC را نشان می‌دهد.



شکل ب-۱- ساخت زنجیره‌های کلید μTESLA از μTPC که در آن هر $K_{i,n}$ از $K_{i+1,1}$ و با استفاده از تابع شبه تصادفی F منتج می‌شود

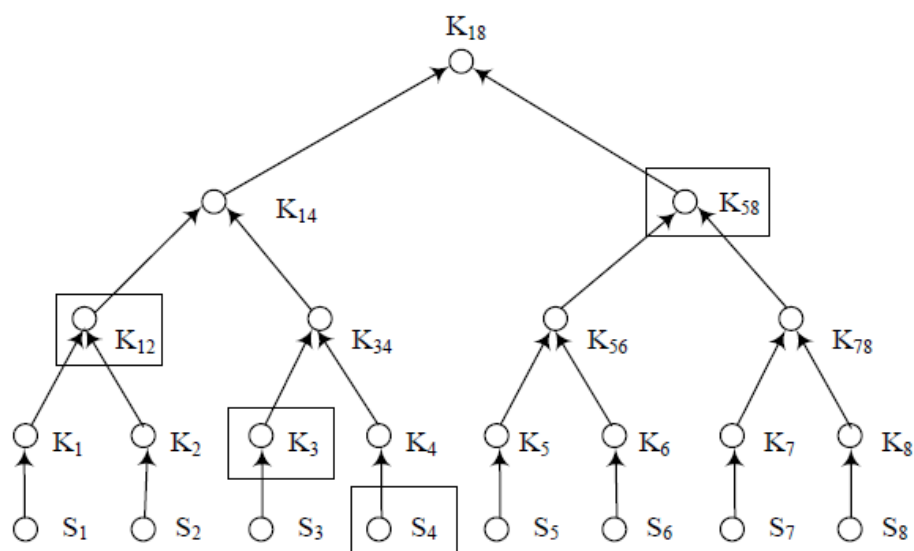


شکل ب-۲- ساخت μTPC که در آن $U_i = H(U_{i+1} \| \mu\text{TP}_i)$

ب-۲- ساختار μTPC

با فرض اینکه m BNode در شبکه‌های حس‌گر وجود دارد. جهت آسودگی فرض می‌شود که $m=2^k$ که در آن k یک عدد صحیح است. پیش از استقرار، BS، m μTPC را پیش رایانش می‌کند که به هریک از آنها یک ID منحصر به فرد با مقدار عدد صحیح بین ۱ و m تخصیص داده می‌شود. به منظور ارایه، زمین مقدار U از μTPC

μTPC به صورت U_{ij} ، i امین μTPC به صورت μTP_{ij} و i امین پارامتر اولیه (شامل $U_{i,0}$ و ID_i) μTPC به صورت S_i مشخص می‌شود. BS سپس $K_i = H(S_i)$ را برای تمام $i \in \{1, \dots, m\}$ رایانش می‌کند. پس از آن یک درخت مرکل را با استفاده از $\{K_1, \dots, K_m\}$ به عنوان گره‌های برگ می‌سازد. هر گره غیر برگ با بکارگیری H برای الحاق گره‌های مولود آن رایانش می‌شود. چنین درخت مرکلی μTPC نامیده می‌شود (درخت چکیده‌ساز مرکل μTPC). شکل ۳ ب μTPCT را با هشت μTPC نشان می‌دهد که در آن $K_{12} = H(K_1 \| K_2)$ ، $K_{14} = H(K_{12} \| K_{34})$ ، $K_{18} = H(K_{14} \| K_{58})$ و غیره است.



شکل ۳ - درخت μTPCT با ۸ گره برگ؛ گره‌ها در هر جعبه تشکیل دهنده اعتبارنامه S_4 است که $PCert_4$ نامیده می‌شود

BS همچنین یک اعتبارنامه پارامتر را برای هر نمونه μTPC می‌سازد. اعتبارنامه برای i امین نمونه μTPC متشکل از S_i و همچنین مقادیر متناظر با هم نیا‌های گره‌ها در مسیر از i امین گره برگ به ریشه μTPCT است. برای مثال، اعتبارنامه پارامتر برای چهارمین نمونه μTPC در شکل ۳، $PCert_4 = \{S_4, K_3, K_{12}, K_{58}\}$ است. برای هر $BNode$ ، که از یک نمونه معین μTPC استفاده خواهد کرد، BS ، μTPC و اعتبارنامه پارامتر متناظر با آن را توزیع خواهد کرد. BS همچنین ریشه μTPCP را برای تمام گیرنده‌های بالقوه پیام‌های پخش همگانی پیش توزیع خواهد کرد.

پیش از ساخت μTPCT در صورتی که قسمت‌های مشابه در تمام μTP ها از μTPC ها وجود داشته باشد، قسمت‌های مشابه μTP با پارامتر اولیه μTPC به عنوان گره‌های برگ در کنار یکدیگر قرار داده‌ای می‌شوند تا μTPCT را بسازند. برای مثال، در صورتی که تأخیر آشکارسازی d و فاصله‌های همگام سازی T_{int} در تمام μTP های i مشابه باشند، d و T_{int} با پارامترهای اولیه μTPC_i به عنوان گره‌های برگ، در کنار یکدیگر قرار می‌گیرند، تا μTPCT را بسازند. مطابق با آن برخی قسمت‌های μTP با اعتبارنامه μTPC ، تنها یکبار، با یکدیگر توزیع خواهند شد. در فرآیند توزیع μTP ، $BNode$ تنها به توزیع قسمت متفاوت نیاز دارد. با این روش، در هزینه ماهیت ارتباط، صرفه جویی خواهد شد.

ب-۳ پخش همگانی اصالت سنجی شده

نمایش پروتکل پخش همگانی اصالت سنجی شده می تواند به پنج قسمت زیر تقسیم شود:

ب-۳-۱ آغاز پروتکل

پیش از استقرار شبکه های حس گر، BS، $\mu Tinst$ (مشخص کننده نمونه $\mu TESLA$)، μTPC و $\mu TPCT$ را مطابق با کمیت و FP تمام BNode ها می سازد. پس از آن، ریشه R از $\mu TPCT$ را، برای RNode (گره دریافت کننده) توزیع می کند.

ب-۳-۲ درخواست μTPC

پیش از پیوستن به شبکه های حس گر، BNode درخواست BREQ ارسال می کند که شامل FP تا BS برای BNode می شود. پس از آن، BS به جستجوی μTPC سازگار (برای مثال μTPC_4 نشان داده شده در شکل ب-۳) مطابق با FP BNode می پردازد. همراه با گواهینامه $PCert_4$ و K_{gen} (مشخص کننده کلید تولید شده زنجیره کلید $\mu TESLA$) تمام $\mu Tinsts$ ، BS، μTPC را به BNode باز می گرداند.

ب-۳-۳ BNode اصالت سنجی

پیش از پخش همگانی، BNode گواهینامه $PCert_4$ خود را برای تمام RNode ها منتشر می کند تا برحق بودن خود را اثبات کند. RNode از R و معادله $H(H(H(H(S_4) \| K_3) \| K_{12}) \| K_{58}) = K_{18}$ برای تأیید $PCert_4$ استفاده می کند. در صورت موفقیت، RNode، پارامتر اولیه $U_{4,0}$ ، ID_4 در μTPC و همچنین قسمت های μTP در μTPC را ذخیره می کند.

ب-۳-۴ توزیع μTP

پس از اصالت سنجی موفق، BNode، اولین زنجیره کلید $\mu TESLA$ را مطابق با K_{gen} اولین $\mu Tinst$ با استفاده از تابع چکیده ساز H ایجاد می کند. پس از آن، BNode، $U_{4,1}$ و $\mu TP_{4,0}$ را برای RNode ها پخش همگانی می کند. مطابق با $U_{4,0} = H(U_{4,1} \| \mu TP_{4,0})$ برحق بودن $\mu TP_{4,0}$ را تأیید می کند. در صورت موفقیت، RNode، $U_{4,1}$ و $\mu TP_{4,0}$ را حفظ می کند؛ در غیر این صورت، رد می شود. سپس BNode، $U_{4,2}$ را به صورت پی درپی پخش همگانی می کند. همزمان، BNode از دومین K_{gen} را برای تولید دومین زنجیره کلید $\mu TESLA$ استفاده می کند. پس از دریافت $U_{4,2}$ ، RNode آن را ذخیره و $U_{4,0}$ را حذف می کند. جهت اطمینان از قابل اطمینان بودن توزیع، BNode به طور مکرر U را پخش همگانی خواهد کرد.

ب-۳-۵ اصالت سنجی پیام پخش همگانی

زمانی که RNode بر مبنای $\mu Tinst_{4,0}$ ، $\mu TP_{4,0}$ را بدست آورد، RNode می تواند تمام پیام های پخش همگانی را از BNode اصالت سنجی کند. بنابراین یک کانال اصالت سنجی پخش همگانی میان RNode و BNode ایجاد می شود. زمانی که $2 * T_{int}$ پیش از انتهای چرخه حیات $\mu Tinst_{4,0}$ در پردازش اصالت سنجی پخش همگانی باقی می ماند، پروتکل متعاقباً اقدام به اجرای مرحله ۴ خواهد کرد. به بیان دیگر BNode، $\mu TP_{4,1}$ را پخش همگانی می کند. RNode استفاده $\mu TP_{4,1}$ از $U_{4,1} = H(U_{4,2} \| \mu TP_{4,1})$ را تأیید می کند. در صورت موفقیت، RNode، $\mu TP_{4,1}$ را ذخیره می کند، در غیر این صورت، رد می شود. باید توجه شود که این پروتکل از اینکه

RNode می‌تواند اصالت سنجی پیام پخش همگانی BNode را در چرخه حیات $\mu Tinst_{4,1}$ ادامه دهد اطمینان حاصل می‌کند. رویه بعدی پروتکل مرحله ۵ را تا انتهای حیات BNode تکرار خواهد کرد.

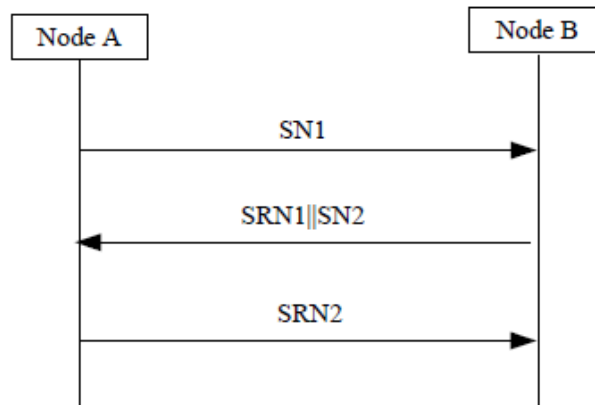
پیوست پ

سازوکار اصالت سنجی در شبکه‌های حس‌گر

(الزامی)

پ-۱- سازوکار مبتنی بر XOR

رویه اصالت سنجی مبتنی بر کلید از پیش به اشتراک گذاشته شده در شکل پ ۱ نشان داده شده است. این رویه شامل یک دست تکانی^۱ ۳ طرفه میان گره‌های A و B می‌شود: یک درخواست اصالت سنجی، یک پاسخ اصالت سنجی و یک تصدیق پاسخ اصالت سنجی.



شکل پ-۱- اصالت سنجی مبتنی بر کلید از پیش به اشتراک گذاشته شده

در متن زیر، PSK و SK به ترتیب مشخص کننده یک کلید از پیش به اشتراک گذاشته شده و یک کلید نشست میان گره‌های A و B هستند.

پ-۱-۱ درخواست اصالت سنجی

A، SN1 را به B می‌فرستد تا رویه اصالت سنجی را آغاز کند. قالب پیام درخواست اصالت سنجی (از A به B) در شکل پ ۲ نشان داده شده است.



شکل پ ۲- قالب پیام درخواست اصالت سنجی

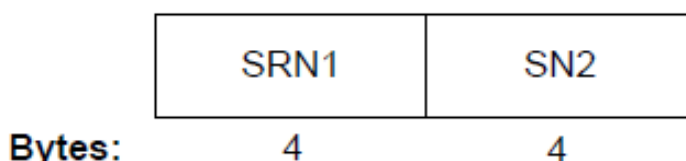
1 -Handshake.

که در آن $SN1=N1\oplus PSK$ و $N1$ یک شماره تصادفی ۴ بایتی است که به وسیله A تولید می‌شود. زمانی که B پیام درخواستِ اصالتِ سنجی را از A دریافت می‌کند، B رویه‌های زیر را اجرا می‌کند:

- (۱) $N1$ را با $SN1\oplus PSK$ محاسبه می‌کند؛
- (۲) $RN1$ را با معکوس کردن $N1$ محاسبه می‌کند؛ و
- (۳) پیام پاسخِ اصالتِ سنجی را می‌سازد و آن را به A ارسال می‌کند.

پ-۱-۲ پاسخِ اصالتِ سنجی

قالب پیام پاسخِ اصالتِ سنجی (از B به A) در شکل پ۳ نشان داده شده است.



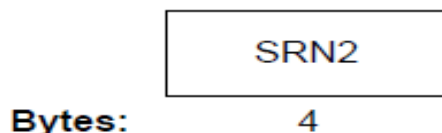
شکل پ۳- قالب پیام پاسخِ اصالتِ سنجی

که در آن $SRN1=RN1\oplus PSK$ ، $SRN2=N2\oplus PSK$ و $N2$ یک شماره تصادفی ۴ بایتی است که به وسیله $MFAN-N(B?)$ تولید می‌شود. هنگام دریافت پیام پاسخِ اصالتِ سنجی از B ، A رویه‌های زیر را اجرا می‌کند:

- (۱) $RN1$ را با $SRN1\oplus PSK$ محاسبه می‌کند، سپس $N1$ را با معکوس کردن $RN1$ محاسبه می‌کند؛
- (۲) در صورتی که مقدار $N1$ محاسبه شده با A ، با مورد تولید شده در ساختِ پیامِ درخواستِ اصالتِ سنجی تطبیق نداشته باشد، پیام را رد می‌کند و فرآیندِ اصالتِ سنجی را متوقف می‌کند؛
- (۳) $N2$ را با $SN2\oplus PSK$ محاسبه می‌کند، سپس $RN2$ را با معکوس کردن $N2$ محاسبه می‌کند؛
- (۴) $SK=N1\oplus N2\oplus PSK$ را مانند کلید نشستِ استفاده شده با B محاسبه می‌کند؛ و
- (۵) پیام تصدیقِ پاسخِ اصالتِ سنجی را می‌سازد و آن را به B ارسال می‌کند.

پ-۱-۳ تصدیقِ پاسخِ اصالتِ سنجی

قالب پیام تصدیقِ پاسخِ اصالتِ سنجی (از A به B) در شکل پ۴ نشان داده شده است.



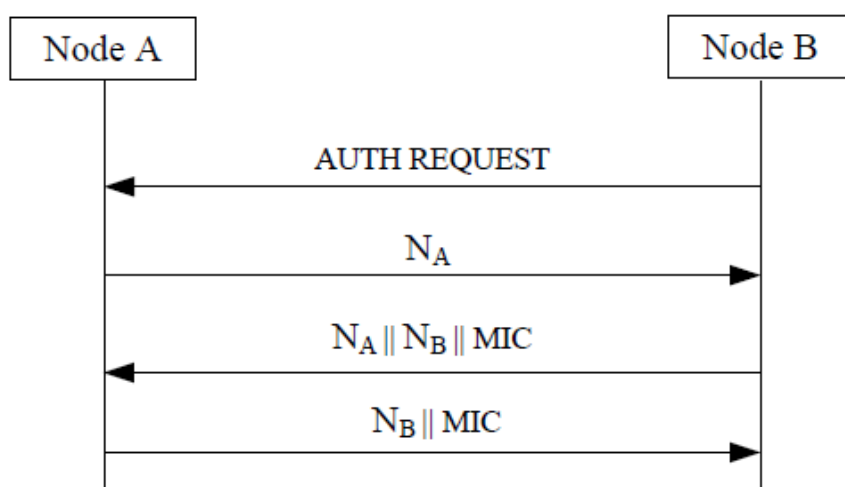
شکل پ۴- قالب پیام تصدیقِ پاسخِ اصالتِ سنجی

که در آن $SRN2=RN2\oplus PSK$ است. هنگام دریافت پیام تصدیقِ پاسخِ اصالتِ سنجی از A ، B رویه‌های زیر را اجرا می‌کند:

- (۱) RN2 را با $SRN2 \oplus PSK$ محاسبه می‌کند، سپس N2 را با معکوس کردن RN2 محاسبه می‌کند؛
- (۲) در صورتی که مقدار N2 محاسبه شده با B، با مورد تولید شده در ساخت پیام درخواست اصالت سنجی تطبیق نداشته باشد، پیام را رد می‌کند و فرآیند اصالت سنجی را متوقف می‌کند؛
- (۳) $SK = N1 \oplus N2 \oplus PSK$ را مانند کلید نشست استفاده شده با B محاسبه می‌کند.

پ-۲ سازوکار مبتنی بر درهم سازی

رویه اصالت سنجی مبتنی بر درهم سازی در شکل پ۵ نشان داده شده است. این رویه دست تکانی ۴ طرفه میان گره‌ها A و B را شامل می‌شود: آغاز اصالت سنجی، درخواست اصالت سنجی، پاسخ اصالت سنجی و تصدیق پاسخ اصالت سنجی.

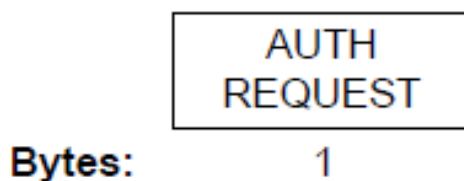


شکل پ۵ - اصالت سنجی مبتنی بر چکیده‌سازی

در متن زیر، PSK مشخص کننده کلید از پیش به اشتراک گذاشته شده میان گره‌های A و B پیش از اصالت سنجی است. SK مشخص کننده یک کلید نشست میان گره‌های A و B منتج شده از PSK است. « ID_{AB} » الحاق شناسانه گره A و شناسانه گره B است.

پ-۲-۱ آغاز اصالت سنجی

B یک پیام آغاز اصالت سنجی را به A ارسال می‌کند تا رویه اصالت سنجی آغاز شود. قالب پیام آغاز اصالت سنجی (از گره B به گره A) در شکل پ۶ نشان داده شده است.

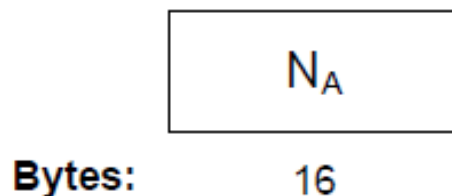


شکل پ۶ - قالب پیام آغاز اصالت سنجی

- هنگام دریافت پیام آغاز اصالت سنجی از گره A ، رویه‌های زیر را اجرا می‌کند:
- (۱) یک شماره تصادفی N_A را تولید می‌کند؛ و
 - (۲) پیام درخواست اصالت سنجی را می‌سازد و آن را به گره B ارسال می‌کند.

پ-۲-۲ درخواست اصالت سنجی

قالب پیام درخواست اصالت سنجی (از گره A به گره B) در شکل پ-۷ نشان داده شده است.



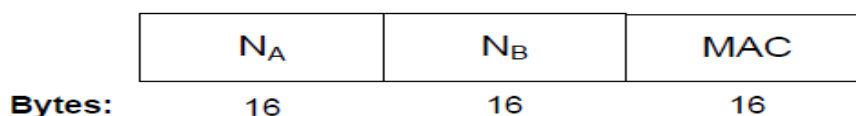
شکل پ-۷- قالب پیام درخواست اصالت سنجی

که در آن N_A یک شماره تصادفی ۱۶ بایتی است که به وسیله گره A تولید می‌شود. هنگام دریافت پیام درخواست اصالت سنجی از A ، رویه‌های زیر را اجرا می‌کند:

- (۱) شماره تصادفی N_B را تولید می‌کند؛
- (۲) کلید نشست را محاسبه می‌کند؛
- (۳) MAC (کد اصالت سنجی پیام) را محاسبه می‌کند؛ و
- (۴) پیام پاسخ اصالت سنجی را می‌سازد و آن را به A ارسال می‌کند.

پ-۲-۳ پاسخ اصالت سنجی

قالب پیام پاسخ اصالت سنجی (از گره B به گره A) در شکل پ-۸ نشان داده شده است.



شکل پ-۸- قالب پیام پاسخ اصالت سنجی

که در آن N_A یک شماره تصادفی در پیام درخواست اصالت سنجی است، N_B یک شماره تصادفی ۱۶ بایتی است که به وسیله گره B ، $MAC=HMAC-SHA256(SK, N_B || N_A)$ ، «بسط کلید جفت برای کلیدهای تک پخشی و افزوده و مقصود فعلی» $SK=KD-HMAC-SHA256(PSK, ID_{AB} || N_B || N_A ||$ تولید می‌شود. هنگام دریافت پیام درخواست اصالت سنجی، گره A رویه‌های زیر را اجرا می‌کند:

- (۱) ابتدا N_A را بازبینی می‌کند. در صورتی که مقدار N_A ، با مورد تولید شده در ساخت پیام ۲ مطابقت نداشته باشد، گره A پیام ۳ را رد می‌کند و فرآیند اصالت سنجی را متوقف می‌کند؛ در غیراین صورت مرحله ۲ را اجرا می‌کند؛

(۲) «بسط کلید جفت برای کلیدهای تک پخشی و افزوده و مقصود فعلی» $SK=KD-HMAC-SHA256(PSK, ID_{AB} || N_B || N_A || MAC)$ را محاسبه می‌کند؛

(۳) پیام ۳ MAC را محاسبه می‌کند؛

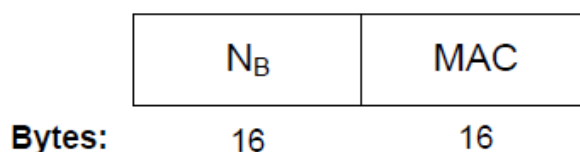
(۴) در صورتی که MAC محاسبه شده با MAC در پیام ۳ مطابقت نکند، پیام ۳ را رد می‌کند؛ در غیر این صورت به مرحله ۵ می‌رود.

(۵) پیام تصدیق اصالت سنجی را می‌سازد و به گره B ارسال می‌کند؛

(۶) SK را برقرار می‌کند.

پ-۲-۴ تصدیق پاسخ اصالت سنجی

قالب پیام پاسخ اصالت سنجی (از گره A به گره B) در شکل پ۹ نشان داده شده است.



شکل پ۹- قالب پیام تصدیق پاسخ اصالت سنجی

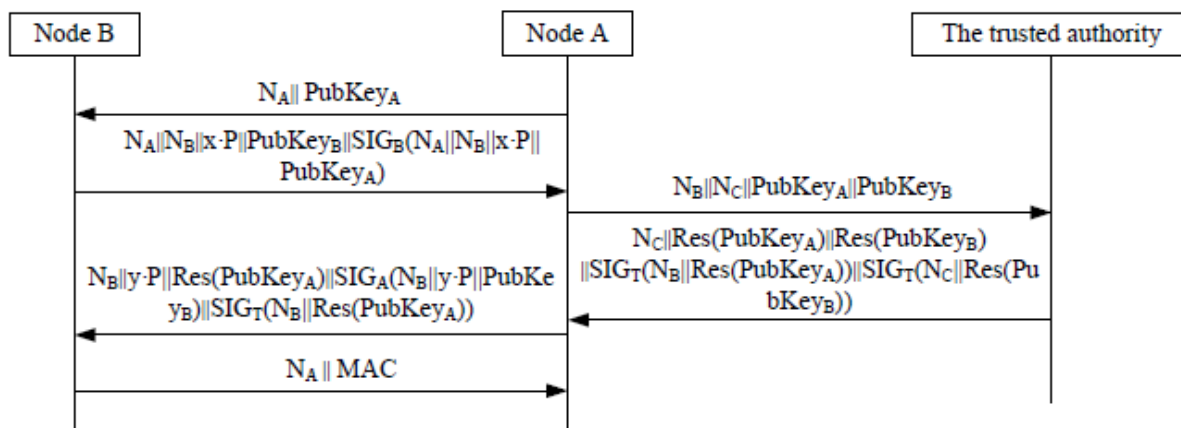
که در آن N_B یک شماره تصادفی در پیام درخواست اصالت سنجی و $MAC=HMAC-SHA256(SK, N_B)$ است. هنگام دریافت پیام تصدیق پاسخ اصالت سنجی از گره A ، B رویه‌های زیر را اجرا می‌کند:

(۱) ابتدا N_B را بازبینی می‌کند. در صورتی که مقدار N_B با مورد تولید شده در ساخت پیام ۳ مطابقت نداشته باشد، پیام ۴ را رد می‌کند و فرآیند اصالت سنجی را متوقف می‌کند؛ در غیر این صورت مرحله ۲ را اجرا می‌کند؛

(۲) پیام ۴ MAC را تأیید می‌کند. در صورتی که MAC محاسبه شده با MAC در پیام ۴ مطابقت نکند، گره A پیام ۴ را رد می‌کند؛ در غیر این صورت SK را برقرار می‌کند.

پ-۳ اصالت سنجی مبتنی بر کلید عمومی

رویه اصالت سنجی مبتنی بر کلید عمومی در شکل پ۱۰ نشان داده شده است. یک مرجع مورد اعتماد برای تأیید هویت گره‌های A و B وجود دارد. گره‌های A و B ، یک متغیر جهانی P مورد استفاده جهت محاسبه کلید عمومی ناپایدار را، به اشتراک می‌گذارند.

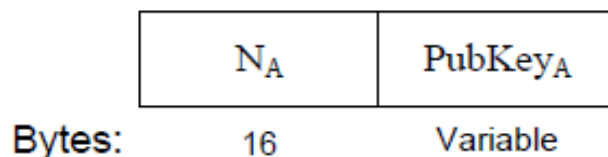


شکل پ ۱۰- اصلت سنجی مبتنی بر کلید عمومی

در متن زیر به ترتیب $PubKey_x$ مشخص کننده کلید عمومی X است، SIG_x به امضای X اشاره دارد و $Res(PubKey_x)$ مشخص کننده نتیجه تأیید $PubKey_x$ است.

پ-۳-۱ درخواست اصلت سنجی

A یک درخواست اصلت سنجی را به گره B ارسال می‌کند تا رویه اصلت سنجی را آغاز کند. قالب پیام درخواست اصلت سنجی (از گره A به گره B) در شکل پ ۱۱ نشان داده شده است.



شکل پ ۱۱- قالب پیام درخواست اصلت سنجی

که در آن N_A یک شماره تصادفی ۱۶ بایتی است که به وسیله گره A تولید می‌شود و $PubKey_A$ کلید عمومی گره A است. هنگام دریافت پیام درخواست اصلت سنجی از A ، رویه‌های زیر را اجرا می‌کند:

- (۱) شماره تصادفی N_B را تولید می‌کند.
- (۲) کلید مخفی ناپایدار X را تولید می‌کند و کلید عمومی ناپایدار $X.P$ را محاسبه می‌کند؛
- (۳) از کلید مخفی جهت محاسبه امضا استفاده می‌کند؛ و
- (۴) پیام پاسخ اصلت سنجی را می‌سازد و آن را به گره A ارسال می‌کند.

پ-۳-۲ پاسخ اصلت سنجی

قالب پیام پاسخ اصلت سنجی (از گره B به گره A) در شکل پ ۱۲ نشان داده شده است.

N_A	N_B	$x \cdot P$	$PubKey_B$	$SIG_B(N_A N_B x \cdot P PubKey_A)$
Bytes: 16	16	variable	Variable	variable

شکل پ ۱۲ - قالب پیام پاسخ اصالت سنجی

که در آن N_A یک شماره تصادفی در پیام درخواست اصالت سنجی است، N_B یک شماره تصادفی ۱۶ بایتی است که به وسیله گره B تولید می‌شود، $x \cdot P$ کلید عمومی ناپایدار برای ECDH است؛ x کلید مخفی ناپایدار است، $PubKey_B$ کلید عمومی گره B است و $SIG_B(N_A || N_B || x \cdot P || PubKey_A)$ امضای استفاده کننده از کلید مخفی گره B است. هنگام دریافت پیام درخواست اصالت سنجی از گره B، گره A رویه‌های زیر را اجرا می‌کند:

(۱) یک شماره تصادفی N_C را تولید می‌کند؛ و

(۲) پیام درخواست تأیید کلید را می‌سازد و آن را به مرجع مورد اعتماد ارسال می‌کند.

پ-۳-۳ درخواست تأیید کلید

قالب پیام درخواست تأیید کلید (از گره A به مرجع مورد اعتماد) در شکل پ ۱۳ نشان داده شده است.

N_B	N_C	$PubKey_A$	$PubKey_B$
Bytes: 16	16	Variable	Variable

شکل پ ۱۳ - قالب پیام درخواست تأیید کلید

که در آن N_B یک شماره تصادفی مانند آن در پیام درخواست اصالت سنجی است، N_C یک شماره تصادفی ۱۶ بایتی است که به وسیله گره A تولید می‌شود، $PubKey_A$ کلید عمومی گره A و $PubKey_B$ کلید عمومی گره B است. هنگام دریافت پیام درخواست تأیید کلید از گره A، مرجع مورد اعتماد رویه‌های زیر را اجرا می‌کند:

(۱) اعتبار $PubKey_B$ و $PubKey_A$ را بازرسی می‌کند؛

(۲) امضای نتیجه بازرسی را محاسبه می‌کند؛ و

(۳) پیام درخواست تأیید کلید را می‌سازد و آن را به گره A ارسال می‌کند.

پ-۳-۴ پاسخ تأیید کلید

قالب پیام پاسخ تأیید کلید (از مرجع مورد اعتماد به گره A) در شکل پ ۱۴ نشان داده شده است.

	N_C	$\text{Res(PubKey}_A)$	$\text{Res(PubKey}_B)$	$\text{SIG}_T(N_B \parallel \text{Res(PubKey}_A))$	$\text{SIG}_T(N_C \parallel \text{Res(PubKey}_B))$
Bytes:	16	1	1	Variable	Variable

شکل پ ۱۴ - قالب پیام پاسخ تأیید کلید

که در آن N_C یک شماره تصادفی مانند آن در پیام درخواست تأیید کلید است، به ترتیب $\text{Res(PubKey}_A)$ نتیجه تأیید PubKey_A ، $\text{Res(PubKey}_B)$ نتیجه تأیید PubKey_B ، $\text{SIG}_T(N_B \parallel \text{Res(PubKey}_A))$ امضا با استفاده از کلید مخفی مرجع مورد اعتماد، $\text{SIG}_T(N_C \parallel \text{Res(PubKey}_B))$ امضا با استفاده از کلید مخفی مرجع مورد اعتماد است. هنگام دریافت پیام پاسخ تأیید کلید از مرجع مورد اعتماد، گره A رویه‌های زیر را اجرا می‌کند:

- (۱) ابتدا N_C را بازبینی می‌کند سپس با بازبینی اینکه آیا مقدار N_C ، با مقدار ارسال شده در پیام درخواست تأیید کلید مطابقت می‌کند، $\text{SIG}_T(N_C \parallel \text{Res(PubKey}_B))$ را بررسی می‌کند؛
- (۲) کلید مخفی ناپایدار را تولید می‌کند و کلید عمومی ناپایدار $y.P$ را محاسبه می‌کند؛
- (۳) «بسط کلید پایه برای کلید و افزونه مقصود فعلی»
 $N_A \parallel N_B$ و محوطولی $((x.y.p))$ $BK_{AB} = KD - HMAC - SHA256$ را محاسبه می‌کند؛
- (۴) پیام نتیجه اصالت سنجی را می‌سازد و آن را به گره B ارسال می‌کند.

پ-۳-۵ نتیجه اصالت سنجی

قالب پیام نتیجه اصالت سنجی (از گره A به گره B) در شکل پ ۱۵ نشان داده شده است.

	N_B	$y.P$	$\text{Res(PubKey}_A)$	$\text{SIG}_A(N_B \parallel y.P \parallel \text{Res(PubKey}_B))$	$\text{SIG}_T(N_B \parallel \text{Res(PubKey}_A))$
Bytes:	16	Variable	1	Variable	Variable

شکل پ ۱۵ - قالب پیام نتیجه اصالت سنجی

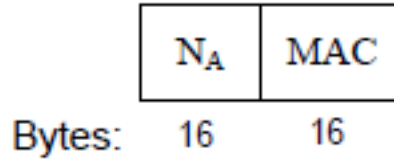
که در آن N_B یک شماره تصادفی مانند پیام پاسخ اصالت سنجی است، $y.P$ کلید عمومی ناپایدار برای ECDH؛ y کلید مخفی ناپایدار، $\text{Res(PubKey}_A)$ نتیجه تأیید PubKey_A ، $\text{SIG}_A(N_B \parallel y.P \parallel \text{Res(PubKey}_B))$ امضا با استفاده از کلید مخفی گره A و $\text{SIG}_T(N_C \parallel \text{Res(PubKey}_A))$ امضا با استفاده از کلید محرمانه مرجع مورد اعتماد است. هنگام دریافت پیام نتیجه اصالت سنجی از گره A، گره B رویه‌های زیر را اجرا می‌کند:

- (۱) N_B را بازبینی می‌کند؛
- (۲) $\text{SIG}_T(N_C \parallel \text{Res(PubKey}_A))$ و $\text{SIG}_A(N_B \parallel y.P \parallel \text{Res(PubKey}_B))$ را به ترتیب با بازبینی N_A و N_B تأیید می‌کند؛
- (۳) «بسط کلید جفت برای کلید و افزوده مقصود فعلی»
 $N_A \parallel N_B$ و محوطولی $((x.y.p))$ $BK_{AB} = KD - HMAC - SHA256$ را محاسبه می‌کند؛
- (۴) $MAC = KD - HMAC - SHA256(BK_{AB}, N_A)$ محاسبه می‌کند؛
- (۵) پیام تصدیق اصالت سنجی را می‌سازد و آن را به گره A ارسال می‌کند؛

۶) BK_{AB} را برقرار می‌کند.

پ-۳-۶ تصدیق اصالت سنجی

قالب پیام تصدیق اصالت سنجی (از گره B به گره A) در شکل پ ۱۶ نشان داده شده است.



شکل پ ۱۶ - قالب پیام تصدیق اصالت سنجی

که در آن N_A یک شماره تصادفی مانند آن در پیام درخواست اصالت سنجی، $MAC=HMAC-SHA256(BK_{AB}, N_A)$ است. هنگام دریافت پیام تصدیق اصالت سنجی از گره B، گره A رویه‌های زیر را اجرا می‌کند:

۱) ابتدا N_A را بازبینی می‌کند؛

۲) MAC را از B بر مبنای BK_{AB} تأیید می‌کند؛

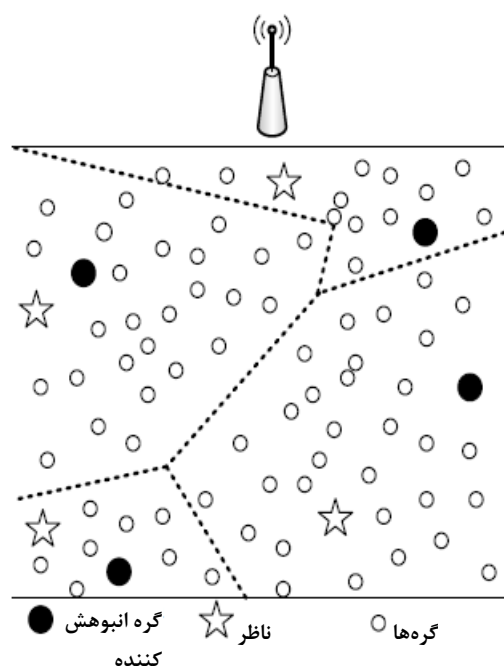
۳) BK_{AB} را برقرار می‌کند.

پیوست ت

انبوهش داده‌های ایمن در شبکه‌های حس‌گر

(الزامی)

شکل ت ۱ یک ساختار نمونه از شبکه‌های حس‌گر را ترسیم نموده است. شبکه می‌تواند به صورت خودکار مطابق با برخی خواص ویژه مانند انرژی، فاصله^۱ و غیره به تعدادی خوشه^۲ تقسیم شود. در یک چرخه ارتباطی^۳، شبکه، باید یک گره انبوهش‌کننده^۴ و یک ناظر^۵ را داخل هر خوشه انتخاب کند. ناظر انتخاب شده، یک نقش نظارتی را در یک دوره معین ایفا می‌کند. یک ناظر پیام‌ها را از گره‌های پیرامونش جمع‌آوری می‌کند و این پیام‌ها را به گره انبوهش‌کننده ارسال می‌کند و سپس گره‌های انبوهش‌کننده، این پیام‌ها را که به وسیله ناظر ایجاد شده‌اند را، به ایستگاه پایه^۶ انتقال می‌دهد. هنگام دریافت این پیام‌ها، یک ایستگاه پایه، این پیام‌ها را با پیام‌های انبوهش شده به وسیله گره‌های انبوهش‌کننده، مقایسه می‌کند و صحیح یا غلط بودن پیام‌های انبوهش شده را قضاوت می‌کند؛ از این رو انبوهش داده‌ها را در شبکه‌های حس‌گر ایمن می‌کند.



شکل ت ۱ - نمایش انبوهش داده‌های ایمن

شرح تفصیلی آن به صورت پیش‌رو است:

- 1 -Distance.
- 2 -Cluster.
- 3-Communication cycle.
- 4 -Aggregation.
- 5 -Supevision.
- 6 -Base station.

ت-۱ انتخاب گره انبوهش کننده و ناظر

ابتدا گره حس گر یک شماره تصادفی را تولید می کند و سپس مقدار انرژی خودش و این شماره تصادفی را پخش همگانی می کند، هر گره آن پیام پخش همگانی شده را از گره های همسایه دریافت می کند و آن مقادیر انرژی ها و شماره های تصادفی را مقایسه می کند؛ گره با بیشترین مقدار انرژی و کوچکترین شماره تصادفی به عنوان گره انبوهش کننده انتخاب می شود و گره با دومین مقدار بیشترین انرژی و دومین کوچکترین شماره تصادفی به عنوان ناظر انتخاب می شود. زمانی که برخی گره ها دارای مقدار انرژی و شماره تصادفی مشابه باشند، این گره ها یک شماره تصادفی را تولید و به طور مکرر، این فرآیند و تراکنش تا حصول به منظور ادامه خواهد یافت^۱. این فرآیند تا زمانی که شبکه یک گره انبوهش کننده و یک ناظر را در هر خوشه، با این اصل، که گره ای که شماره تصادفی آن کمینه است یک گره انبوهش کننده می شود و گره ای که شماره تصادفی آن دومین کمینه است گره ناظر می شود، به پایان نخواهد رسید.

چرخه گره ناظر T_S می تواند براساس فرمول $T_S \geq \sum_{n=1}^n T_m$ ، $T_C = T_S$ تعریف شود که در آن T_m چرخه ارتباطی گره های معمولی در خوشه است، T_C چرخه گره انبوهش کننده ای است که برابر با چرخه گره ناظر است، T_C ، بیشتر یا مساوی بیشینه درمیان چرخه گره انبوهش کننده است، چرخه ناظر و چرخه گره معمولی در یک خوشه است. هدف تضمین این است که فرآیند نظارت و فرآیند انبوهش در این دوره تکمیل شود، یعنی گره انبوهش کننده و ناظر در یک خوشه برای تضمین امنیت ارتباطات شبکه، روزآمد شوند.

ت-۲ پیاده سازی کارکردهای ناظر

کارکردهای ناظر و انبوهش داده های باید همزمان انجام گیرند. ناظران، پیام های نظارتی را از گره های معمولی که به گره انبوهش کننده نیز فرستاده شده اند، جمع آوری می کنند و از الگوریتم انبوهش مشابه برای پیام های نظارتی استفاده می کنند، سپس پیام های نظارتی را صادر می کنند.

ت-۳ بارگذاری پیام نظارتی

پیام های نظارتی به وسیله یک ناظر به گره انبوهش ارسال می شود و سپس به ایستگاه پایه هدایت (پیشسویی) می شود. امنیت پیام های نظارتی به وسیله جفت کلید میان ناظر و ایستگاه پایه تضمین می شود.

ت-۴ تعیین اعتماد گره های انبوهش کننده

پس از دریافت پیام نظارتی از گره های انبوهش کننده، ایستگاه پایه آنها را بیت به بیت مقایسه می کند. زمانی که نتیجه تطبیقی متناقض باشند، گره انبوهش کننده می تواند به عنوان گره غیرمعمول تعیین شود. همچنین، در صورتی که ایستگاه پایه، اطلاعات نظارتی را طی زمان آستانه که توسط سامانه پیکربندی شده است، دریافت نکند، گره انبوهش کننده، می تواند به عنوان گره نامعتمد تعیین شود.

ت-۵ ارسال پیام ابطال

1 -Negotiate.

زمانی که ایستگاه پایه تعیین کند که گره انبوهش نامعتمد است، پیام ابطال را برای کل شبکه پخش همگانی می‌کند تا گره انبوهش کننده را لغو کند. این خوشه باید گره انبوهش و گره ناظر را مجدد انتخاب کند.

کتابنامه

- IEEE 802.15.3:2003, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs).
- IEEE 802.15.4:2006, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).
- IETF RFC 4082 (2005), Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction.
- ISO/IEC 15408-1:2009, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
- Akyldiz, I.F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002), A Survey on Sensor Networks, IEEE Communications Magazine, pp.102-114, August.
- Chan, H., and Perrig, A. (2003), Security and Privacy in Sensor Networks. Computer, pp. 103-105, October.
- Karlof, C., and Wagner, D. (2003), Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, Elsevier, pp. 293-315.
- Perrig, A., Szewczyk, R., Tygar, J.D., Wen V., and Culler, D. E., (2002), Spins: Security Protocols for Sensor Networks, Kluwer Academic Publishers.
- Perrig, A., Canettiz, R., Tygary, J. D., and Song D. (2000), Efficient authentication and signing of multicast streams over lossy channels, in proceeding of IEEE symposium on Security and Privacy.
- Spencer, J. (2000), The Strange Logic of Random Graphs; Algorithms and Combinatorics Vol. 22, Springer-Verlag, ISBN 3-540-41654-4.
- Technical Document of ISO/IEC JTC 1, Study Group on Sensor Networks (SGSN).