محلی سازی ایمن در شبکه های حسگر بیسیم

مریم عاقلی [1]

[1] دانشجوی کارشناسی ارشد نرم افزار، دانشگاه آزاد اسلامی ، واحد دامغان، دانشکده فنی دارالفنون،
m.aqeli1369@gmail.com

چکیده

محلی سازی ایمن نودهای ناشناخته در یک شبکه حسگر بی سیم(WSN) یکی ار مهم ترین موضوعات تحقیق است.زمانی که wsnها در مکان های خطرناکی مثلا جنگ مستقر می شوند حمله های زیادی مانند لانه کرم , منجلاب و سیبل اتفاق می افتد.دو مسئله برای محلی سازی امن نودهای ناشناخته باید در نظر گرفته شود.اول این است که ممکن است مهاجمان تغییر قیافه دهند و یا به صورت ناشناخته حمله کنند و گره های لنگر با محلی سازی امن تداخل پیدا کنند.مهاجمان ممکن است قلابی باشند, اطلاعات محلی سازی را جهت برآورد غلط موقعیت ها تغییر دهند با پخش کنند.

اخیرا محققان تکنیک های مبتنی بر محدوده و مستقل از آن مانند HiRLoc, ROPE, ,SeRLoc و.. را برای حل این دو مسئله مطرح کرده اند.در این تحقیق ما حملات رایج در این شبکه ها و الگوریتم های محلی سازی را بیان می کنیم.

کلمات کلیدی

محلی سازی ایمن, **Wsn(Wireless Sensor Network)**

1- مقدمه

محلی سازی یکی از مهم ترین موضوعات در شبکه های حسگر بی سیم(WSN) و روش های اساسی در این شبکه ها است برای مثال مسیر یابی جغرافیایی, توزیع[1] کلید جغرافیایی و تصدیق مبتنی بر مکان نیازمند موقعیت های نودهای ناشناخته هستند. همچنین موقعیت های نودهای ناشناخته نقش حیاتی در برنامه های کاربردی شبکه های حسگر بی سیم دارند از قبیل برنامه های مانیتورینگ شامل نظارت بر محیط زیست[2] , نظارت بر سلامتی و برنامه های کاربردی ردیابی شامل ردیابی اشیا , حیوانات, انسان ها و وسایل نقلیه.

زمانی که یک WSN در محیط دشمن مستقر میشه , در مقابل تهدیدات و خطرات آسیب پذیر می شود. خیلی از حملات مانند لانه کرم , منجلاب و سیبل باعث تخمین نادرست موقعیت ها می شوند بویژه برای برخی از برنامه های کاربردی مثل کاربردهای نظامی(نظارت بر میدان جنگ) یا برنامه های کاربردی محیطی مانند کشف آتش[3] سوزی جنگل , موقعیت های نادرستی که ممکن است منجر به عواقب شدید تر شود برای مثال تصمیم گیری های اشتباه نظامی در میدان جنگ و دادن هشدار غلط به مردم. از این رو مسائل محلی سازی امن باید در شبکه های حسگر بی سیم خطاب شوند.

محلی سازی امن [4]می تواند از دو جهت در نظر گرفته شود. اول اینکه, ما حملات به گره ها را بحث می کنیم , از یک مهاجم که می تواند سازش کند یا وانمود به ناشناخته شدن کند یا یک گره لنگر که با فرایند محلی سازی تداخل پیدا می کند.بنابراین ما نیازمند احراز هویت گره امن هستیم(SNA). دوم اینکه ما درباره حملات به اطلاعات از یک مهاجم که می تواند اطلاعات محلی سازی را برای تخمین نادرست موقعیت ها جعل ,[5] تغییر یا پخش کند بحث می کنیم.بنابراین ما نیاز به کشف صحت اطلاعات محلی سازی داریم, که در این مقاله آن را تایید اطلاعات امن می نامیم(SIV). در ادامه مقاله به شرح زیر است: بخش دوم حالت های بیانیه مشکل. بخش سوم توضیحات مدل حمله. بخش چهارم و پنجم نمایش شمای SIV و SNA می باشد.بخش ششم نتیجه گیری و مشکلات تحقیقات باز را می دهد.

2- معرفی شبکه حسگربیسیم(WSN)

شبکه حسگر/کارانداز (حس/کار) شبکه ای است متشکل از تعداد زیادی گره کوچک. در هر گره تعدادی حسگر و/یا کارانداز وجود دارد. شبکه حس/کار بشدت با محیط فیزیکی تعامل دارد. از طریق حسگرها اطلاعات محیط را گرفته و از طریق کار انداز ها واکنش نشان می دهد. ارتباط بین گره ها بصورت بی سیم[6] است. هرگره بطور مستقل و بدون دخالت انسان کار میکند و نوعا از لحاظ فیزیکی بسیار کوچک است ودارای محدودیت هایی در قدرت پردازش, ظرفیت حافظه, منبع تغذیه, ... میباشد. این محدودیت ها مشکلاتی را بوجود می آورد که منشأ بسیاری از مباحث پژوهشی مطرح در این زمینه است.

2-1-ساختار کلی شبکه حس/کار بی سیم

حسگر : وسیله ای که وجود شیئ رخداد یک وضعیت یا مقدار یک کمیت فیزیکی را تشخیص [8]داده و به سیگنال الکتریکی تبدیل می کند. حسگر انواع مختلف دارد مانند حسگرهای دما, فشار, رطوبت, نور, شتاب سنج, مغناطیس سنج و...

کارانداز : با تحریک الکتریکی یک عمل خاصی مانند باز و بسته کردن یک شیر یا قطع و وصل یک کلید را انجام می دهد.

گره کارانداز: به گره ای گفته می شود[9] که فقط شامل یک یا چند کارانداز باشد.

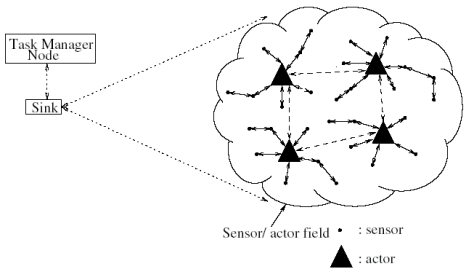
گره حسگر/کارانداز: به گره ای گفته می شود که مجهز به حسگر و کار انداز باشد.

شبکه حسگر : شبکه ای که فقط شامل گره های حسگر باشد. این شبکه نوع خاصی از شبکه حس/کاراست. در کاربردهایی که هدف جمع آوری اطلاعات و تحقیق در مورد یک پدیده می باشد کاربرد دارد. مثل مطالعه روی گردبادها.

میدان حسگر/کارانداز : ناحیه کاری[10] که گره های شبکه حس/کار در آن توزیع میشوند.

چاهک: گرهی که جمع آوری داده ها را به عهده دارد. و ارتباط بین گره های حس/کار و گره مدیر وظیفه را برقرار می کند.

گره مدیر وظیفه: گرهی که یک شخصی بعنوان کاربریا مدیر شبکه از طریق آن با شبکه ارتباط برقرار میکند. فرامین کنترلی و پرس و جو ها از این گره به شبکه ارسال شده و داده های جمع آوری[11] شده به آن بر میگردد.



شکل(1): ساختار کلی شبکه های حسگر بی سیم

2-2- کاربردهای WSN

کاربردها به سه دسته نظامی تجاری پزشکی تقسیم می شوند. سیستم های ارتباطی, فرماندهی, شناسایی, دیده بانی ومیدان مین هوشمند, سیستم های هوشمند دفاعی از کاربردهای نظامی[7] می باشد. در کاربردهای مراقبت پزشکی سیستم های مراقبت از بیماران ناتوان که مراقبی ندارند. محیطهای هوشمند برای افراد سالخوده و شبکه ارتباطی بین مجموعه پزشکان با یکدیگر و پرسنل بیمارستان و نظارت بر بیماران از جمله کاربرد های آن است.کاربردهای تجاری طیف وسیعی از کاربردها را شامل می شود مانند سیستم های امنیتی تشخیص و مقابله با سرقت, آتش سوزی(درجنگل), تشخیص آلودگی های زیست محیطی از قبیل آلودگی های شیمیای, میکروبی, هسته ای, سیستم های ردگیری, نظارت وکنترل وسایل نقلیه و ترافیک, کنترل کیفیت تولیدات صنعتی, مطالعه در مورد پدیده های طبیعی مثل گردباد, زلزله, سیل, تحقیق در مورد زندگی گونه های خاص از گیاهان و جانوران و .. در برخی از کاربردها نیز شبکه حس/کار بعنوان گروهی از رباتهای کوچک که با همکاری هم فعالیت خاصی را انجام می دهند استفاده میشود.

3 – محلی سازی ایمن در شبکه های حسگر بی سیم

3-1- بیان مشکلات

قبل از بحث درباره مشکلات محلی سازی ضروری است به نگاهی به برخی از مفاهیم کلی استفاده شده در فرایند محلی سازی بیاندازیم.اساسا دو دسته بندی برای نودهای حسگر وجود دارد: نودهای لنگر و ناشناخته.نودهای ناشناخته [12]هیچ آگاهی از موقعیتشان و یا سخت افزار خاصی برای بدست اوردن موقعیت خود ندارند. نودهای لنگر که همچنین نودهای فانوس دریایی نیز نامیده می شوند در حقیقت موقعیتشان بوسیله قرار دادن دستی یا تجهیزات اضافی مانند GPS(سیستم تعیین موقعیت جهانی) بدست می آیند.بنابراین نودهای ناشناخته می توانند از با استفاده از اطلاعات محلی نودهای لنگر اطلاعات خود را محلی کنند.معمولا فرایند محلی سازی به دو مرحله تقسیم می شود: 1- کسب اطلاعات 2- تعیین موقعیت.

3-1-1-کسب اطلاعات

تقریبا طرح های محلی موجود WSNها به دو دسته[13] تقسیم می شوند: طرح بر اساس محدوده و طرح های آزاد برد یا بدون محدوده. برای طرح های محلی سازی مبتنی بر محدوده فاصله یا اطلاعات زاویه توسط RSSI(دریافت سیگنال شاخص قدرت) TOA(زمان رسیدن به مقصد) TDOA اختلاف زمان در رسیدن به مقصد و AOA زاویه ورود اندازه گیری می شود. برای طرح های محلی[14] بدون محدوده ,محلی سازی بر اساس اتصال به شبکه یا اطلاعات دیگر انجام میشود

که می تواند[15] توسط DV-Hop , محدب بهینه سازی و MDS-MAP بدست آید.

3-2-2- تعیین موقعیت

طرح های تعیین موقعیت[16] به دو دسته تقسیم می شوند:1- طرح های مبتنی بر ترمینال 2- طرح های مبتنی بر زیر ساخت. در طرح های مبتنی بر ترمینال نودهای ناشناخته خودشان را محلی می کنند. پس از اتصال اطلاعات موجود در مورد فاصله[17] /زاویه و موقعیت گره لنگر, موقعیت یک نود ناشناخته می تواند به سادگی بوسیله سه زاویه ای, چند بعذی و سه گوش کردن بدست آید.در طرح های مبتنی بر زیر ساخت گره های مرجع [18]شامل گره های همسایه مورد اعتماد هستند.اساسا گره های لنگر برای محلی سازی گره های ناشناخته هستند.

دشمنان می توانند در دو مرحله[19] به محلی سازی حمله کنند.هدف دشمن به دست آوردن موقعیت های نادرست گره های ناشناخته با به خطر انداختن گره های عادی و فرستادن اطلاعات غلط یا وانمود کردن به نودهای قانونی بودن برای تغییر, جعل و پخش سیگنال ها است.بنابراین اقدامات امنیتی برای ایجاد موقعیت های تخمین زده شده تحت حمله مورد نیاز است.فرایند محلی سازی می تواند با راه های مختلفی مورد حمله قرار گیرد.محققان مجموعه ای از حمله های شناخته شده را معرفی کرده اند.حملات شناخته شده می تواند به دو دسته تقسیم شوند: حملات داخلی[20] و خارجی

دشمن اگر خارج WSN باشد و پیاده سازی رفتارهای مخرب بدون کلید رمزنگاری راست باشد خارجی است.

دشمنی که داخلی است[21] می تواند یک یا چندین نود متقلب را کنترل کند.

3-انواع حملات

در این مقاله حملات به[26] دو دسته تقسیم می شوند:

الف)حمله نودها

ب)حمله به اطلاعات

3-1-حمله به نودها

در این مقاله نودهای مخرب شامل مهاجمان و نودهای به خطر افتاده است. یک مهاجم یک نود خارجی است که خودش را به WSN تحمیل می کند.یک نود به خطر افتاده[27] یک نود معمولی است (با یک نود لنگر یا ناشناخته) که توسط مهاجم تحت خطر قرار گرفته است.

حمله به نودها به صورت زیر لیست شده اند:

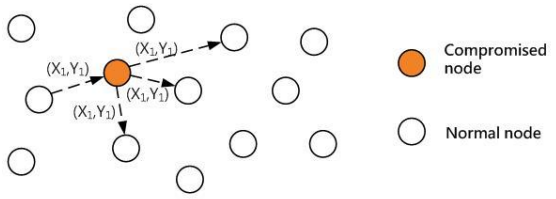
- **سازش**

سازش گره اساسی ترین حمله[20] در WSN است که منجر به حملات دیگر می شود. این زمانی اتفاق می افتد که یک مهاجم دستاوردهای یک نود را در WSN کنترل کند.به طور معمول نودهای به خطر افتاده می توانند به وسیله متدهای زیر بوجود آیند:

1)مهاجمان نودهای معمولی را گرفته و آن ها را مجدد برنامه ریزی می کنند

2)مهاجمان نودها را با منابع محاسباتی[22] بزرگتر مانند لپ تاپ ها برای حمله به نودهای معمولی گسترش می دهند.

با نود به خطر افتاده یک مهاجم می تواند نود را برای شنود اطلاعات در WSN , لغو گره های قانونی, داده های مخرب ورودی و حملات داخلی مانند DOS , تغییر دهد.



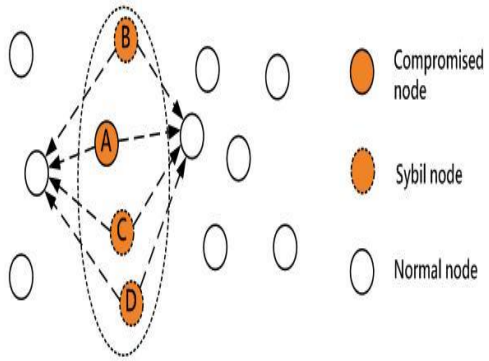
شکل(2): حمله سازش(Compromise)

- **تکثیر**

اگر یک دشمن[23] برای تصرف یک گره مدیریت شود و کلیدهای رمزنگاری و تصدیق را استخراج کند, می تواند تعداد زیادی کپی از آن گره با همان id تولید کند و آن را در مکان های انتخاب شده در WSN قرار دهد که این نوع حمله, حمله تکثیر گره نامیده می شود. از آنجایی که اعتبار کپی ها همه کلون هایی هستند که از نودها گرفته شده است, کپی ها می توانند به عنوان اعضای قانونی شبکه در نظر گرفته شوند.به نظر می رسد که دشمن[24] نتواند idهای جدیدی برای نودهای تکثیر شده ایجاد کند, از آنجایی که مهاجمان مجبورند امنیت اطلاعات مربوطه(کلیدها , کدها و غیره) را ایجاد کنند, در اکثر مواقع این کار خیلی سخت و نشدنی است.هنگامی که دشمن یک یا چند نود حسگر را کپی می کند, آن می تواند عملیات مخرب را اجرا کند.مثلا, نودهای کپی شده ممکن[25] است اطلاعات محلی سازی کاذب را به WSN تزریق کنند.

- **حمله Sybil:**

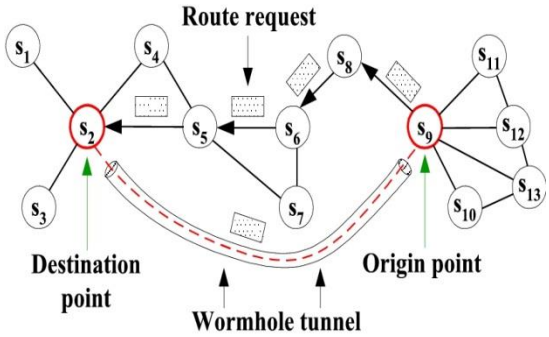
حمله سیبل بوسیله یک نود مخرب راه اندازی شده که چندین هویت مجازی دارد(id). هویت های اضافی گره های مخرب را به عنوان نودهای سیبل اشاره داریم.یک نود Sybil می تواند هویت را از یکی از دو راه زیر بگیرد.می تواند[24] یک هویت جدید بسازد یا هویت را از یک نود قانونی سرقت کند.یک نود Sybil می تواند یک پیام را با idهای مختلف ارسال کند.برای مثال ,در فرایند محلی سازی یک نود مخرب , ممکن است به صورت چندین نود لنگر برای ارسال اطلاعات غلط در همان زمان تغییر قیافه دهد.



شکل(3): حمله سیبل

- **حمله لانه کرم(کرم چاله):**

در [25]یک حمله کرم چاله, مهاجم بسته یا بیت های منحصر به فرد یک بسته را در یک مکان در شبکه را ثبت می کند. سپس بسته را(احتمالا به صورت انتخابی) به مکان دیگر تونل می زند و آن را کپی می کند. تونل می تواند به روش های مختلفی تاسیس شود, برای مثال از طریق کانال باند , کپسوله سازی بسته, انتقال با قدرت بالا, تقویت بسته و انحراف پروتکل در فرایند محلی سازی, حمله ممکن است به صورت کامل متفاوت و با اطلاعات محلی سازی اشتباه تونل بزند.



شکل(4): حمله (wormhole)

3-2- حمله به اطلاعات

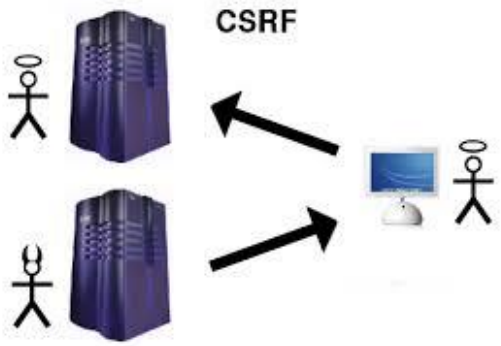
در سیستم های محلی سازی, نودهای ناشناخته همیشه اطلاعات محلی سازی نود لنگر[32] را برای محلی سازی خودشان استفاده می کنند هدف نودهای مخرب معمولا ایجاد اطلاعات نادرست از محلی سازی است.حمله به اطلاعات به صورت زیر دسته بندی شده اند:

- **جعل اسناد:**

در حمله های جعل اسناد , نود مخرب اطلاعات گمراه کننده را در سیستم های محلی سازی ارسال می کند برای مثال در سیستم فعال, نود مخرب وانمود به نود لنگر[26] بودن می کند تا به طور داوطلبانه اطلاعات را ارسال کند.در سیستم غیر فعال, نود مخرب وانمود به نود ناشناخته بودن می کند تا محلی شود.

- **تغییر:**

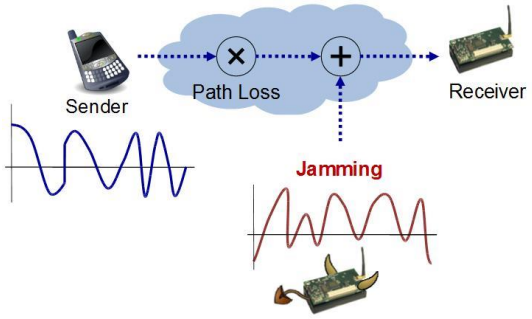
این حمله مستقیم ترین [27]حمله است. اهداف این حمله رد و بدل کردن اطلاعات بین یک نود ناشناخته و یک نود لنگر است. دشمنان ممکن است به طور مستقیم مختصات, زمان یا تعدادی هاپ را تغییر دهند و خطاهای محلی سازی نودهای ناشناخته را افزایش دهند. برای مثال در یک همکاری همه نودهای مخرب می توانند با یکدیگر برای تغییر اطلاعات تبانی کنند.



شکل(5):حمله (forgery)

- **تداخل:**

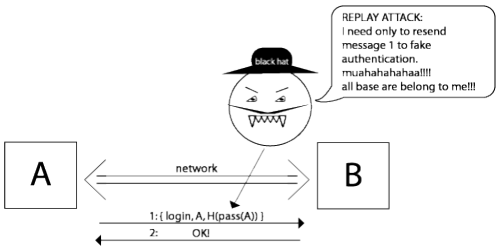
حمله[31] تداخل نود مخربی است که با اندازه گیری سیگنال تداخل دارد. برای مثال در سیستم های محلی سازی مبتنی بر محدوده نودهای مخرب ممکن است موانعی بین سیگنال ارسال کننده و دریافت کننده را برای طولانی تر کردن زمان اشغال , تغییر زاویه ورود یا تضعیف قدرت سیگنال دریافت شده قرار دهند.



شکل(6):حمله تداخل(Interference)

- **پخش:**

عمومی ترین یا ساده ترین[33] نوع حمله است, به ویژه زمانی که قابلیت ها ومنابع دشمن محدود شده است.در این نوع حمله نود مخرب اطلاعات انتقالی بین فرستنده و گیرنده را می گیردسپس اطلاعات قدیمی را پخش می کند. با استفاده از اطلاعات قدیمی نودهای ناشناخته موقعیت های نادرست را محاسبه می کنند. بر خلاف حملات دیگر , حمله پخش می تواند با یک نود کل شبکه را نابود کند.



شکل(7):حمله پخش (replay)

- **سیل:**

مانند حملات جاری شدن[29] سیل اطلاعات در پروتکل مسیریابی , حمله سیل در محلی سازی به صورت نود مخربی است که مقدار زیادی از بسته های داده را غیر قابل استفاده را به همه نودها در دامنه ارتباطات خود پخش می کند. مشخصه بارز حمله سیل اگزوز خروجی قابل دسترسی پهنای باند ارتباطات شبکه است بنابراین دیگر نودها نمی توانند با یکدیگر ارتباط داشته باشند. علاوه بر این , فرستنده گیرنده برای ارسال یا دریافت بسته های زیاد از مهاجم و مصرف مقدار زیادی از منابع شبکه اشغال است.

- **حمل و نقل انتخابی:**

در [30]حمله حمل و نقل انتخابی, نود مخرب مانند سوراخ سیاه رفتار می کند. حمله حمل ونقل انتخابی برای تشخیص دشوار است . اول اینکه برای جلوگیری از افزایش سو ظن و تردید دشمن یک بسته انتخابی را به جای هر بسته ای رها می کند.بعلاوه دلایل زیادی در رها کردن بسته وجود دارد برای مثال ارتباطات بی سیم نا معتبر.
و در بعضی موارد نودهای حساس برای ذخیره نیرو به حالت خواب می روند آن ها نمی توانند در این دوره داده ای ارسال یا دریافت نمایند بنابراین برای تشخیص بسته ترک تحصیل کرده ایجاد شده توسط حمل و نقل انتخابی یا هر دلیل دیگر ضروری است.

3- الگوریتم های محلی سازی امن برای نودهای ناشناخته

در این مقاله ما محلی سازی امن برای نودهای ناشناخته را نیز به دو دسته تقسیم می کنیم :

3-1-محلی سازی امن بر اساس محدوده :

- **VMو Spine**

پیشنهاد چند[37] بعدی تایید شده(VM) با یک قدرت مرکزی و چندین نود لنگر که تصدیق کننده نیز نامیده می شود, VM یک محاسبه و رسیدگی امن از موقعیت های نودهای ناشناخته در حضور مهاجمان را قادر می سازد .

در VM بازبین ها (v1,v2,….vn) که در محدوده [33]ارتباطی گره نامعلوم u هستند, فاصله را به گره u متصل می کنند و کران های فاصله db1,…dbn را حاصل می آورند. این کران های فاصله و موقعیت های بازبین ها به مرجع مرکزی گزارش می شوند. آنگاه این مرجع یا منبع یک موقعیت تخمینی (Xu, Yu) گره نا معلوم را با استفاده از کران های فاصله محاسبه می کند.سپس این منبع دو آزمایش را اجرا می کند :1) آزمون -6 برای تمام cVi آیا فاصله بین (Xu ,Yu) و Vi از کران فاصله اندازه گیری شده dbi تفاوت دارد؟این فاصله کمتر از اشتباه اندازه گیری فاصله 6است؟
2)نقطه گذاری در آزمون مثلث , آیا (Xu,Yu) درون حداقل یک مثلث فیزیکی شکل گرفته توسط یک سه تایی بازبین قرار می گیرد؟اگر 6 و این نقطه گذاری در آزمون های مثلث مثبت باشند, مرجع (Xu,Yu) را صحیح می داند, در غیر این صورت موقعیت پذیرفته نمی شود.
بر اساس VM , محققان [31],[34],یک مکانیسم موقعیت یابی ایمن و هماهنگ را با نام Spine پیشنهاد دادند.Spine در 3 مرحله اجرا می شود:1)گره های ناشناخته کران های فاصله را تا مجاورهای خود اندازه گیری می کنند2)کران های فاصله از طریق VM تایید می شوند و 3)موقعیت های گره های نامشخص از طریق یک [39]الگوریتم توزیعی با به وسیله مرجع مرکزی با استفاده از یک الگوریتم متمرکز موقعیت یابی محاسبه شوند.بنابراین گره ها در Spine نمی توانند اندازه گیری های متعدد فاصله را ایجاد کنند. با این وجود Spine به منظور انجام چند جانبی قابل تایید , چند مشکل دارد و وجود تعداد بالایی از بازبین ها لازم و ضروری است.

- **SLA**

انجوم و همکارانش یک الگوریتم محلی سازی[35] ایمن با نام SLA را ارائه دادند.بررسی می شود که هر گره انکر به منطور تغییر سطح قدرت دارای یک توانایی است.هر سطح قدرت با یک محدوده ارتباطی مطابقت دارند .زمانیکه یک گره نامعلوم در یک محل قرار می گیرد گره سینک از گره های انکر می خواهد تا یک نانس محل را به این گره بر طبق سطوح متفاوت قدرت بفرستد. در نتیجه, هر گره نا معلوم یک مجموعه نانس منحصر یه فرد دارد و آن ها را به حالت برگشتی, به سینک دوباره می فرستد. این سینک سپس موقعیت گره نامعلوم را تعیین می کند.در مقایسه با VM , SLA نیاز به همزمان سازی ندارد.اما مدل سطح قدرت و محدوده انتقال برای محیط بیرونی مناسب هستند نه برای محیط درونی.علاوه بر آن SLA دارای چند اشکال و عیب است:1) فرض می شود که گره های انکر و سینک مطمئن هستند 2)تنها بررسی یک گره سنسور مورد توافق قرار می گیرد و جلوی حملات مشترک بین گره های سنسور گرفته می شود

3)SLA یک رویکرد متمرکز است که موانع و معایب را در ایستگاه ایجاد می کند.

- SLS

ژانگ و همکارانش SLS را برای شبکه های سنسور با پهنای باند فوق العاده(UWB) را پیشنهاد می کنند.به منظور محلی سازی یک گره , گره های انکر در ابتدا فاصله مربوطه با گره را به وسیله یک روش دو طرفه TOA به نام فاصله -k اندازه گیری می کند.لنگر رهبر, تمام فاصله های تخمینی را جمع آوری می کند و به موجب آن محل mmse را برآورد می کند.متعاقبا, SLS یک آزمون صحت منطقه را از طریق بررسی آنکه آیا منطقه داخل چند ضلعی است یا نه اجرا می کند, این چند ضلعی توسط تمام گره های انکر به منظور کشف حملات احتمالی شکل می گیرد.در مقایسه با VM , SLS قوی تر است و با استفاده از گره های متحرک انکر, گره های ثابت را جایگزین می کند و باعث می شود هر گره انکر به عنوان رهبر به منظور متعادل کردن کاربرد منابعشان شرکت کند.با این وجود پروسه SLS نسبت به پروسه VM پیچیده تر است و انرژی بیشتری را مصرف می کند.

در [39] , بر اساس مدل مبتنی بر حمله , طرح محلی سازی پیشرفته و ایمن(ESLS) پیشنهاد گردید, این طرح ایده مطرح شده در [38] را توسعه و بسط می دهد و نه تنها بر ضد حملات کاهش فاصله بلکه بر ضد حملات گسترش فاصله دفاع می کند. مهمترین مشارکت آن در اولین زمان, استفاده از شبکه perti به منظور تایید طرح امنیت برای WSN است.

- GML

در [40] اریسار و همکارانش یک مکانیسم مکان یابی , ملاقات و برخورد (GML) را برای تخمین منطقه امن بر اساس بخشی کردن جغرافیایی ارائه دادند.GML شامل سه مرحله است: برخورد , ملاقات و مکان یابی. 1)برخورد یا تلاقی: یک طرح تعیین اعتبار سبک , پروتکل +HB که به منظور اجرای تعیین اعتبار دو طرفه از طریق گره های نامعلوم و انکر به کار می رود 2)ملاقات: استفاده از الگوریتم تعویض کلید Diffie Hellman امکان تعویض کلیدهای اشتراکی و مخفی بین دو کاربر را در یک محیط مخالف در طی یک رسانه ارتباطی نا امن فراهم می کند. 3)مکان یابی: این مکان بر اساس تکنیک مبتنی بر TOA(زمان رسیدن به مقصد) تخمین زده می شود.علاوه بر آن یک مکانیسم, میانگین شدن دو برابر به منظور به حداقل رساندن خطای مکان یابی ارائه می شود.

3-2- محلی سازس ایمن محدوده آزاد:

- SerRloc

در [43] , محققان یک الگوریتم محلی سازی محدوده آزاد با نام SeRloc ارائه می کنند , این الگوریتم نیازی به ارتباط بین گره های ناشناخته ندارد.SerLoc از مکان یاب های مجهز به یکسری آنتن های قدرت بالا به منظور جایگزین کردن گره های انکر, استفاده می کند.این محل یاب ها نسبت به گره های نامعلوم دارای محدوده ی ارسالی طولانی تری هستند.آن ها امواج رادیویی را به گره های نامعلوم می فرستند , این امواج شامل موقعیت های آنها و نواحی آنتن است.زمانیکه یک گره از محل چند مکان یاب باخبر می شود این گره مرکز گرانش بخش های مرتبط با مکان یاب ها را به عنوان موقعیت خود محاسبه می کند.SerLoc در برابر حملات شدید WSN مثل حمله wormhole یا کرم چاله , حمله Sybil و گره های سنسور مقاوم است.با این وجود SerLoc بر اساس این فرضیه است که هیچ پارازیتی از جانب رسانه بی سیم وجود ندارد.و از حملات مبتنی بر اطلاعات محل یاب دفاع نمی کند, حملاتی که به وسیله ی بررسی ویژگی های شبکه مثل یگانگی بخش و محدوده ارتباطی اجتناب می شوند. علاوه بر آن به منظور کاهش منطقه مشترک و بهبود مکان یابی, ما نیاز به افزایش تعداد مکان یاب ها و آنتن ها داریم.

به منظور کاهش این تاثیر بر روی صحت منطقه در SerLocهمانند امواج رادیویی گمراه کننده انکر, سیستم قوی موقعیت یابی ROPE ارائه گردید, این تاثیر به وسیله حملات متفاوت ایجاد می شود.با ترکیب ها تکنیک ها در SerLoc و VM , ROPE هم وظیفه تعیین محل و هم وظیفه تایید محل را دارد.در تعیین محل, هر گره نا معلوم , منطقه دقیق خود را به وسیله VM به دست می آورد زمانیکه حداقل درون یک سه گوش شکل گرفته توسط محل یاب ها قرار می گیرد و زمانی که درون هر 3 گوشی قرار نگیرد هنوز محل خود را به وسیله مرکز جاذبه تخمین می زند.مکانیسم تایید محل, تقاضاهای گره های نامعلوم را برای محل تایید می کند.از آنجا که هر گره نامعلوم می تواند با حداقل یک مکان یاب ارتباط داشته باشد زمانیکه گره نا معلوم داده ها را به محل یاب گزارش می کند, محل یاب می تواند موقعیت گره نا معلوم را از طریق اجرای پروتکل اتصال فاصله تایید می کند: در مقایسه با SerLoc , ROPE در برابر پارازیت رسانه ی ارتباطی مقاوم است و حداکثر تاثیر حقه بازی را محدود می کند و به علت حمله Sybil , به وسیله آرایش چگالی پایین محل یاب ها, مانع از حقه بازی محل می شود.با این وجود, ROPE درای نیازهای بالاتر سخت افزاری مثل همزمان سازی زمان نانوثانیه و ظرفیت پردازش لحظه ای است, این ظرفیت برای WSN ارزان قیمت مناسب نیست.

در [46] , زنگ و همکارانش یک طرح محلی سازی را مبتنی بر شمارش پرش(Hop-Count)(SHoloc) ارائه می دهند, این طرح

در برابر حملات گوناگون مثل حمله کاهش شمارش پرش و بسته های جعلی مقاوم است.در SHoloc , گره های انکر, مسئول بررسی امکان ناپذیری فاصله بین گره ها هستند.در پایان از کوچکترین مربعات میانگین(LMS) به منظور بررسی مراجع بدمحل استفاده می شود.

PLV -

در [50],[49] الگوریتم تصدیق احتمالی محل(PLV) ارائه می گردد.مهمترین ایده تاثیر روابط آماری بین تعداد پرش ها در یک شبکه سنسور و فاصله اقلیدسی است.در ابتدا, یک گره نامعلوم , پیامی را در شبکه با استفاده از غرقه سازی(جاری شدن سیل) منتشر می کند, این پیام شامل منطقه ی آن و شمارش یا تعداد پرش می باشد.هر بازبین یا تصدیق کننده ی دریافت کننده این پیام می تواند فاصله نسبی بین آن و گره نامعلوم را محاسبه کند.سپس هر بازبین, حداکثر مقادیر احتمال و مقادیر سکون احتمال را محاسبه می کند. در پایان گره مرکزی دو مقادیر احتمال را از اتمام بازبین ها جمع آوری می کند و صحت انتشار محل محاسبه می شود.

گره مرکزی از این صحت به منظور پذیرفتن یا رد محل استفاده می کند.

بر اساس پروسه منطقه یابی DV-Hop , وو و همکارانش یک طرح محلی سازی ایمن مبتی بر مطلب به منظور دفاع در برابر حمله ی wormhole پیشنهاد می دهند, در این طرح بسته های تحویل داده شده از طریق پیوند با حلقه wormhole حذف می شوند.در ابتدا گره های انکر متمایز و مطابق با ارتباط جغرافیایی آنها, طبقه بندی می شوند.سپس گره های نامعلوم متمایز و با استفاده از نتایج طبقه بندی گره های انکر مجاور, طبقه بندی می شوند.پس از حذف ارتباطات غیر طبیعی بین گره های طبقه بندی شده مجاور انکر به وسیله حمله ی wormhole آلوده شده اند, روش منطقه یابی DV-Hop می تواند اجرا شود.طرح محلی سازی DV-Hop بر اساس برچسب یا طبقه بندی می تواند حمله wormhole را کشف کند و در برابر اثرات گوناگون آن با احتمال بالایی مقاومت کند.

در [52] ابرا اویی و همکارانش یک طرح محلی سازی DV-Hop مستقل از wormhole (WFDV) را به منظور خنثی کردن حملات wormhole در الگوریتم DV-Hop پیشنهاد دادند.مهم ترین نظرWFDV , پلاگین متقابل فعال با نام جلوگیری از آلودگی در برابر طرح DV-Hop است.جلوگیری از آلودگی شامل دومرحله است:ساخت لیست مجاور یا همسایه (NLC) و اصلاح لیست همسایه (NLR). NLC , RSSI و RTT (تاخیر سفر دو طرفه یک لینک) را به کار می برد و از اطلاعات محلی برای ساخت لیست های همسایه استفاده می کند.NLR تنها زمانی به کار می رود که حمله ی wormhole به منظور حذف بسته های تحویلی از طریق لینک wormhole حدس زده شود.در این مرحله, از مکانیسم های CTS , RTS و جهش زیادی به منظور تایید وجود wormhole و اصلاح لیست های همسایه استفاده می شود.

پس از حذف ارتباطات غیر قانونی, روش محلی سازی DV-Hop می تواند با موفقیت اجرا شود.

مقایسه طرح های بالا(طرح های محدوده سازی ایمن محدوده آزاد) در جدول II نشان داده شده است.

محلی سازی امن برای گره های انکر:1) طرح های محلی سازی ایمن: دو و همکارانش LAD(کشف نابهنجاری محلی سازی) را به منظور کشف گره های غیر طبیعی انکر در پروسه های محلی سازی پیشنهاد می کنند.

زمانی که گره های سنسور به صورت گروه ها آرایش می یابند, هر گروه, توزیع دو بعدی نرمال را دنبال می کند, این توزیع در مرکز نقطه آرایش گروه گره قرار می گیرد.فرض می شود که مرحله محلی سازی تقریبا به پایان رسیده است و هر گره نامعلوم تقریبا یک موقعیت را بدست آورده است . LAD از اطلاعات آرایش بندی و ارتباط گروه بین گره های سنسور مجاور استفاده می کند تا بررسی کند آیا موقعیت های محاسبه شده ی گره های نامعلوم با اطلاعات مشخص شده ی آرایش بر طبق سه معیار مطابقت دارد یا نه, این 3 معیار شامل معیار تفاوت معیار جمع کل و معیار احتمال می باشند.LAD دارای سرعت بالای کشف و میزان پایین اشتباه است, اما گره های غیر طبیعی , انکر را پس از کشف آنها بررسی نمی کند.

لیو و همکارانش یک تکنیک مناسب را به منظور کشف و حذف گره های انکر به خطر افتاده پیشنهاد می دهند.

گره های انکری که مسئول کشف هستند, گره های کشف کننده نامیده می شوند و گره ی انکر کشف شده , گره هدف نامگذاری می گردد.در ابتدا گره کشف کننده با استفاده از id متفاوت گره با نام id کشف کننده پیام درخواست را به یکدیگر می فرستند, این گره یک گره مشترک است.زمانیکه گره هدف پیام را دریافت میکند , آن را به سیگنال رادیویی می فرستد, این سیگنال شامل منطقه گره است, این گره می تواند فاصله بین آنها را بر اساس منطقه خود و منطقه گره هدف محاسبه کند.اگر تفاوت بین آن ها بزرگتر از حداکثر خطای فاصله بود, گره کشف کننده می تواند استنباط کند که سیگنال رادیویی دریافت شده مغرضانه است.سپس از کشف کننده wormhole و RTT(زمان سفر رفت و برگشت) به منظور فیلتر کردن سیگنال های رادیویی آرایش یافته از wormhole و سیگنال های رادیویی محلی استفاده می شود.در پایان ایستگاه بررسی می کند که آیا تعداد اعلان خطر گره هدف بیشتر از آستانه ی معین است یا نه. اگر این تعداد بیشتر باشد گره هدف به عنوان یک گره مخرب در نظر گرفته می شود و از شبکه حذف می شود.

در DRBTs [55] و [56] اسرینیواسان و همکارانش یک طرح مبتنی بر اعتبار یا شهرت جدید با نام سیستم اطمینان به امواج رادیویی مبتنی بر اعتبار و شهرت (DRBTS) برای خارج کردن گره های مخرب انکر, پیشنهاد می دهند.DRTBS یک پروتکل توزیع شده امنیت در جهت گسترش این طرح در [59] است.در DRBTS

هر گره انکر همسایگی یک جهشی خود را به جهت گره های بد رفتار کنترل می کند و بر طبق آن , اعتبار گره انکر مجاور خود را در جدول اعتبار-همسایه (NRT) به روز رسانی می کند.بنابراین این گره های نامعلوم می توانند چند گره معتبر انکر را بر اساس روش حداکثر آرا انتخاب کنند.

گره های نامعلوم تنها از گره های معتبر انکر برای محاسبه موقعیت خود استفاده می کنند, این اعتبار و اعتماد توسط گره های انکر مجاور مشخص می شود..

حتی زمانیکه گره های انکر مخرب بیشری نسبت به گره های انکر بی خطر در WSN وجود داشته باشند, TMCA هنوز می تواند به منظور ایجاد نتایج دقیق محلی سازی , به خوبی کار کند.

مقایسه طرح های بالا(محلی سازی ایمن برای نودهای انکر) در جدول III نشان داده شده است.

طرح های SIV را می توان به دو گروه طبقه بندی کرد: اطلاعات تایید کننده محل و اطلاعات فیلتر کننده محل.

کارهای زیادی در جهت فیلتر کردن تاثیر اطلاعات نادرست محل گره های انکر انجام شده اند.در [58] , لی و همکارانش تحمل و مقاومت در برابر حملات را بجای حذف آن پیشنهاد می دهند.دو طبقه از محلی سازی با نام مثلث بندی و انگشت نگاری مبتنی بر RF آزمایش می شوند.برای محلی سازی مبتنی بر مثلث بندی , از LMS به منظور فیلتر کردن اطلاعات اشتباه محلی سازی استفاده می شود . برخلاف روش های قدیمی که خطای یک مربع حسابی رابه حداقل می رساند, روش LMS میانگین خطاهای مربع را کاهش می دهد.

یک روش مبتنی بر انگشت نکاری , با اندازه کافی ایمن نیست از این رو آن ها روش نزدیک ترین همسایه مبتنی بر میانگین را ارائه می کنند.

لیو و همکارانش دو روش مبتنی بر محدوده را برای منطق مقاومت در برابر حملات دشمن را پیشنهاد می دهند.اولین روش تخمین منطقه مقاوم در برابر حمله با نام ARmmSE است. در ابتدا ARmmSE از روش های مبتنی بر mmSE به منظور تخمین موقعیت گره های نامعلوم استفاده می کند.سپس, ARmmSE ارزیابی می کند که آیا این موقعیت تخمین زده شده می تواند از یکسری اطلاعات همسان محل گره های انکر نشئت بگیرد یا نه. اگر این موقعیت تخمینی از از اطلاعات همسان نشئت بگیرد , موقعیت تخمین زده شده پذیرفته می شود, در غیر این صورت اطلاعات مخالف و ناسازگار محل, شناسایی و حذف خواهند شد.این پروسه ممکن است تا زمانی ادامه یابد که یک سری اطلاعات سازگار محل یافت شود یا امکان پیدا کردن چنین مجموعه ای وجود نداشته باشد.

دومین روش تخمین محل بر اساس رای گیری است.ARmmSe یک سری اطلاعات محلی بدست می اورد که این اطلاعات میانگین خطای مربع حسابی را بر اساس زیر مجموعه آستانه محاسبه می کند.در الگوریتم مبتنی بر رای گیری , حوزه استقرار به یک شبکه از سلول ها تقسیم می شوند. هر گره انکر به سلول های تقسیم شده رای می دهد و مرکز سلول ها با بالاترین رای , موقعیت تخمینی گره نامعلوم است.

در [61] ژانگ و همکارانش اثبات می کنند که الگوریتم هایی وجود دارند که درجه تضمین دقت محلی سازی را ارائه می دهند, اگر تعداد گره های انکر مخرب کمتر یا مساوی (n-3/2(Kmax=n-3/2 باشد(n تعداد گره های انکر است). همچنین دو الگوریتم به منظور تعیین محل گره های نامعلوم بر اساس پیدا کردن یک منطقه داخل حلقه های Kmax+3 ارائه می شوند.با این وجود, چنین نتیجه ای تحت شرایطی حاصل می آید که خطای اندازه گیری اپسیلون باشد.در حمله آلودگی(pollution) , زمانیکه Kmax=n-3/2 باشد این دشمن می تواند به طور جدی موقعیت تخمین زده شده را بد جلوه دهد.

در [63] میسرا و همکارانش یک آستانه بحرانی B را برای تعداد گره های مخرب انکر پیشنهاد می دهند, این آستانه می تواند در پروسه محلی سازی بدون متزلزل ساختن دقت و درستی حفظ شود.

اگر گره های انکر n در محدوده ارتباطی یک گره ی مخرب وجود داشته باشند , حداکثر تعداد گره های مخرب انکر که می توانند مقاومت کنند , [n/2]-2 است. سپس , تکنیک پیشرفته و معتبر تعیین فاصله (E-MAD) به منظور فیلتر کردن گره های به خطر افتاده ی انکر پیشنهاد می شود. پروتکل E-MAD مانع از حملات کاهش فاصله می شوند.بنابراین گره های مخرب انکر پروسه ی محلی سازی را از طریق گسترش فاصله ی تخمین زده شده بر هم می زنند.

مقایسه طرح های بالا در جدول IV نشان داده شده است.(مقایسه روش های فیلترینگ)

به منظور کاهش نیاز به زمان دقیق نانو ثانیه و سخت افزار پیشرفته , ساستری و همکارانش پروتکل Echo را پیشنهاد می دهند به منظور آنکه بررسی کنند آیا یک اثبات کننده p واقعا درون یک منطقه خاص است یا نه. در Echo بازبین V یک نانس را با استفاده از RF به P می فرستد و زمان سنج شروع به کار می کند , سپس اثبات کننده p فورا با استفاده از فراصوت , نانس را منعکس می کند.V می تواند از زمان تلف شده برای محاسبه فاصله بین آن ها استفاده کند.از آنجا که سیگنال فراصوت آهسته تر از RF منتقل می شود, در مقایسه با پروتکل محدوده فاصله, اکو نیاز مطلق به ساعت یا زمان دقیق و توانایی فوری پروسه ندارد.با این وجود بدون هر نوع اثبات یا تاییدی, این امکان برای حمله کننده در جهت گرفتن پاسخ درست اثبات کننده و اتصال هویت خود, فراهم می شود.

در [64] میدوز و همکارانش یک پروتکل جدید را برای محدوده فاصله پیشنهاد کرده اند, در این پروتکل نیاز به پیام و نوشته های رمزی کمتری نسبت به پروتکل مشابه در [33] است. در ابتدا تحلیل تمام عیارو رسمی یک پروتکل محدوده فاصله به منظور کاهش پیام و پیچیدگی نوشته رمزی بدون تحلیل امنیت ارائه می شود.سپس حمله

تبانی مورد مخاطب قرار می گیرد.این نشان می دهد که پروتکل های متداول تعیین فاصله برای حملات تبانی کافی نیستند.

در [65] ورا و همکارانش یک پروتکل جدید تایید اطلاعات محل را بر اساس ماهیت انتشار ارتباط رادیویی پیشنهاد می کنند.دو نوع بازبین وجود دارد: یک پذیرنده و یک رد کننده. بر طبق توانایی بازبین در تعیین محل اثبات کننده , این شبکه به 3 ناحیه تقسیم می شود: ناحیه پذیرش, ناحیه ابهام و ناحیه عدم پذیرش. ناحیه خاص حفاظت امن است اگر هر نقطه خارج از ناحیه ی حفاظت در ناحیه عدم پذیرش نیز باشد.پذیرندگاه و رد کنندگان به ترتیب در داخل و مرز منطقه حفاظت شده مستقر می شوند. پروسه تایید , مخصوص اثبات کننده است , در این کار اثبات کننده قدرت سیگنال خود را افزایش می دهد و یک سیگنال را منتشر می کند تا زمانیکه بازبین متوجه سیگنال شود و به آن پاسخ دهد. تایید کنندگان(بازبین ها) اثبات کننده را می پذیرد اگرچه هیچکدام از رد کنندگان متوجه اثبات کننده در طی این پروسه نشوند.

در [66] وانگ و همکارانش یک الگوریتم را به منظور کشف گره های فانتوم ارائه می کنند, گره های فانتوم بیشترین و بزرگترین زیر مجموعه ی سازگار هستند که شامل تمام گره های نرمال می باشند.این الگوریتم به دو مرحله مهم تقسیم می شود: مرحله اندازه گیری فاصله و مرحله فیلترینگ. در مرحله اول هر گره فواصل را تا همسایگان خود اندازه گیری می کند. در مرحله دوم هر گره در ابتدا به طور تصادفی دو همسایه را به منظور ایجاد نقشه محلی انتخاب می کند.پروسه های بالا برای زمان های داده شده تکرار می شوند و این بزرگترین زیر مجموعه در تمام مراحل انتخاب می شود, این زیر مجموعه شامل تمام گره های نرمال است. در این روش تمام گره ها نقش بازبین ها را ایفا می کنند. حتی اگر تعداد گره های فانتوم بزرگتر از تعداد گره های صادق باشند , ما می توانیم هنوز بیشتر گره های فانتوم را فیلتر کنیم.

در [67] وی و همکارانش دو الگوریتم تایید محل را با نام فیلترینگ حریصانه بوسیله ماتریس(GFM) و شاخص قابلیت اطمینان (TI) پیشنهاد می کنند.در الگوریتم GFM مرکز تایید (VC) چندین ماتریس مانند ماتریس مشاهده , ماتریس تفاوت و ماتریس وزن را بر اساس موقعیت های تخمین زده شده ی گره های نا معلوم و مشاهدات همسایگی آن ها محاسبه می کند.از این رو ماتریس ها به منظور شناسایی و باطل کردن اطلاعات ناسازگار و مغایر با محل, استفاده می شود.در الگوریتم TI مرکز تایید(VC) شاخص های قابلیت اعتماد را برای بر گره نا معلوم محاسبه می کند و آن هایی را می پذیرد که شاخص های نهایی آنها, بیشتر ار حد آستانه باشند.

در [68] دلات و همکارانش اولین پروتکل توزیع شده قطعی را با نام findmap برای شناسایی دقیق گره های سنسور جعلی بر اساس تکنیک تعیین مسافت پیشنهاد می دهند.نشان داده شده است زمانیکه RSSI به کار می رود, findmap حداکثر گره های سنسور جعلی [n/2]-2 را کنترل می کند.زمانی که از تکنیک زمان پرواز(TOF) استفاده می شود, findmap حداکثر گره های مخرب سنسور [n/2]-3 را مدیریت می کند.با این وجود اثبات می شود که اگر عدد سنسورها [n/2]-1 باشد هیچ پروتکل قطعی نمی تواند سنسورهای جعلی را شناسایی کند.

در [69] لی و همکارانش بر مسئله ی تایید منطقه متمرکز هستند و یک الگوریتم تایید محل امن را پیشنهاد می دهند.در ابتدا یک مشتری(هر گره ای که نیاز به تایید داشته باشد) یک نانس تصادفی چالش را منتشر می کند.گره های انکر دریافت کننده این نانس, قدرت سیگنال را بر اساس مدل افت سیگنال محاسبه می کنند. سپس قدرت سیگنال , id مشتری و اطلاعات مربوط به محل گره های انکر به ایستگاه فرستاده می شوند.

در پایان ایستگاه الگوریتمی با نام Vesec را به منظور تایید اعتبار قدرت سیگنال اجرا می کند.اگر قدرت سیگنال یک گره با قدرت سیگنال گره های دیگر در منطقه مغایر باشد آن گره به عنوان گره دشمن در نظر گرفته می شود.

مقایسه طرح های بالا در جدول V نشان داده شده است.(مقایسه متدهای تایید)

4- راه حل پیشنهادی

4-1- هدف

روشی که بتواند از اطلاعات خود نود استفاده کند.توان عملیاتی را بالا ببرد.از سخت افزار کمتری استفاده گردد.قابلیت توسعه شبکه بالا رود.ترکیبی از روشهای دیگر باشد.استفاده از نودهای مرجع یا انکر یا راهنما هزینه برو دشوار است. زیرا قرار دادن دستی آن ها در محیط توسط انسان یا رباط در محیطهایی مثل جنگ دشوار است.هدف اصلی کاهش هزینه است.

4-2- شرح روش

از ایستگاه های اصلی شروع می کنیم و به صورت گام به گام یک پیام را که مبتنی بر مکانیابی به نودهای دیگر است را توسط آن ارسال می کنیم

در این حالت نودهای دیگر در زمان خیلی کوتاه آنتن های هوشمند خود را روشن می کنند

با این پیام با تشخیص قدرت و جهت سیگنال مبدا می توانند مکان خود را نسبت به آن ایستگاه مشخص کنند. و دوباره هر نود بعد از دریافت پیام مکان یابی وپیدا کردن مکان فیزیکی خود ,پیغام مکان یابی را برای بقیه می فرستد تا الی آخر..

نکته مهم این است که اطلاعات نودها و پیام ها به صورت رمزی پیاده شده است.

در این صورت شبکه ما از بسیاری حملات در امان است.

5- نتیجه گیری

در این مقاله رسیدن به محلی سازی ایمن مورد توجه قرار گرفت.حملات شناخته شده را بر روی سیستم های محلی سازی و طرح های پیشنهاد شده محلی سازی ایمن طبقه بندی و شرح دادیم.

اهداف بعدی در باره الگوریتم های محلی سازی ایمن عبارتند از:

1)ساخت مدل های حمله مخرب و واقع تر بر ضد محلی سازی ایمن

2)بهبود طرح های امنیت به منظور افزایش سرعت کشف نابهنجاری بدون ساعت های نانو ثانیه, اطلاعات استقرار و هر سخت افزار اضافی

3)تحقیق درباره شناسایی و تعیین مناطق جدید یا پیشنهادات تایید به منظور کاهش زمان محلی سازی و مصرف انرژی

4)ارزیابی عملکرد الگوریتم های محلی سازی ایمن با یکسری استانداردها 5)کاربرد فن آوری حوزه های دیگر تحقیقات مثل شبکه perti 6)گسترش و توسعه چالش های جدید در WSN خاص مثل شبکه های سنسور چند رسانه ای و متحرک.

6- مراجع

[1] B. Karp and H. T. Kung, “GPSR: Greedy Perimeter Stateless Routing for wireless networks,” in Proceedings of the 6th Annual International Conference on Mobile Computing and Network, 2000, pp. 243–354.

[2] D. Liu and P. Ning, “Location-based pairwise key establishments for static sensor networks,” in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003, pp. 72–82.

[3] S. U. Sastry, N. and D. Wagner, “Secure verification of location claims,” in Proceedings of the 2nd ACM workshop on Wireless security, September 2003.

[4] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor networks: a survey,” Computer Networks, vol. 52, no. 12, pp. 2292–2330, August 2008.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks, vol. 38, no. 4, pp. 393–422, March 2002.

[6] Y. Zeng, J. Cao, J. Hong, and L. Xie, “Secure localization and location verification in wireless sensor networks,” in IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, October 2009, pp. 864–869.

[7] S. Zhu and Z. Ding, “A simple approach of range-based positioning with low computational complexity,” IEEE Transactions on Wireless Communications, vol. 8, no. 12, December 2009.

[8] M. Heidari, N. Alsindi, and K. Pahlavan, “Udp identification and error mitigation in toa-based indoor localization systems using neural network architecture,” IEEE Transactions on Wireless Communications, vol. 8, no. 7, July 2009.

[9] S. Lee, E. Kim, C. Kim, and K. Kim, “Localization with a mobile beacon based on geometric constraints in wireless sensor networks,” IEEE Transactions on Wireless Communications, vol. 8, no. 7, pp. 5801–5805, December 2009.

[10] H. Chen, Q. Shi, H. Vincent Poor, and K. Sezaki, “Mobile element assisted cooperative localization for wireless sensor networks with obstacles,” IEEE Transactions on Wireless Communications, vol. 9, no. 3, March 2010.

[11] P. Bahl and V. Padmanabhan, “RADAR: An In-Building RF-Based User Location and Tracking System,” in Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 21, 2000, pp. 755–784.

[12] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, “The anatomy of a context-aware application,” in Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, 1999, pp. 59–68.

[13] L. Girod and D. Estrin, “Robust range estimation using acoustic and multimodal sensing,” in Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems, 2001, pp. 1312–1320.

[14] D. Niculescu and B. Nath, “Ad hoc positioning system (APS) using AoA,” in Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, April 2003, pp. 1734–1743.

[15] ——, “Ad hoc positioning system (APS),” in Proceedings of the 2001 IEEE Global Telecommunications Conference of the IEEE Communications Society, vol. 5, 2001, pp. 2926–2931.

[16] L. Doherty, K. Pister, and L. Ghaoui, “Convex position estimation in wireless sensor networks,” in Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, 2001, pp. 1655–1663.

[17] Y. Shang, W. Ruml, Y. Zhang, and M. Fromherz, “Localization from mere connectivity,” in Proceedings of the 4th International ACM Symposium on Mobile Ad Hoc Networking & Computing, 2003, pp. 201–212.

[18] A. Ferreres, B. Alvarez, and A. Garnacho, “Guaranteeing the authenticity of location information,” IEEE Pervasive

April 2008.
[29] P. Yi, Z. Dai, Z. Y., and S. Zhang, "Resisting flooding
attacks in ad hoc networks," in Proceedings of the International
Conference on Information Technology: Coding
and Computing, no. 2, April 2005, pp. 657–662.
[30] L. Bysani and A. Turuk, "A survey on selective forwarding
attack in wireless sensor networks," in Proceedings of the
International Conference on Devices and Communications
(ICDeCom), February 2011, pp. 1–5.
[31] S. Capkun and J. Hubaux, "Secure positioning of wireless
devices with application to sensor networks," in Proceedings
of the 24th Annual Joint Conference of the IEEE
Computer and Communications Societies, no. 3, 2005, pp.
1917–1928.
[32] S. Capkun, K. Rasmussen, M. Cagalj, and M. Srivastava,
"Secure location verification with hidden and mobile base
stations," in IEEE Transactions on Mobile Computing,
vol. 7, no. 4, 2008, pp. 470–483.
[33] S. Brands and D. Chaum, "Distance-bounding protocols,"
in Proceedings of the the EUROCRYPT 93 Workshop on
the Theory and Application of Cryptographic Techniques
on Advances in Cryptology, 1994, pp. 344–359.
[34] S. Capkun and J. Hubaux, "Secure positioning in wireless
network," in IEEE Journal on Selected Areas in Communications,
vol. 24, no. 2, 2006, pp. 221–232.
[35] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization
with hidden and mobile base stations," in Proceedings
of the 25th IEEE International Conference on Computer
Communications, 2006, pp. 1–10.
[36] F. Anjum, S. Pandey, and P. Agrawal, "Secure localization
in sensor networks using transmission range variation," in
Proceedings of the 2nd IEEE International Conference on
Mobile Adhoc and Sensor Systems Conference, November
2005, pp. 203–211.
[37] S. Ganu, A. Krishnakumar, and P. Krishnan,
"Infrastructure-based location estimation in wlan
networks," in IEEE Wireless Communications and
Networking Conference, March 2004, pp. 465–470.
[38] Y. Zhang,W. Liu, Y. Fang, and D.Wu, "Secure localization
and authentication in ultra-wideband sensor networks,"
in IEEE Journal on Selected Areas in Communication,
vol. 24, no. 4, 2006, pp. 829–835.
[39] D. He, L. Cui, and H. Huang, "Design and verification
of enhanced secure localization scheme in wireless sensor
Computing, vol. 7, no. 3, pp. 72–80, July 2008.
[19] A. Savvides, C.-C. Han, and M. Srivastava, "Dynamic
fine-grained localization in ad-hoc networks of sensors,"
in Proceedings of the 7th annual international conference
on Mobile computing and networking, 2001, pp. 166–
179.
[20] X. Chen, Defense Against Node Compromise in Sensor
Network Security. FIU Electronic Theses and Dissertations,
http://digitalcommons.fiu.edu/etd/7, 2007.
[21] C. Yu, C. Lu, and S. Kuo, "Efficient and distributed detection
of node replication attacks in mobile sensor networks,"
in Proceedings of Vehicular Technology Conference Fall
(VTC Fall), September 2009, pp. 1–5.
[22] K. Xing, F. Liu, C. Cheng, and D. Du, "Real-time detection
of clone attacks in wireless sensor networks," in Proceedings
of the 28th International Conference on Distributed
Computing Systems, June 2008, pp. 3–10.
[23] K. Glynos, P. Kotzanikolaou, and C. Douligeris, "Preventing
impersonation attacks in manet with multi-factor
authentication," in Proceedings of the Third International
Symposium on Modeling and Optimization in Mobile, Ad
Hoc, and Wireless Networks, April 2005, pp. 59–64.
[24] J. Newsome, E. Shi, D. Song, and A. Perrig, "The
sybil attack in sensor networks: Analysis & defenses,"
in Proceedings of the Third International Symposium on
Information Processing in Sensor Networks, April 2004,
pp. 259–268.
[25] M. Jain and H. Kandwal, "A survey on complex wormhole
attack in wireless ad hoc networks," in Proceedings of the
2009 International Conference on Advances in Computing,
Control, and Telecommunication Technologies, December
2009, pp. 555–558.
[26] A. Quazi, "An overview on the time delay estimate in
active and passive systems for target localization," IEEE
Transactions on Acoustics Speech and Signal Processing,
vol. 29, no. 3, pp. 527–533, June 1981.
[27] J. Jiang, G. Han, S. L., H. Chao, and S. Nishio, "A novel
secure localization scheme against collaborative collusion
in wireless sensor networks," in the 7th International Wireless
Communications & Mobile Computing Conference,
July 2011.
[28] X. Cao, B. Yu, G. Chen, and F. Ren, "Security analysis
on node localization systems of wireless sensor networks,"
China Journal Of Software, vol. 19, no. 4, pp. 879–887,

[51] J. Wu, H. Chen, W. Lou, Z. Wang, and Z. Wang, "Labelbased
dv-hop localization againstwormhole attacks in wireless
sensor networks," in Proceedings of the 5th IEEE
International Conference on Networking, Architecture, and
Storage, September 2010, pp. 79–88.
[52] N. Labraoui and M. Gueroui, "Secure range-free localization
scheme in wireless sensor networks," in Proceedings
of the 10th International Symposium on Programming and
Systems (ISPS), April 2011, pp. 1–8.
[53] W. Du, L. Fang, and P. Ning, "LAD: Localization anomaly
detection forwireless sensor networks," in The Journal of
Parallel and Distributed Computing, vol. 66, no. 7, 2006,
pp. 874–886.
[54] D. Liu, P. Ning, and W. Du, "Detecting malicious beacon
nodes for secure location discovery in wireless sensor
networks," in Proceedings of the 25th IEEE International
Conference on Distributed Computing Systems, 2005, pp.
609–691.

[55] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed
reputation-based beacon trust system," in Proceedings
of the 2nd IEEE International Symposium on
Dependable, Autonomic and Secure Computing, 2006, pp.
277–283.
[56] A. Srinivasan, J. Wu, and J. Teitelbaum, "Distributed
reputation-based secure localization in sensor networks,"
in Journal of Autonomic and Trusted Computing, 2007.
[57] X. Wang, L. Qian, and H. Jiang, "Tolerant majoritycolluding
attacks for secure localization in wireless sensor
networks," in Proceedings of 5th International Conference
on Wireless Communications, Networking and Mobile
Computing, 2009, pp. 1–5.
[58] Z. Li, W. Trappe, and B. Nath, "Robust statistical methods
for securing wireless localization in sensor networks,"
in Proceedings of the 4th International Symposium on
Information Processing in Sensor Networks (IPSN), 2005,
pp. 91–98.
[59] D. Liu, P. Ning, and W. Du, "Attack-resistant location
estimation in sensor networks," in Proceedings of the 4th
International Symposium on Information Processing in
Sensor Networks (IPSN), April 2005, pp. 99–106.
[60] D. Liu, P. Ning, A. Liu, W. Wang, and W. Du, "Attackresistant
location estimation in sensor networks," in ACM
Transactions on Information and System Security (TISSEC),
networks," in IEEE transactions on Parallel and Distributed
Systems, vol. 20, no. 7, July 2009.
[40] S. Arisar and A. Kemp, "Secure location estimation in
large scale wireless sensor networks," in Proceedings of the
3rd International Conference on Next Generation Mobile
Applications, Services and Technologies, 2009, pp. 472–
476.
[41] J. Alfaro, M. Barbeau, and E. Kranakis, "Secure localization
of nodes in wireless sensor networks with limited
number of truth tellers," in Proceedings of the 7th Annual
Communications Networks and Services Research Conference,
2009, pp. 86–93.
[42] ——, "Secure geolocalization of wireless sensor nodes in
the presence of misbehaving anchor nodes," in Annals of
Telecommunications, November 2010, pp. 1–18.
[43] L. Lazos and R. Poovendran, "SeRLoc: Secure rangeindependent
localization for wireless sensor networks,"
in Proceedings of the 3rd ACM Workshop on Wireless
Security, 2004, pp. 21–30.
[44] ——, "ROPE: robust position estimation in wireless sensor
networks," in Proceedings of the 4th International Symposium
on Information Processing in Sensor Networks, April
2005, pp. 324–331.
[45] ——, "HiRLoc: High-resolution robust localization for
wireless sensor networks," in IEEE Journal on Selected
Areas in Communications, vol. 24, no. 2, 2006, pp. 233–
246.
[46] Y. Zeng, S. Zhang, S. Guo, and L. Xie, "Secure hop-count
based localization in wireless sensor networks," in 2007
International Conference on Computational Intelligence
and Security, December 2007, pp. 907–911.
[47] A. Perrig, R. Canetti, D. Tygar, and D. Song, "Efficient
authentication and signature of multicast streams over
lossy channels," in Proceedings of Oakland, May 2000,
pp. 56–73.
[48] P. Rousseeuw and A. Leroy, "Robust regression and outlier
detection," in WileyInterscience, 2003.
[49] E. Ekici, J. Mcnair, and D. Al-Abri, "A probabilistic
approach to location verification in wireless sensor networks,"
in IEEE International Conference on Communications,
vol. 8, June 2006, pp. 3485–3490.
[50] E. Ekici, S. Vural, J. Mcnair, and D. Al-Abri, "Secure
probabilistic location verification in randomly deployed
wireless sensor networks," in Ad Hoc Networks, vol. 6,
no. 2, 2008, pp. 195–209.

vol. 11, no. 4, 2005, pp. 1–39.
[61] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, "Towards a theory of robust localization against malicious beacon nodes," in Proceedings of the 27th IEEE International Conference on Computer Communication, 2008, pp. 1391–1399.
[62] Y. Zeng, J. Cao, Z. S., S. Guo, and L. Xie, "Pollution attack: A new attack against localization in wireless sensor networks," in Proceedings of Wireless Communications and Networking Conference, April 2009, pp. 2038–2043.
[63] S. Misra, G. Xue, and S. Bhardwaj, "Secure and robust localization in a wireless ad hoc environment," in IEEE Transactions on Vehicular Technology, vol. 58, no. 3, 2009, pp. 1480–1489.
[64] C. Meadows, R. Poovendran, D. Pavlovic, L. Chang, and P. Syverson, "Distance bounding protocols: Authentication logic analysis and collusion attacks," in Secure Localization and Time Synchronization in Wireless Ad Hoc and Sensor Networks, 2007, pp. 279–298.
[65] A. Vora and M. Nesterenko, "Secure location verification using radio broadcast," in IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, December 2006, pp. 377–385.
[66] J. Hwang, T. He, and Y. Kim, "Detecting phantom nodes in wireless sensor networks," in Proceedings of the 26th IEEE International Conference on Computer Communications, May 2007, pp. 2391 – 2395.
[67] Y. Wei, Z. Yu, and Y. Guan, "Location verification algorithms for wireless sensor networks," in Proceedings of the 27th International Conference on Distributed Computing Systems, June 2007, p. 70.
[68] S. Delaet, P. Mandal, M. Rokicki, and T. S., "Deterministic secure positioning in wireless sensor networks," in IEEE International Conference on Distributed Computing in Sensor Networks (DCOSS), June 2008, pp. 469–477.
[69] C. Li, F. Chen, Y. Zhan, and L. Wang, "Security verification of location estimate in wireless sensor networks," in Proceedings of the 2010 6th International Conference on Wireless Communications Networking and Mobile Computing