امنیت شبکه های حسگر بی سیم:

شبکه های حسگر بی سیم در اصل برای جمع آوری اطلاعات از محیطی غیر قابل اعتماد به وجود آمده اند. تقریبا همه پروتکل های امنیتی برای WSN معتقدند که دشمن یا نفوذگر می تواند از طریق ارتباط مستقیم، کنترل کامل یک نود حسگر را در دست گیرد. امنیت اهمیت به سزایی در پذیرش و استفاده از شبکه های حسگر، در کاربردهای متعدد دارد.

حملات در شبکه های حسگر بی سیم:

یک شبکه حسگر بی سیم در مقایس بزرگ از هزاران نود از حسگرها تشکیل شده است و ممکن است در یک محیط پهناور پراکنده شده باشد. نودهای حسگر نوعاً کوچک هستند با توانایی محدود درمحاسبات و ارتباطات که توسط باتری تغذیه می شوند. این نودهای حسگر کوچک مستعد انواع مختلفی از حملات هستند. حملات در شبکه های حسگر بی سیم می توانند طبقه بندی شوند به حملات بر روی لایه های فیزیکی، ارتباط(کنترل دسترسی به رسانه یا واسط)، شبکه، انتقال و لایهٔ کاربرد. حملات می توانند همچنین بر پایهٔ توانایی های مهاجمان طبقه بندی شوند، هم چون سطح حسگر و سطح لپ تاپ.

انواع حملات:

حملات می توانند به دو دستهٔ داخلی و خارجی تقسیم بندی شوند. یک مهاجم خارجی به بیشتراجزای رمزنگاری در شبکهٔ حسگر دسترسی ندارد، در حالی که یک مهاجم داخلی ممکن است بخشی ازاجزای کلید را در اختیار داشته باشد و مورد اعتماد برخی از نودهای دیگر باشد. شناسایی و مقابله با حملات داخلی بسیار مشکل است.

حملات انکار سرویس:

حملات انکار سرویس (DOS =DENIAL OF SERVICE)به حملاتی می گویند که هدف اصلی آن ممانعت از دسترسی قربانیان به منابع کامپیوتری، شبکه ای و یا اطلاعات است. در این گونه حملات معمولا از دسترسی قربانیان به اطلاعاتی که برای مقابله با این گونه حملات مفید است، نیز جلوگیری می شود. دراین نوع حملات، مهاجمان با ایجاد ترافیک های بی مورد و بی استفاده، حجم زیادی از منابع سرویس دهنده و پهنای باند شبکه را مصرف یا به نوعی درگیر رسیدگی به این تقاضا های بی مورد می کنند و این تقاضا ها تا جایی که دستگاه سرویس دهنده را از کار بیندازد، ادامه پیدا می کند.

انواع حملات در شبکه های حسگر بی سیم:

براي هر نمونه از حمله، 3 آيتم به ترتيب زير ارائه شده است: نام حمله، لايۀ شبكه متناظر و تكنيک هاي تدافعي ممكن.حملات شبکه های حسگر بی سیم و تکنیک های تدافعی ممکن را می توان به صورت زیر خلاصه نمود:

1Jamming(لایۀ فیزیکی) : طیف گسترده ، چرخه کاری پایین تر.

2مداخله کردن (لایۀ فیزیکی): آزمون مداخله، طرح مدیریت مؤثر کلید.

3 تصادم(لایه اتصال): کد تصحیح خطا.

4 خستگی(لایۀ اتصال): محدودیت نرخ.

5 دستکاری اطلاعات مسیر یابی(لایه شبکه): اعتبار سنجی و رمز گذاري.

6حمله ارسال انتخابی(لایه شبکه): فراوانی، کاوش.

7حمله Sybil (لایه شبکه): اعتبار سنجی.

8 حمله حفره(حفره سیاه)(لایه شبکه): اعتبار سنجی، نظارت، افزونگی.

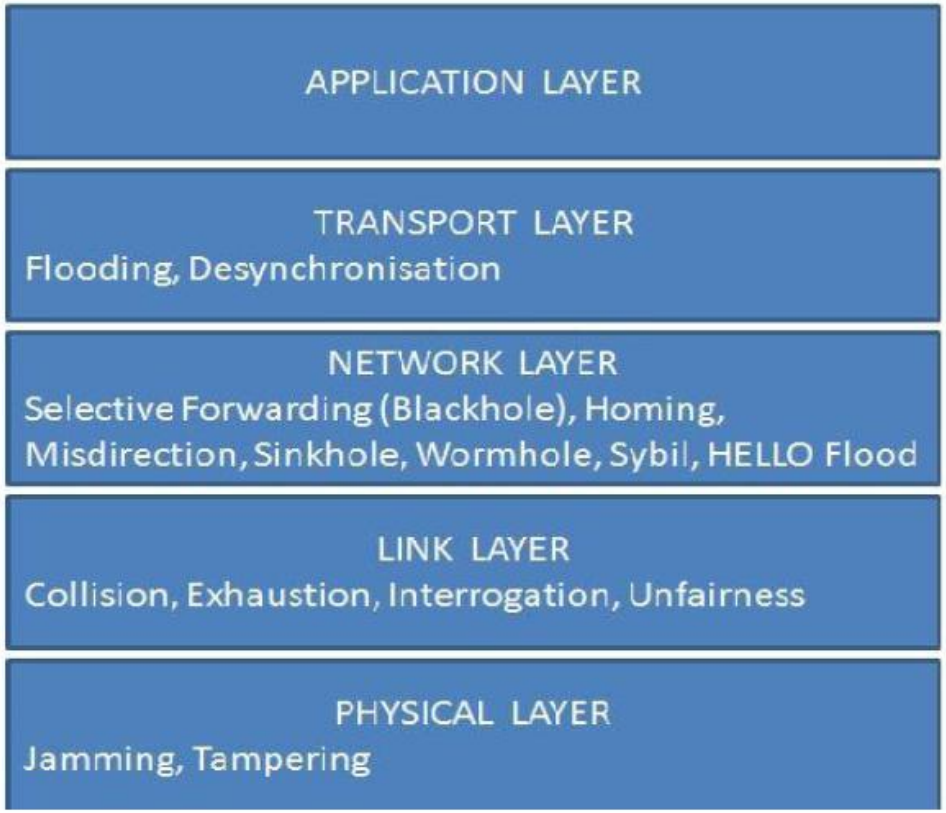
9 حمله حفره کرم(لایه شبکه): نظارت، انتخاب انعطاف پذیر مسیر.

10 حمله سلام سیل آسا(لایه شبکه): اعتبار سنجی 2 راهه، دست دادن 3 راهه.

11 سیل(لایه انتقال): محدودیت تعداد ارتباطات، جدول کلاینت ها.

12 حمله کپی(لایه کاربرد): کلید دوگانۀ واحد و ...

رده بندی حملات:



رده بندی حملات

تحلیل حمله:

هر مهاجمی که به هر روشی حمله به یک شبکه را طراحی کرده است، یک نیت سوء دارد که طبق یک برنامهٔ از پیش مشخص شده پیش می رود. با استفاده از تحلیل حمله قادر خواهیم بود مکانیزمی را ایجاد کنیم که بتوانیم حملات را پیش بینی، جلوگیري، محافظت و پوشش دهیم. یک مهاجم می تواند در 4 بعد تقسیم بندی شود: " انگیزه، اراده، دانش و منابع". چهار بعد فوق به طور موثری می توانند مورد استفاده قرار گیرند برای پاسخ به سوالات اساسی پیرامون یک حملهٔ مورد انتظار در یک شبکه. اگر سوالات فوق قبل از توسعهٔ شبکه پاسخ داده شوند آنگاه شبکه می تواند گسترش یابد درحالی که تهدیدات احتمالی دیده می شوند.

سوالاتی برای تحلیل حمله:

سوالات بالقوه اي كه نياز است پاسخ داده شوند برای تحلیل یک مهاجم و قصد و نیت آن عبارتند از:

- مهاجم کیست؟
- یک مهاجم قادر به چه کارهایی است؟
- هدف چیست؟
- چگونه حمله صورت می گیرد؟
- نتیجه یا پیامد حمله چه چیزهایی هستند؟

اهداف امنیت:

نهایی امنیت تامین محرمانگی، جامعیت، اعتبار سنجی و در دسترس بودن همهٔ پیام ها با وجود مهاجمان کاردان و ماهر است. هر دریافت کننده می بایست همه پیام ها را با در نظر داشتن موارد فوق دریافت کند و بتواند تمامیت هر پیام را همچون هویتی که از سمت فرستنده داشته است را تشخیص دهد. مهاجمان نباید بتوانند به محتویات پیام ها پی ببرند. در شبکه های کامپیوتری رایج هدف اصلی امنیت، تحویل مطمئن پیام است.

مکانیزم End-To-End:

اعتبار پیام، تمامیت و محرمانگی معمولاً توسط یک مکانیزم End-To– End حاصل می شوند. این به دلیل است که الگوی ترافیکی حاکم ارتباط END-TO-END است، در جایی که نه نیاز است و نه مطلوب که محتویات پیام ها برای مسیریاب های واسط قابل دسترس باشد. در صورت وجود حملات داخلی، اقدامات امنیتی می بایست تضمین کنند که شبکه حسگر می تواند عملیات اصلی را تأمین کند با حداقل تراکم.

مدیریت کلید:

برای دستیابی به امنیت در شبکه های حسگر بی سیم مهم است که بتوان عملیات روز نگاری متفاوتی را انجام داد، شامل رمزگذاری، اعتبار سنجی و موارد مشابه. کلیدهای این عملیات رمزنگاری باید توسط نودهای ارتباطی ست شوند قبل از اینکه آنها بتوانند اطلاعات امنیتی را تغییر دهند. مدل های مدیریت کلید مکانیزم هایی هستند که نمونه های متنوعی از کلیدها را منتشر و در شبکه توزیع می کنند، همچون کلیدهای منفرد، کلیدهای دوگانه، کلیدهای گروهی.مدیریت کلید یک عملیات اصلی و ضروری است در رمزنگاری که عملیات امنیتی دگر بر مبنای آن شکل می گیرند.4 نوع مدل مدیریت کلید وجود دارد: سرور مورد اعتماد، وجود اجرا کننده، کلید پیش توزیع، کلید رمزنگاری عمومی.

همزمان سازی امن:

به خاطر ذات همکاری در نودهای حسگر، همزمان سازی برای بسیاری از عملیات شبکه های حسگر مهم می باشد، مانند کارهای حسی مرتبط، زمانبندی حسگرها(بیدار و خواب)، پیگیری اجسام متحرك، دسترسی تقسیم زمانی (TDMA) ، کنترل دسترسی به رسانه، تراکم داده ها و پروتکل تشخیص هویت منابع Multicast . پروتکل زمانی شبکه (NTP) برای همزمان سازی در اینترنت مورد استفاده قرار می گیرند. یک شبکه حسگر یک سیستم توزیع شده محدود است و NTP نمی تواند به طور مستقیم توسط شبکه های حسگر مورد استفاده قرار می گیرد. چندین الگوریتم همزمان سازی برای شبکه های حسگر پیشنهاد شده است.

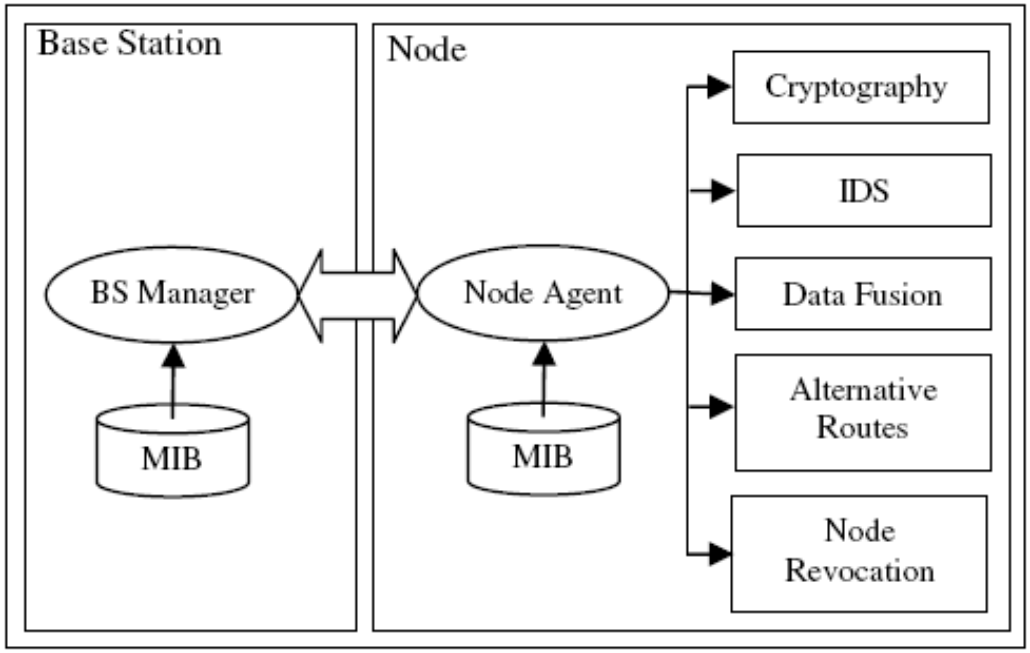
حملات ممکن در همزمان سازی حسگرها:

4حملهٔ ممکن در همزمان سازی حسگرها شناسایی شده اند:

- حملهٔ فریبکارانه: فرض کنید نود A براي دو تا از همسایگانش یک منبع را راهنمایی می کند و B و C . یک مهاجم وE می تواند وانمود کند که B است و اطلاعات همزمان سازي نادرست را با C تبادل کند، که فرآیند همزمان سازي را بین B و C مختل می کند.
- حملهٔ دوباره: استفاده از همان سناریویی که در حملهٔ قبلی گفته شد، مهاجم E می تواند به بسته هاي زمانی قدیمی B پاسخ دهد، که C را به صورت نادرست همزمان می کند.
- حملهٔ دستکاري پیام: در این حمله، یک مهاجم ممکن است کم کند، تغییر دهد یا حتی جعل کند پیام هاي زمانی تبادل شده را که فرآیند همزمانی را مختل می کند.
- حملهٔ تأخیر: مهاجم مدبرانه برخی از پیام ها را دچار تأخیر می کند که در فرآیند همزمانی به عنوان خطا مطرح می گردد.

مدل مدیریت شبکه:

در این مدل شبکه مرجع، یک شبکه مسطح همگن است، بدین معنا که همه نودها مشخصه های سخت افزاری مشابه دارند و توابع یکسانی را مانند توابع مسیریابی و ارسال را پردازش می کنند. مدل مدیریت از یک مدل مبتنی بر اطلاعات، تبادل پیغام ها و رویداد ها تشکیل شده است. شکل زیر عناصر واجزای شبکه را نشان می دهد.



مدل معماری امنیت

مولفه های امنیت:

برای رویارویی با مسائل امنیتی در شبکه های حسگر بی سیم تکنیک ها، الگوریتم ها و استراتژی های زیادی مطرح شده اند. برای پشتیبانی از طرح پیشنهادی و تصدیق معماری مدیریت، یک مجموعه ای از راه حل هاي مدیریتی امنیتی انتخاب شده اند. البته این مجموعه کامل نیست اما راه حلهاي خوبی رامطرح می کند. برای امنیت داده ها و جامعیت سرویس های رمزنگاری در نظر گرفته شده اند، برای توسعه و ارتقای در دسترس بودن شبکه، مکانیزم مقابله با مهاجم انتخاب شده است برای یافتن مشکلات امنیتی،مکانیزم مسیریابی امن و پیوستگی امن داده ها برای تضمین تحویل داده ها به ایستگاه پایه.

سطوح امنیت:

در شبکه های ملزم به استفاده کم از انرژی، استراتژی بدین گونه است که استفاده از اجزاء امنیتی فقط بر حسب نیاز باشد. معیار تشخیص لزوم استفاده از آن عناصر هم مبتنی بر وجود مهاجمان است. بدین معنا که با تشخیص حضور مهاجمان، به نسبت مخاطرات امنیتی، عناصر امنیتی فعال یا غیرفعال شوند. در این طرح، اجزای امنیتی به 2 دستهٔ **فعال** و **غیرفعال** پس از رخداد یک اتفاق خاص تقسیم می شوند. این منجر به ایجاد حالت های عملیاتی متفاوتی در شبکه ها می شود که سطح امنیتی نامیده می شود؛تصمیم گیری خودکار را برای مدیر بر پایهٔ اطلاعات رسیده از نودها آسانتر می کند. در هر سطح امنیتی،یک زیر مجموعه ای از عناصر امنیتی برای محافظت در برابر مهاجمان فعال می شوند. شبکه می تواند بنا به نیاز به سطوح امنیتی بالاتر تغییر حالت دهد و یا با ناپدید شدن مهاجمان یاکمبود انرژی به سطوح امنیتی پائین تر تغییر حالت دهد.

استراتژی های امنیتی درWSN:

الف- بدون راه حل امنیتی.

ب- وجود برخی راه حل های امنیتی.

ج- استفاده از یک چهارچوب امنیتی براي ایجاد تعادل بین راه حل های امنیتی و استفاده از انرژی،همان گونه که مطرح گردید.

استراتژی اول، بدون راه حل امنیتی، می تواند برای شبکه های بسته مفید باشد که در هر صورت ازحضور دشمن جلوگیری می شود. در اکثر کاربردهای رایج، حضور یک دشمن می بایست مد نظر قرارگیرد. بنابراین باید تفاوت های ما بین استفاده از انرژی را در استراتژی های دیگر مورد ارزیابی قرار دهیم، با راهکارهای امنیتی تمام وقت یا با مدیریت امنیت.