فصل دوم

امنیت در شبکه موردی

۲-۱-مقدمه

شبکه‌های موردی Ad Hocدر بسیاری از برنامه‌های کاربردی در ارتش، محیط زیست و نواحی مرتبط با سلامت ، پژوهش و تحقیقات مورد استفاده قرار می گیرند. این کاربردها معمولاً شامل نظارت و بررسی اطلاعات حساس از قبیل جابجایی دشمن در میدان جنگ یا موقعیت و دیده بانی نواحی حساس و نظامی می باشد . از این رو امنیت و صحت اطلاعات دریافتی بدلیل موقعیت حساس شبکه های موردی Ad Hoc بسیار مهم است. با توجه به ماهیت شبکه های موردی Ad Hoc، اینگونه شبکه ها از محدودیتهای بسیاری رنج می برند . از جمله فضای دخیره سازی اندک، منابع انرژی محدود و استفاده از کانال های ارتباطاتی ناامن بی سیم . این محدودیت ها امنیت را در شبکه های موردی Ad Hoc به چالش می کشند . سعی ما بر این است تا مشکلات و راهکار های مطرح را در این شبکه ها مشخص و دسته بندی نمائیم.

۲-۲-معرفی شبکه های متحرک بی سیم اقتضایی

شبکه های *Ad-hoc* به شبکه های آنی و یا موقت گفته می شود که برای یک منظور خاص به وجود می آیند . در واقع شبکه های بی سیم هستند که گره های آن متحرک می باشند. تفاوت عمده شبکه های *Ad-hoc* با شبکه های معمول بی سیم ۸۰۲.۱۱ در این است که در شبکه های *Ad-hoc* مجموعه ای از گره های متحرک بی سیم بدون هیچ زیرساختار مرکزی، نقطه دسترسی و یا ایستگاه پایه برای ارسال اطلاعات بی سیم در بازه ای مشخص به یکدیگر وصل می شوند.

ارسال بسته های اطلاعاتی در شبکه های بی سیم *Ad-hoc* توسط گره های مسیری که قبلا توسط یکی از الگوریتمهای مسیریابی مشخص شده است، صورت می گیرد. نکته قابل توجه این است که هر گره تنها با گره هایی در ارتباط است که در شعاع رادیویی اش هستند، که اصطلاحا گره های همسایه نامیده می شوند.

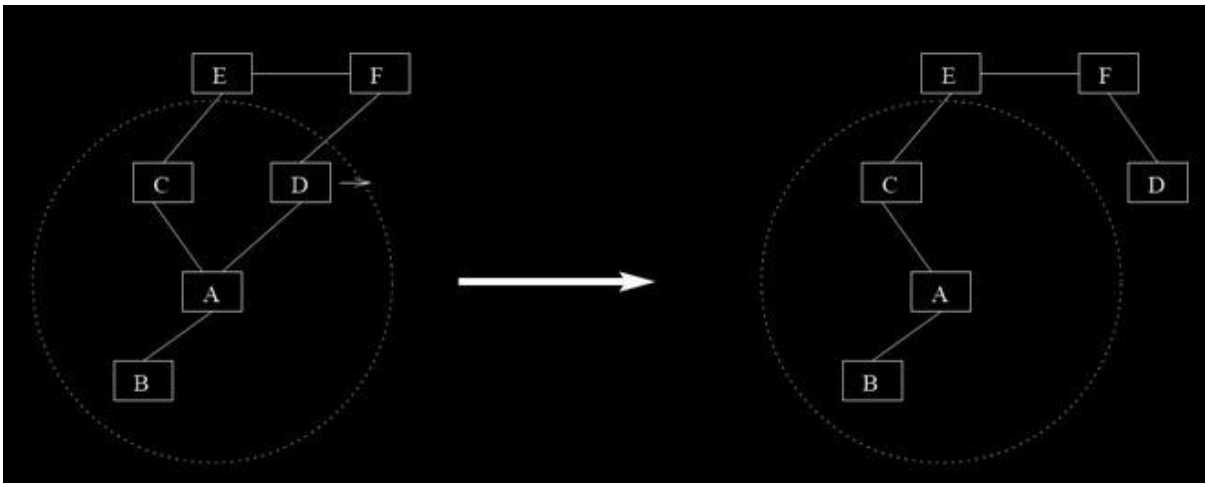
پروتکلهای مسیریابی بر اساس پارامترهای کانال مانند تضعیف، انتشار چند مسیره، تداخل و همچنین بسته به کاربرد شبکه به صورت بهینه طراحی شده اند. در هنگام طراحی این پروتکلها به امر تضمین امنیت در شبکه های *Ad-hoc* توجه نشد . در سالهای اخیر با توجه به کاربردهای حساس این شبکه ا ز جمله در عملیاتهای نظامی، فوریتهای پزشکی و یا مجامع و

کنفرانسها، که نیاز به تامین امنیت در این شبکه ها بارزتر شده است، محققان برای تامین امنیت در دو حیطه عملکرد و اعتبار پیشنهادات گوناگونی را مطرح کردند و می کنند.

شبکه های بی سیم *Ad-hoc* فاقد هسته مرکزی برای کنترل ارسال و دریافت داده می باشد و حمل بسته های اطلاعاتی به شخصه توسط خود گره های یک مسیر مشخص و اختصاصی صورت می گیرد. توپولوژی شبکه های *Ad-hoc* متغیر است زیرا گره های شبکه می توانند تحرک داشته باشند و در هر لحظه از زمان جای خود را تغییر بدهند.

وقتی گره ای تصمیم می گیرد که داده ای را برای گره مورد نظر خود بفرستد. ابتدا با انجام یک پروتکل مسیریابی پخش شونده کوتاهترین مسیر ممکن به گره مورد نظر را بدست می آورد و سپس با توجه به این مسیر داده را ارسال میکند . به هنگام به روز رسانی یا کشف مسیر مورد نظر تمام گره های واقع بر روی مسیر اطلاعات مربوط به راه رسیدن به گره مقصد را در جدول مسیریابی خود تنظیم می کنند، تا در هنگام ارسال داده از مبدا روند اجرای عملیات ارسال داده به درستی از طریق کوتاهترین مسیر ممکن انجام شود.

در شکل ۲-۱نمایی از یک شبکه متحرک بی سیم *Ad-hoc* را مشاهده می کنید که در آن گره D شروع به حرکت به سمت راست می کند و در نهایت همانطور که در سمت راست شکل مشخص شده است، از دید رادیویی گره A خارج می شود.



شکل ۲-۱ نمایی از توپولوژی در حال تغییر یک شبکه Ad-hoc

۲-۳-امنیت، شرط لازم

- عدم وجود اعتماد کامل به گره های شبکه برای انجام اعمال شبکه
- وابستگی شدید عملکرد شبکه به رفتار گره ها
- محدودیت توان محاسباتی و توان مخابراتی
- امنیت شرط لازم برای انجام صحیح اعمال شبکه
  - انجام صحیح و امن اعمال توسط گره های شرکت کننده در عملیات
  - تسهیم منصفانه اعمال بین گره ها

۲-۴-امنیت در شبکه‌های بی سیم

این شبکه‌ها به شدت در مقابل حملات آسیب پذیرند و امروزه مقاومت کردن در برابر حملات از چالش‌های توسعه این شبکه هاست. دلایل اصلی این مشکلات عبارتند از :

- کانال رادیویی اشتراکی انتقال داده
- محیط عملیاتی ناامن
- قدرت مرکزی ناکافی
- منابع محدود
- آسیب پذیر بودن از لحاظ فیزیکی
- کافی نبودن ارتباط نودهای میانی.

۲–۵–منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول

ساختار این شبکه‌ها مبتنی بر استفاده از سیگنال های رادیویی به جای سیم و کابل، استوار است . با استفاده از این سیگنال ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرتمند این شبکه‌ها، خود را به عنوان عضوی از این شبکه‌ها جازده و در صورت تحقق این امر، امکان دست یابی به اطلاعات حیاتی، حمله به سرویس‌دهنده‌گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد. در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است :

- نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌ای دست یابند.
- حمله‌های DOS به تجهیزات و سیستم‌های بی سیم بسیار متداول است.
- کامپیوترهای قابل حمل و جیبی، که امکان استفاده از شبکه ی بی سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می توان اولین قدم برای نفوذ به شبکه را برداشت.
- یک نفوذگرمی تواند از نقاط مشترک میان یک شبکه ی بی‌سیم در یک سازمان و شبکه ی سیمی آن (که در اغلب موارد شبکه ی اصلی و حساس‌تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکه ی بی‌سیم عملاً راهی برای دست یابی به منابع شبکه سیمی نیز بیابد.

۲-۶-سه روش امنیتی در شبکه‌ای بی سیم

۲-۶-۱-*WEP*

در این روش از شنود کاربرهایی که در شبکه مجوز ندارند جلوگیری به عمل می آید که مناسب برای شبکه‌های کوچک بوده زیرا نیاز به تنظیمات دستی مربوطه در هر سرویس گیرنده می‌باشد. اساس رمز نگاری *WEP* بر مبنای الگوریتم *RC۴* بوسیله *RSA* می‌باشد.

۲-۶-۲-SSID

شبکه‌های *WLAN* دارای چندین شبکه محلی می‌باشند که هر کدام آنها دارای یک شناسه یکتا می‌باشند این شناسه‌ها در چندین نقطه دسترسی قرار داده می‌شوند. هر کاربر برای دسترسی به شبکه مورد نظر بایستی تنظیمات شناسه *SSID* مربوطه را انجام دهد.

۲-۶-۳-MAC

لیستی از *MAC* آدرس‌های مورد استفاده در یک شبکه به نقطه دسترسی مربوطه وارد شده بنابراین تنها کامپیوترهای دارای این *MAC* آدرس‌ها اجازه دسترسی دارند به عبارتی وقتی یک کامپیوتر درخواستی را ارسال می کند *MAC* آدرس آن با لیست *MAC* آدرس مربوطه در نقطه دسترسی مقایسه شده و اجازه دسترسی یا عدم دسترسی آن مورد بررسی قرار می گیرد. این روش امنیتی مناسب برای شبکه‌های کوچک بوده زیرا در شبکه‌های بزرگ امکان ورود این آدرس‌ها به نقطه دسترسی بسیار مشکل می‌باشد. در کل می‌توان به کاستن از شعاع تحت پوشش سیگنال‌های شبکه کم کرد و اطلاعات را رمزنگاری کرد.

۲-۷-کنترل دسترسی

کنترل دسترسی شامل ابزارهایی است برای کنترل کردن مسیر کاربران یا کاربران مجازی، مانند فرآیندهای سیستم عامل (موضوعات)که بتوانند به داده(اشیاء)دسترسی داشته باشند. تنها گره های مجاز می توانند به گروه ها ملحق شوند، آنها را ترک کنند، خراب کنند یا به آنها شکل دهند. همچنین کنترل دسترسی به معنی راه داخل شدن گره ها به سیستم شبکه بندی است تا برای اولین بار که وارد شبکه می شوند قادر به برقراری ارتباط با دیگر گره ها باشند. اینها خط مشی های مختلف کنترل دسترسی هستند:

کنترل دسترسی احتیاطی *(DAC)* ابزاری را برای تعیین کنترل دسترسی کابران برای خود آنها ارائه می کند (مانند ابزاری که برای محدود کردن دسترسی به بخشهای مختلف اینترنت وجود دارد.

کنترل دسترسی اجباری *(MAC)* شامل مکانیزم های متمرکزی است که برای کنترل دسترسی اشیاء با یک سیاست اجازه دادن قراردادی، اجرا می شود.

کنترل دسترسی مبتنی بر نقش *(RBAC)* مفهومی از نقش را در میان موضوعات و اشیاء ایجاد می کند.

۲-۸-امنیت در شبکه های*ad hoc*

در رفتارهای امنیتی که یک شبکه*adhoc* با آن مواجه است توصیف می کنیم الگوی گرفته شده فرمت پیام ها را توضیح می دهد، به علاوه پروتکل هایی که تصدیق هویت را فراهم می کنند .معماری می تواند از الگوهای مختلف تصدیق هویت استفاده کنند .سرویس مدیریت کلیدی ما یک پیش نیاز برای چنین معماری های امنیتی است.

۲-۹-کمبود ایمنی در شبکه های*Adhoc* :

ساختار شبکه*Adhoc* طوری مجسم می شود که در آن جا پشتیبانی دستیابی بی سیم یا پشتیبان سیم دار , میسر نیست – شبکه تک کاره , هیچ پایه و اساس از پیش تعریف شده ندارد و تمام خدمات شبکه ای در موقع اجرا پیکر بندی می شوند و به وجود می آیند . از این رو بدیهی است که با فقدان پشتیبانی زیر بنایی و حملات لینک بی سیم آسیب پذیر ,

ایمنی در شبکه*Adhoc* , نقطه ضعف ذاتی است . دستیابی به ایمنی در داخل شبکه سازی*Adhoc* بنا به دلایل ذیل مشکل آفرین است:

۲-۹-۱-توپولوژی دنیامیکی و عضویت:

-توپولوژی شبکه ای*Adhoc* خیلی دنیامیک است به طوریکه متحرک بودن گروهها یا عضویت گره ها خیلی تصادفی و سریع است این امر به دینامیکی بودن نیاز برای راه حل های ایمن تاکید می کند.

۲-۹-۲-لینک بی سیم آسیب پذیر:

حملات لینک فعال / غیر فعال نظیر استراق سمع , کلک زدن , انکار خدمات رسانی , تقلید و جعل هویت امکان پذیر هستند.

۲-۹-۳-پر سه زدن در محیط خطرناک:

هر گونه بدرفتاری بدخواهی می تواند سبب ایجاد حملات خصمانه شود یا تمام گروهها را از فراهم نمودن خدمات محروم کند.

گره های موجود در محیط متحرک با دستیابی به لینک رادیویی مشترک در تنظیم*Adhoc infrastructu* به آسانی مشارکت می کنند . اما ارتباطات ایمن در میان گره ها مستلزم ایجاد ارتباط در لینک ارتباطات ایمن است . قبل از تعیین لینک ارتباطات ایمن , گره باید بتواند گره دیگر را شناسایی کند . در نتیجه گره , گره هویت خود و نیز مدارک مربوطه به گره دیگر را فراهم می سازد.

اما مدارک و احراز هویت ارائه شده باید مورد تایید و حفاظت قرار گیرند به طوری که اصالت یکپارچگی مدارک و هویت ارائه شده را نمی توان طبق گره گیرنده مورد سوال قرار داد هر گره می خواهد مطمئن شود که مدارک و هویت ارائه شده به گروههای دریافت کننده تطبیق داده نمی شود . از این رو لازم است ساختار ایمن برای شبکه ای سازی تک کاره و ایمن فراهم شود . مساله هویت فوق الذکر فورا به مساله خصوصی سازی منجر می شود به طور کلی گره سیار از انواع هویت ها استفاده می کند و آن از سطح لینک تا سطح کاربر / کاربر تغییر می کند همچنین در محیط سیار بصورت مکرر گره سیار آماده نیست تا مدارک یا هویتش را به گره سیار دیگر از نقطه نظر خصوصی سازی آشکار سازد هر گونه هویت سازگار شده باعث می شود که حمله کننده ها تهدید و خصوصی سازی برای دستگاه کاربر ایجاد کند متاسفانه استانداردهای سیار جاری هیچ گونه خصوصی سازی ممکن فراهم نمی کند و در بسیاری از موارد آشکار ساختن هویت برای تولید لینک ارتباطات اجتناب ناپذیر است از این رو حفاظت خصوصی سازی بی درز برای مهار کردن کاربرد شبکه ای سازی تک کاره مورد نیاز است.

۲–۱۰–مسائل و چالشهای اصلی

۲–۱۰–۱–ایمنی سطح لینک

در محیط بی سیم لینک ها نسبت به حملاتی که استراق سمع کننده به آسانی می تواند ارتباطات پیوسته را دست اندازد آسیب پذیر هستند چون هیچ حفاظتی نظیر فایروال ها یا کنترل دستیابی از شبکه *Adhoc* وجود ندارد هر گره نسبت به حملاتی که از هر جهت یا هر گروه به دست می آیند آسیب پذیر می باشد نتایج این حملات شامل دست اندازی هویت گره , دستکاری کردن مدارک گره , آشکار ساختن اطلاعات محرمانه یا جعل هویت گره است این نوع حملات به آسانی می توانند با جنبه های اصلی ایمنی نظیر خصوصی بودن , یکپارچگی , دسترس پذیری و محرمانگی گره سازگار شوند.

۲–۱۰–۲–اهداف ایمنی در شبکه های*Adhoc* از طریق مکانیسم های رمز نگاری

رمز نگاری کلید مهری یا امضاء دیجیتالی به دست می آیند این مکانیسم ها از طریق مدیریت کلید متمرکز را پشتیبانی می شوند . که در این جا مسئول گواهی نامه کلید عمومی را برای گره های سیار فراهم می کند بنابراین گره ها می توانند اعتماد دو طرفه بین یکدیگر ایجاد کنند هرگونه دستکاری*CA* می تواند ایمنی کل شبکه را به آسانی سازگار سازد .

مکانیسم های پیشنهادی به کار رفته برای هویت نظیر راز مشترک , رمز نگاری کلید عمومی , تاییدیه طرف سوم راه حل های جزئی فراهم می کنند . به طوری که آنها حساس هستند یا قادر نیستند مقیاس بندی کنند . تمام راه حل های پیشنهادی مستلزم آن است که کاربران سیار از کلیدهای رمز نگاری شده در شبکه*Adhoc* به دست نمی آید که این امر به علت متحرک تصادفی گره ها است که در آن جا اتصال پیوسته حفظ نمی شود.

۲–۱۰–۳–خصوصی سازی

دستکاری هویت یا هر گونه اطلاعات خصوصی باعث ایجاد تهدیدهای خصوصی سازی می شود و بعدها مهندسی می شود تا اینکه محلات*DOS* به وجود می آورند از این رو خصوصی سازی یکی از مسائل اصلی در مورد شبکه ای سازی ویژه است.

۲–۲۰–۴–اهداف امنیتی

امنیت مهمترین مقوله برای شبکه های*Ad-hoc* است به خصوص برای کاربردهای که به امنیت بسیار حساس هستند برای امن سازی یک شبکه*Ad-hoc* ما گزینه های زیر را در نظر گرفته ایم:

قابلیت دسترسی ، محرمانگی ، جامعیت تصدیق هویت

$$a \rightarrow b$$

قابلیت دسترسی بقای سرویس های شبکه ای را در برابر حملات سرویسی تضمین می کند مقاومت در برابر حملات به سرویس می تواند در هر لایه ای از شبکه *Ad-hoc* وجود داشته باشد در لایه های فیزیکی و کنترل دستیابی یک دشمن می تواند از گیرها و کمبودها برای دخالت در ارتباطات از طریق کانال های فیزیکی استفاده کند . در لایه های بالاتر

دشمن می تواند پروتکل مسیریابی را قطع کند و شبکه را قطع کند .در لایه های بالاتر دشمن می تواند کیفیت سرویس های سطح بالا را پایین آورد چنین هدفی اصلی ترین مدیریت سرویس است . ضروری ترین سرویس برای هر چارچوب امنیتی است . محرمانگی تضمین می کند که اطلاعات مشخصی هیچ گاه برای موجودیت های بدون مجوز قابل دسترسی نخواهند بود انتقال اطلاعات حساس از طریق شبکه مثل اطلاعات استراتژیکی یا اطلاعات تاکتیکی نظامی نیاز به محرمانگی دارند کسری از چنین اطلاعاتی می تواند برای دشمنان مفید باشد.

مسیریابی اطلاعات نیز باید در موارد مشخصی محرمانه بماند زیرا اطلاعات می توانند برای دشمن به منظور شناسایی و مشخص سازی مکان آنها در موضع هاشان در میدان جنگ کمک کنند . یکپارچگی تضمین می کند که به پیغام هیچ گاه منحرف نمی شود یک پیغام می تواند به دلیل خرابی مثل خرابی در گسترش رادیویی یا حملات بداند نشانه به شبکه

اتفاق افتد احراز هویت به یک نود اجازه می دهد تا هویت نودی را که با آن ارتباط برقرار می کند شناسایی کند . بدون ابراز هویت دشمن می تواند یک نود را وارد شبکه کند و آن را به عنوان یک نود از شبکه جابرنند و به اطلاعات سری دست پیدا کنند و یا با سایر نودها ارتباط برقرار کنند.

سرانجام قابلیت عدم انکار*(non – repudiation)* این امکان را می دهد که منبع ارسال پیغام نمی تواند ارسال پیغام مشخصی را انکار کند و بگوید این پیغام را نفرستاده ام قابلیت عدم انکار برای مشخص سازی مکان نودهای موجود در شبکه بسیار مفید خواهد بود وقتی نودA یک پیغام نادرست از نودB دریافت می کند می تواند شهادت دهد کهB

آن پیغام را فرستاده و سایرین را نیز متقاعد سازد کهB دارای مشکل یا ... است.

۲-۱۱-سرویسهای امنیتی شبکه

- دسترسی (*Availability*)
- محرمانگی (*Confidentiality*)
- احراز اصالت (*Authentication*)
- یکپارچگی (*Integrity*)
- کنترل دسترسی (*Access Control*)
- انکارناپذیری (*Non-repudiation*)
- مدیریت کلید (*Key Management*)
- مسیریابی امن (*Secure Routing*)
- اجبار تعاون (*Cooperation Enforcement*)
- شناسایی نفوذگر (*Intrusion Detection*)
- مدیریت اعتماد (*Trust Management*)
- امنیت در لایه های پایین تر

۲-۱۲-۱-حملات شناخته شده *(1)*

- حملات فعال (*Active*)
  - پرداخت هزینه انرژی توسط گره بدرفتار (*malicious*) برای اجرای تهدید
  - هدف: قطع و گسستگی شبکه از هم + ضرر رساندن به گره های دیگر
  - تغییر پیام (*modification*)
  - جعل هویت گره (*impersonation*)

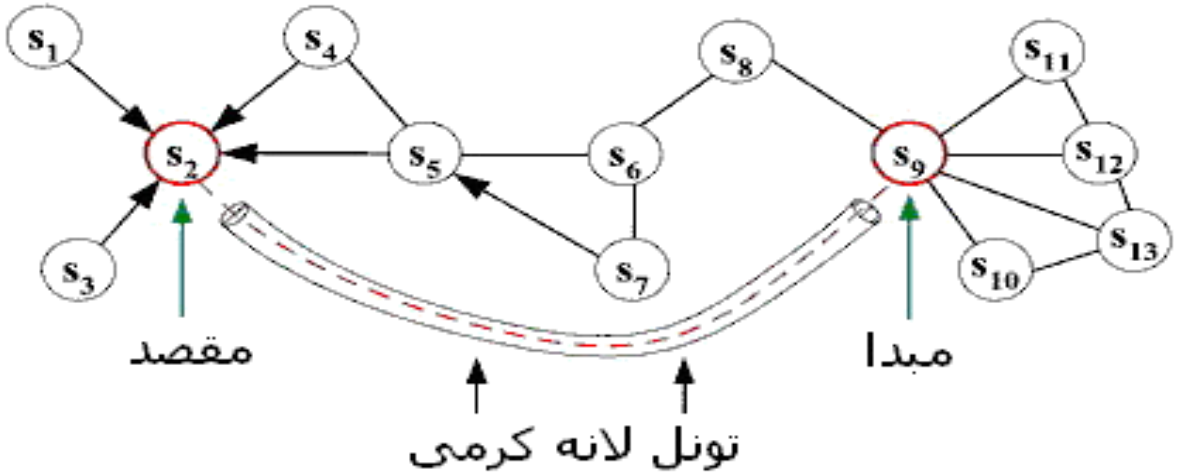
- جعل پیام (*fabrication*)
- حملات غیرفعال (*Passive*)
- امتناع گره خودخواه (*selfish*) از همکاری به قصد ذخیره انرژی
- هدف: کاهش عملکرد شبکه + تقسیم شبکه

۲-۱۲-۲-حملات شناخته شده *(2)*

- **حملات انکار سرویس (Denial of Service)**
- حمله سیاهچاله (*Black-hole*)
- حمله چاله خاکستری (*Grey-hole*)
- حمله انحراف بلاعوض (*Gratuitous Detour*)
- حمله سریع (*Rushing*)
- حمله لانه کرمی (*Wormhole Attack*)

۲-۱۳-حمله لانه کرمی

- ایجاد یک تونل (ارتباط خصوصی مجازی *VPN*) توسط دو مهاجم فعال
- اتصال کوتاه کردن جریان عادی حرکت پیام ها
- نزدیک نشان دادن فاصله دو گره غیرمجاور



شکل 2-2-حمله لانه کرمی

۲-۱۴-چالش ها (دغدغه ها)

موارد مهم و برجسته ای که در شبکه های *Ad-hoc* مطرح است و مشکلات و هم چالش ها در دستیابی به این اهداف امنیتی است.

استقراق سمع پیام ها و پاسخ آنها ممکن است به دشمن امکان دسترسی به اطلاعات سری را بدهد . حملات *active* ممکن است به دشمن امکان از بین بردن پیام و ثانیا نودهایی که دارای حفاظ امنیتی فیزیکی کم هستند که در محیط دشمن گردش می کنند (مثلا در یک جبهه) احتمال خرابی بالایی دارند بنابراین ما فقط نباید نگران حملات خصمانه از بیرون از شبکه باشیم بلکه ممکن است یک نود از داخل نیز باعث مختل شدن سیم شود بنابراین برای دستیابی به *survivability*، شبکه های *Ad-hoc* باید یک معماری توزیع شده بدون موجودیت های متمرکز داشته باشند با ارائه هر موجودیت متمرکز به راه حل امنیتیمان ، باعث آسیب پذیری سیستم خواهیم شد چنانچه این موجودیت متمرکز صدمه بیند تمام شبکه نابود خواهد شد.

یک شبکه *Ad-hoc* دینامیک است و به دلیل تغییراتی که هم در شکل و هم عضویت نودها وجود دارد (مثلا نودها مداوم به شبکه اضافه می شوند و یا خارج می شوند) ارتباط میان نودها نیز تغییر می کند برای مثال وقتی نودهای

مشخصی برای عضویت در شبکه پیدا می شوند برخلاف سایر شبکه های موبایل بی سیم مثل IP سیار، نودها در شبکه $Ad\text{-}hoc$ ممکن است به صورت دینامیک به هم بپیوندند راه حل های و تنظیمات ثابت کافی نخواهند بود . بنابراین یک مکانیزم امنیتی که با این تغییرات در پرواز باشد بسیار مناسب خواهد بود . در پایان یک شبکه $Ad\text{-}hoc$ ممکن است از صدها یا هزاران نود تشکیل شده باشد مکانیزم های امنیتی باید طوری باشد که بتواند چنین شبکه های را مدیریت کنند.

۲-۱۵-*Scope and roadmap*

مکانیزم های امنیتی مثل پروتکل های تصدیق هویت امضای دیجیتالی و رمزنگاری هنوز نقش مهمی در دستیابی به اطمینان یکپارچگی و قابلیت عدم انکار در ارتباطات شبکه های $Ad\text{-}hoc$ ایفا می کنند همچنین این مکانیزم ها به تنهایی کافی نخواهند بود.

۲-۱۶-مقایسه عملکرد و امنیت پروتکل ها

معیار	عملکرد			امنیت		
پروتکل	عملیات سرریز	آرایش کلید	عملیات رمز	محرمانگی	احراز اصالت	دسترسی
ARAN	AODV	ساده	بد	دارد	خوب	ندارد
ARIADNE	DSR	پیچیده	خوب	دارد	خوب	ادعا میشود!
SecMR	X*AODV	متوسط	متوسط	دارد	متوسط	نسبی

SELMAR	2* AODV	متوسط	متوسط	دارد	خوب	خوب

جدول 2-1

۲–۱۷–لزوم امنیت در شبکه های اقتضایی

شبکه های *Ad-hoc* نیز مانند بسیاری از شبکه های بی سیم و سیمی برای انجام و کارکرد صحیح اعمال شبکه که در اینجا شامل مسیریابی، جلورانی بسته های داده، نگهداری و به روز رسانی اطلاعات مسیریابی است، به امنیت نیازمند هستند . در واقع امنیت شرط لازم برای عملکرد درست اعمال شبکه است و بدون نبود آن تضمینی برای انجام صحیح ا ین اعمال وجود ندارد و مهاجمان به راحتی می توانند یکپارچگی شبکه را بر هم بزنند.

سیاستی که در این راستا تدبیر می شود آن است که اعتماد کامل به گره های شبکه برای انجام اعمال حیاتی شبکه کاری عبث و بیهوده است و این رابطه اعتماد تنها در برخی از سناریوهای شبکه *Ad-hoc* قابل فرض است . مثلا در یک شبکه *Ad-hoc* که گره های آن سربازان یک گروهان باشند می توان از قبل، یعنی پیش از شروع عملیات، کلیدهای متقارن مشترک و یا کلیدهای عمومی افراد (بسته به نوع رمزنگاری متقارن یا نامتقارن) را با یکدیگر مبادله کرد . ولی مشکلات و محدودیتهای دیگری همچنان باقی می ماند. از جمله اینکه چنین شبکه ای نمی تواند امنیت را برای قرارگیری افزایشی تامین کند. چرا که گره های جدیدی که می خواهند در شبکه قرار گیرند باید به نوعی خود را به گره های دیگر معرفی کنند و احراز اصالت متقابل برای همه آنها بتواند، صورت بگیرد.

با توجه به بحثهای اخیر می توان چنین برداشت کرد که گره های شبکه *Ad-hoc* برای انجام مدیریت کلید به یک محیط مدیریت شده نیاز دارند. در واقع باید یک یا چند مرکز معتمدوجود داشته باشند تا گره های تازه وارد را در شبکه ثبت کنند و گره های مخرب را از شبکه خط بزنند و بدین ترتیب امنیت شبکه مورد نظر را بر اساس گره های سالم موجود تامین کنند، چرا که گره های مخرب در لیست ابطال قرار گرفته اند.

۲–۱۸–لزوم امنیت در کارکرد صحیح شبکه

منظور از کارکرد صحیح اعمال شبکه این است که هر گره ای از شبکه به وظایف خود مبنی بر جلورانی بسته ها و مسیریابی به درستی عمل کند و در این عملیاتها به خوبی با دیگر گره ها همکاری و مشارکت کند. یعنی اینکه در نهایت اعمال شبکه بین گره ها به صورت منصفانه تسهیم شود.

با توجه به ماهیت ذاتی شبکه های *Ad-hoc* بسادگی می توان چنین برداشت کرد که عملکرد شبکه شدیدا وابسته به رفتار گره های شبکه می باشد. یعنی اگر گره ای وظایفش را به درستی انجام ندهد، بازده عملکرد شبکه به شدت افت میکند و تبادل اطلاعات حیاتی ممکن است به خطر افتد. بر این اساس در برخی از مدلهای پیشنهادی برای برقراری امنیت از منطق اکثریت استفاده میکنند و رفتار ناصحیح گره ها را بر اساس سابقه اعمال آنها بررسی میکنند و اگر این سابقه از یک حد آستانه مربوط به متوسط اعمال بدتر باشد رفتار گره مخرب تشخیص داده می شود. البته این تصمیم گیریها تا حدی نسبی اند و هرگز به طور مطلق نمی توان تعیین کرد که هر رفتاری که از گره ای سر میزند صحیح است یا ناصحیح.

برای پیداکردن گره خرابکار به انجام اعمالی چون ردیابی، نگهبانی و دیده بانی نیاز است که خود محتاج پردازش ارتباطاتی بالا می باشد که هم انرژی می طلبد و هم پهنای باند و حافظه. در نتیجه در شبکه های بی سیم چون *Ad-hoc* نمی توان از پروتکلهای شبکه های بی سیم چون*BGP* استفاده کرد هم از جهت محدودیت پردازش ارتباطاتی و هم از این جهت که توپولوژی شبکه دائم در حال تغییر است.

۲–۱۹–ارتقاء امنیت پروتکل‌های مسیریابی در شبکه‌های اقتضایی

رشد روز افزون شبکه های اقتضایی به دلیل سهولت قرارگیری و کم هزینه بودن آن ها، تامین امنیت در این شبکه ها را با اهمیت جلوه داده است . بهای سادگی راه اندازی این شبکه ها در پیچیدگی پیاده سازی و یکپارچه نگه داشتن اجزای آن پرداخت می‌شود. از این حیث علاوه بر مشکلات کلاسیک امنیتی در شبکه های قطب و پره مسایل نوینی چون حملات لانه کرمی در شبکه‌های اقتضایی مطرح است.

این مقاله در گام اول نیازها و اهداف مطلوب امنیتی در شبکه های اقتضایی بررسی و تدوین می شود. سپس کارکرد پروتکل های پیشنهادی برای ایمن سازی مسیریابی ار زیابی و مقایسه می شود، همچنین به مزایا و معایب هر کدام بر اساس معیارهای مدون اشاره می شود. بر اساس روش های شناخته شده در طراحی پروتکل های مسیریابی امن بعلاوه نکات قابل حصول برای ایجاد امنیت در شبکه های اقتضایی، پروتکل های *ELMAR* و *SELMAR* پیشنهاد می شوند که امنیت مسیریابی در شبکه های اقتضایی را نسبت به معضل عدم همکاری گره ها و حملات فعالی چون حمله لانه کرمی ارتقاء می دهند. نتایج شبیه‌سازی نحوه کارکرد این پروتکل ها توسط شبیه ساز *MANET*، که به همین منظور طراحی شده است، نشان می دهد که این پروتکل‌ها در برابر حملات شناخته‌شده از مقاومت لازم و خوبی برخوردارند.

پروتکلهای مسیریابی بر اساس پارامترهای کانال مانند تضعیف، انتشار چند مسیره، تداخل و همچنین بسته به کاربرد شبکه به صورت بهینه طراحی شده اند. در هنگام طراحی این پروتکلها به امر تضمین امنیت در شبکه های *Ad-hoc* توجه نشد. در سالهای اخیر با توجه به کاربردهای حساس این شبکه از جمله در عملیاتهای نظامی، فوریتهای پزشکی و یا مجامع و کنفرانسها، که نیاز به تامین امنیت در این شبکه ها بارزتر شده است، محققان برای تامین امنیت در دو حیطه عملکرد و اعتبار پیشنهادات گوناگونی را مطرح کردند و می کنند.

شبکه های بی سیم *Ad-hoc* فاقد هسته مرکزی برای کنترل ارسال و دریافت داده می باشد و حمل بسته های اطلاعاتی به شخصه توسط خود گره های یک مسیر مشخص و اختصاصی صورت می گیرد. توپولوژی شبکه های *Ad-hoc* متغیر است زیرا گره های شبکه می توانند تحرک داشته باشند و در هر لحظه از زمان جای خود را تغییر بدهند.

وقتی گره ای تصمیم می گیرد که داده ای را برای گره مورد نظر خود بفرستد. ابتدا با انجام یک پروتکل مسیریابی پخش شونده کوتاهترین مسیر ممکن به گره مورد نظر را بدست می آورد و سپس با توجه به این مسیر داده را ارسال میکند. به هنگام به روز رسانی یا کشف مسیر مورد نظر تمام گره های واقع بر روی مسیر اطلاعات مربوط به راه رسیدن به گره مقصد

را در جدول مسیریابی خود تنظیم می کنند، تا در هنگام ارسال داده از مبدا روند اجرای عملیات ارسال داده به درستی از طریق کوتاهترین مسیر ممکن انجام شود.

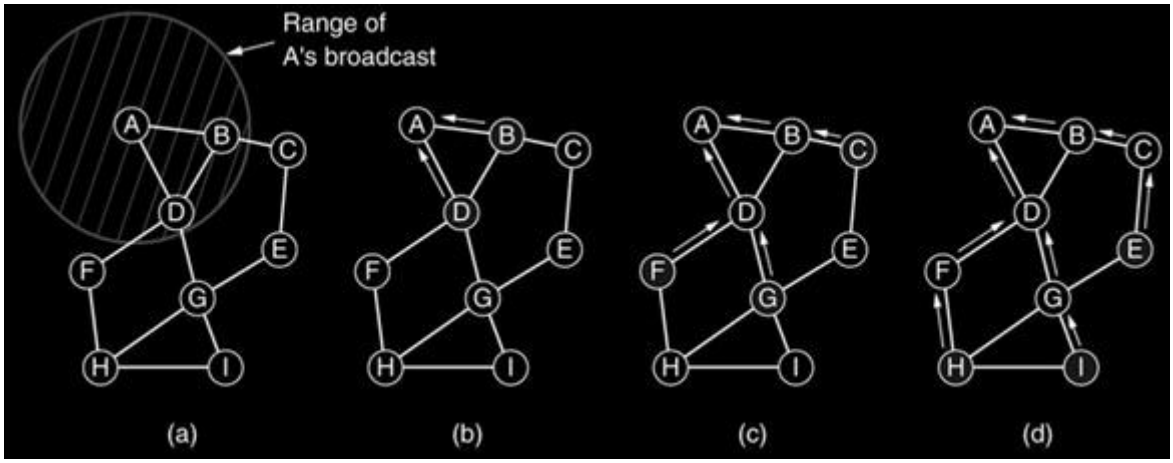
۲-۱۹-۱-پروتکل مسیریابی AODV

پروتکل $AODV$ نمونه ای از یک پروتکل مسیریابی بر حسب نیاز است که بر اساس مسیریاب بردار فاصله

عمل میکند. نمایی از نحوه عملکرد این پروتکل در شکل ۲-۳آمده است. همانطور که در شکل ۲-۳ مشاهده می شود ابتدا گره مبدا (A) بسته درخواست مسیر خود به گره مقصد (I) را می سازد و آن را به اطراف پخش میکند.

سپس هر گره ای که در شعاع رادیویی گره مبدا باشد (گره های B و D) بسته $RReq$ را شنود میکند و اگر بسته تکراری باشد، آنگاه آن را دور می ریزد و اگر تکراری نباشد، به جدول مسیر خود نگاه میکند . اگر مسیر تازه ای به مقصد درخواستی در جدول موجود باشد، آنگاه بسته جواب مسیررا می سازد و برای گره مبدا در یک جهت پخش میکند.

ولی اگر مسیر تازه ای وجود نداشت، آنگاه به شمارنده گره یک واحد می افزاید، بسته $RReq$ را دوباره به همه گره های همسایه پخش میکند و اطلاعات مبدا را برای مسیریابی معکوس ذخیره میکند.



شکل ۲-۳ نمایی از پروتوکل مسیریابی AODV

مقادیر و پارامترهای مربوط به بسته های *RReq* و *RRep* که شامل آدرس مبدا و مقصد، شماره درخواست در *RReq*، شماره مسلسل مبدا و مقصد، شمارنده گره و طول عمر بسته می باشد، در شکل ۲-۴ نشان داده شده است.

Route Request Packet

Source address	Request ID	Destination address	Source sequence #	Dest. sequence #	Hop count

Route Reply Packet

Source address	Destination address	Destination sequence #	Hop count	Lifetime

شکل ۲-۴ بسته RReq و RRep در پروتکل مسیریابی AODV

۲–۲۰–انواع حملات بر روی شبکه های اقتضایی

حملات انجام شده بر روی شبکه های *Ad-hoc* را می توان از چند جنبه دسته بندی کرد . در اینجا ابتدا یک دسته بندی کلاسیک از حملات ارائه شده است و در ادامه به طور مستقل به حملات ممکن پرداخته می شود.

حملات فعال که در آنها گره بدرفتار برای اجرای تهدید خودش باید هزینه انرژی آن را بپردازد . چنین گره ای اصطلاحا گره مخرب یا بداندیش نامیده میشود. هدف از انجام این حمله از هم گسستگی شبکه یا ضرر رساندن به گره های دیگر است.

حملات غیرفعال که در آنها گره بدرفتار به قصد ذخیره انرژی از همکاری امتناع میکند. چنین گره ای گره خودخواه نامیده میشود. هدف از انجام این حمله کاهش عملکرد شبکه یا تقسیم شبکه با شرکت نکردن در عملیاتها است.

از دیدگاهی دیگر می توان حملات را به سه بخش زیر تقسیم کرد که هر کدام از این بخشها را می توان جزئی از حمله فعال ذکر شده در بالا نیز محسوب کرد. در واقع حمله غیرفعال می تواند به طور غیرمستقیم بر روی عملکرد شبکه تاثیر بگذارد لذا آن را به عنوان یک مورد خاص هم می توان در نظر گرفت. در عمل همواره ترکیبی از حمله فعال به همراه غیرفعال وجود دارد.

حمله به قصد تغییر بر روی پروتوکلهای فعلی قابل اعمال است چرا که پروتوکلهای فعلی هیچ حفاظتی در برابر یکپارچگی اطلاعات ندارند لذا براحتی قابل تغییرند. در نتیجه گره خرابکار می تواند یکپارچگی محاسبات مسیریابی را با تغییر بر هم بزند و بدین طریق بسته های اطلاعات صحیح را دور بریزد و پروسه را به کشف مسیر نادرست هدایت کند و یا اینکه مسیر ترافیک را طولانی کند و یا اینکه باعث ازدیاد ترافیک در یک مسیر خاص شود.

حمله به قصد جعل هویت به این صورت است که گره خرابکار اصالت خود را به گره دیگری تغییر می دهد و از آنجا که در پروتوکلهای فعلی بسته ها احراز اصالت نمی شوند، مهاجم با هویت نادرست شناخته می شود. به این حمله در امنیت شبکه اصطلاحا *Spoofing* گفته می شود که در اینجا مهاجم حتی می تواند تصویر توپولوژی شبکه را تغییر دهد و یا در اطلاعات مسیریابی حلقه تکرار بینهایت ایجاد کند.

حمله به قصد جعل پیام برای تولید پیامهای مسیریابی غلط توسط گره مخرب و حذف گره همسایه با ارسال خطای مسیریابی جعلی است. متاسفانه این حملات به سختی قابل تشخیص اند چرا که جاعل پیام را نمی توان براحتی شناسایی کرد و مهاجم براحتی می تواند قسمتهای مختلف پیام را به نفع خود تنظیم کند و بعد آنها را در میان شبکه پخش کند.

از انواع دیگر حملات می توان حمله *DoS*را نام برد که مهاجم بسته صحیح داده را به قصد گسستن مسیریابی در مسیر غلط هدایت میکند. از دیگر انواع این حمله می توان از حمله مصرف منابع نام برد که در آن حمله کننده برای اشغال پهنای باند کانال، توان محاسباتی، یا حافظه گره ها به شبکه داده بی مورد تزریق میکند.

در حمله سیاهچاله مهاجم با انتشار اخبار دروغین مسیریابی برای کوتاه‌ترین مسیر، ترافیک شبکه را به طرف خود جذب میکند و سپس آن را دور میریزد. مدل پیشرفته تر حمله سیاهچاله حمله *Grey-hole* است که در آن مهاجم تنها بسته های داده را دور میریزد، ولی بسته های مسیریابی را *forward* میکند تا مسیر ساختگی خود را پابرجا نگاه دارد!

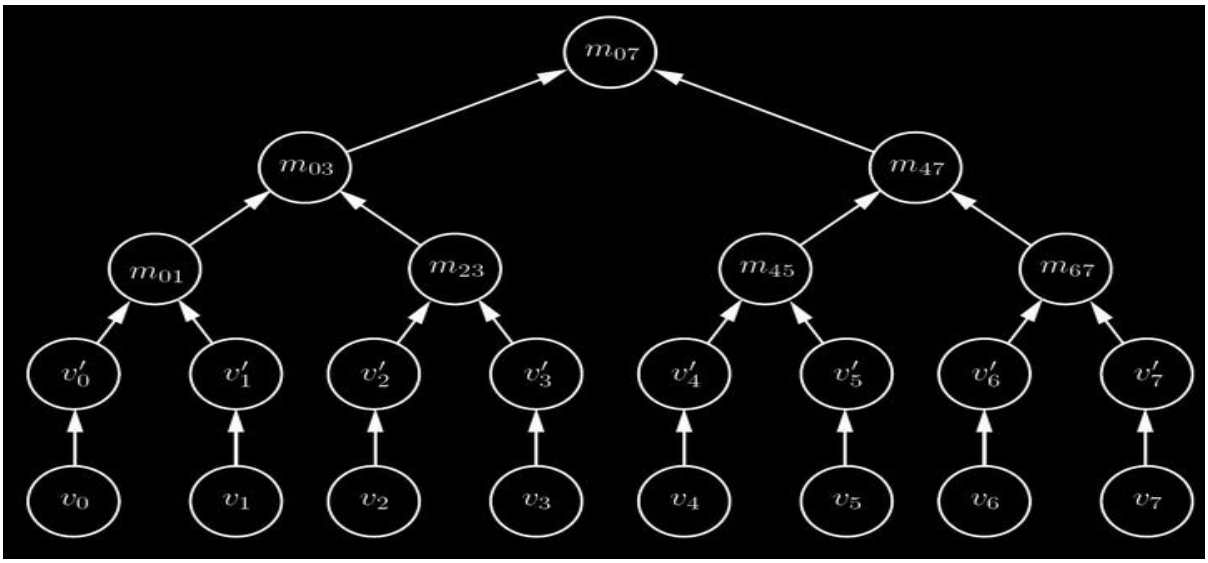
در حمله انحراف بلاعوض مهاجم با افزودن گره های مجازی به اطلاعات مسیریابی مسیر را بلندتر نشان میدهد.

در حمله سریع مهاجم اخبار نادرست درخواست مسیر را به سرعت در سراسر شبکه پخش میکند تا گره ها به علت تکرار پیام درخواست صحیح مسیریابی را دور بریزند.

حمله لانه کرمی به عنوان یک حمله ماهرانه تلقی می شود که در آن دو مهاجم فعال با ایجاد یک تونل ارتباط خصوصی مجازی جریان عادی حرکت پیامها را اتصال کوتاه میکنند و با این روش می توانند دو گره غیرمجاور را با هم همسایه کنند و یا از پروتکل کشف مسیر جلوگیری کنند . متاسفانه بسیاری از پـروتکلهای مسیریابی مانند *DSR*، *AODV*، *OLSR*، و *TBRPF* به این حمله آسیب پذیرند.

یکی از روشهای مقابله با حمله لانه کرمی استفاده از افسار بسته که به دو صورت جغرافیایی و زمانی انجام می شود . ایده اصلی آن است که گیرنده با احراز اصالت اطلاعات دقیق مکان یا زمان به همراه تمبر زمانی متوجه سفر غیرواقعی بسته برای یک توپولوژی خاص شبکه میشود.

در افسار بسته زمانی زمان سفر بسته از تفاوت بین زمان گیرنده و تمبر زمانی بدست می آید که این زمان هم با این فرض بدست آمده که گره های شبکه سنکرون باشند و در عمل همواره یک ماکزیمم خطای همگامی داریم که باید لحاظ شود . یکی از متدهای مورد استفاده در افسار بسته زمانی پروتکل *TESLA* می باشد که در آن از درخت درهم ساز *Merkle* استفاده شده است. همانطور که در شکل ۲-*5* می بینید برای احراز کردن مقدار *m07* با فرض داشتن *v'3*، *m01*، و *m47* مقدار خروجی رابطه ۱را بدست می آوریم و با مقدار *m07* مقایسه می کنیم.



شکل ۲-۵

Merkle Hash Tree (1980)

$$H\left[H\left[m_{01} \,||\, H\left[\,H[\,v_2\,] \,||\, v'_3\,\right]\right] \,||\, m_{47}\right]$$

محاسبه مقدار راس در Merkle Hash Tree

در افسار بسته جغرافیایی یا مکانی از اطلاعات مکانی و کلاکهای همگام آزاد استفاده می شود و از روی خطای همگامی $\pm\Delta$، حد بالای سرعت گره v، تمبر زمانی Ts، زمان محلی گیرنده Tr، مکان گیرنده Pr، و مکان فرستنده Ps مقدار حد بالای فاصله بین فرستنده و گیرنده را به صورت زیر بدست می آورند.

$$d_{sr} \le \left\| p_s - p_r \right\| + 2v \cdot (t_r - t_s + \Delta) + \delta$$

حد بالای فاصله بین گیرنده و فرستنده

افسار بسته مکانی یا جغرافیایی به دلیل وابستگی شدید به توپولوژی شبکه و پارامترهای کانال همچون مقدار تضعیف و *Short and Long Range Fading* در عمل با توجه به مدل انتشار رادیویی بسیار آسیب پذیر است و بیشتر از مدل زمانی آن که بهینه تر است، استفاده می شود.

۲-۲۱-آرایش کلید در شبکه های اقتضایی

در شبکه های *Ad-hoc* مصالحه گره توسط مهاجم یک تهدید فاجعه آمیز است. قدرت حمله مهاجم توسط

تعداد گره های در اختیار خودش به همراه تعداد گره های مصالحه شده یا لو رفته توسط او تعیین می شود . از این جهت نیز می توان برای قدرت تخریب و نفوذ حملات باند بالا و پایین در نظر گرفت. همانطور که گفته شد برای جلوگیری از این حملات نیاز به یک محیط مدیریت شده حیاتی است.

برای یک شبکه اختصاصی توزیع کلیدهای جلسه می تواند قبل از قرارگیری گره ها از طریق یک بخش ثالث معتمد انجام شود و به منظور تمیز دادن گره های سالم از بقیه گره ها هر گره سالم با چند کلید منحصر به فرد احراز هویت میشود . مشکل آرایش کلید در شبکه های *Ad-hoc* این است که چگونه اطلاعات کلید معتبر را توزیع کنیم!

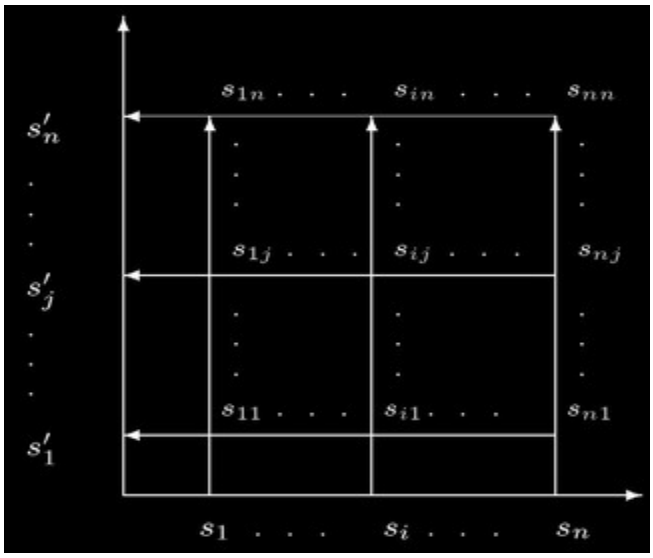
یکی از روشها این بود که کلیدهای مخفی مشترک تولید کنیم، همانند مدل احیای جوجه اردک که در آن دو گره برای اتصال گره *Slave* به گره *Master* به هم وصل میشوند و اطلاعات تبادل کلید از طریق آنها برقرار می شود، یا مدل کانال کناری برای یافت فرستنده ها. این مدلها همگی دارای محدودیتهای ساختاری هستند و انعطاف پذیری موجود در شبکه های *Ad-hoc* را به نوعی مقید می کنند.

اگر فرض کنیم که هر گره لیست کلیدهای عمومی معتبر گره های سالم را قبل از قرارگیری در شبکه دارد . بعد از توزیع کلیدهای عمومی با استفاده از پروتوکل تبادل کلید *Diffie-Hellman* بین هر دو گره مورد نظر می توان کلید مخفی مشترک را مبادله کرد. در نتیجه لزوم وجود مرکزی معتمد (*TA*) برای ثبت گره های جدید و کلا برقراری زیرساختار کلید عمومی شبکه کاملا احساس می شود. همچنین برای تبادل کلید مخفی وجود ارتباط امن (بدون شنود) بین *TA* و گره تازه وارد لازم است و برای تبادل لیست کلید گره های سالم وجود ارتباط امن از حمله فعال الزامی است.

یک راه حل برای حل این مشکل استفاده از آدرسهای *SUCV*بود که در آن هر گره یک کلید عمومی و یک کلید خصوصی برای خود دارد و آدرس *SUCV* را بر اساس درهم شده کلید عمومی بدست می آورد . ولی در این روش همچنان مشکل بدست آوردن لیست نام گره های سالم (بدون کلید عمومی) باقی است. برای رفع این مشکل در برخی شبکه های *Ad-hoc* یک یا چند *CA* تعریف می کنند که کار آنها صدور گواهینامه گره که شامل آدرس، کلید عمومی و امضای *CA* است، می باشد. مراکز *CA* نمی توانند همواره درون خط باشند چرا که دوباره یک وابستگی چرخشی بین مسیریابی و امنیت بوجود می آید. زیرا مسیریابی به امنیت نیازمند است و پیاده سازی امنیت نیازمند مسیریابی درون خط است. در نتیجه در موارد حیاتی *CA*ها به صورت برون خط عمل می کنند.

روش پیشنهادی دیگر برای حل مساله زیرساختار کلید عمومی استفاده از رمزنگاری آستانه ای می باشد که در آ ن سهمی از هر کلید خصوصی بین گره ها به اشتراک گذاشته می شود. این روش در واقع نوع بسط یافته از مبحث

تسهیم راز می باشد. همانطور که در شکل ۲-٦ نشان داده شده است هر t انتخاب از serverهای S1 تا Sn می تواند به بازیابی یا به روز رسانی کلید یکی از serverها منجر شود.



شکل ۲-۶ مصداقی از رمزنگاری آستانه ای در شبکه های Ad-hoc

راه حل بعدی استفاده از اعتماد تراگذراست که نمونه ای از آن در شبکه اعتماد PGP استفاده می شود و بدین صورت عمل میکند که گره A هویت یا کلیدعمومی گره B را با توجه به امضاهای گره های معتمد (از نظر گره A) پای کلیدعمومی گره B احراز میکند. مشکل اساسی در این ساختار ابطال کلیدهای جعلی است و اینکه چگونه به سرعت اطلاعات لیست کلیدهای ابطال شده را در شبکه پخش کرد.

۲-۲۲-نمونه هایی از پروتکلهای امن پیشنهادی در شبکه های *Ad-hoc*

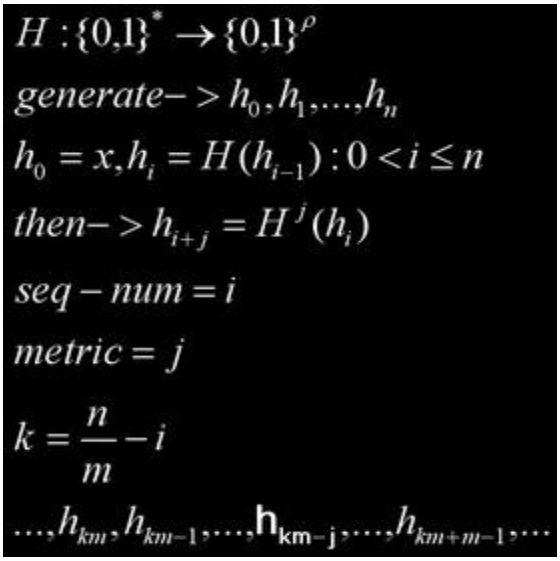
این بخش به معرفی اجمالی برخی از پروتکلهای امن که در شبکه های $Ad\text{-}hoc$ برای برقراری مسیریابی و نگهداری امن آن استفاده می شود، پرداخته است. بیشتر این پروتکلها یا بر مبنای پروتکلهای معمول مسیریابی در قدیم بوده اند که به آنها یک

پسوند یا پیشوند امنیتی اضافه شده است و یا بر اساس مطالب بیان شده در بخشهای قبلی مدل پیشنهادی بیشتر از حیث پروتکلهای امنیت شبکه نمود یافته است و عملکرد بهینه مسیریابی در آن لحاظ نشده است.

۲-۲۲-۱-پروتکل مسیریابی SEAD

پروتکل مسیریابی SEAD در برابر حملات ناهماهنگ فعال مقاوم است و از رمزنگاری متقارن استفاده میکند . مسیریابی با توجه به پروتکل مسیریابی DSDV که مدل بهبود یافته پروتکل مسیریابی بردار فاصله است، صورت میگیرد. لازم به ذکر است که در مسیریابی با بردار فاصله، متریک هر مقصد (که معمولا همان تعداد گره های عبوری در مسیر است) و اولین گره مسیر به مقصد در برداری به نام بردار فاصله مشخص می شود و در مدل بهبود یافته آن شماره مسلسل آخرین باری که مقصد بهروز رسانی شده است هم ذکر می شود.

در پروتکل مسیریابی SEAD از زنجیره اعداد درهم شده استفاده می شود. بدین صورت که مجموعه ای از اعداد درهم شده متوالی توسط مبدا و مقصد تولید می شود و احراز اصالت پیام دریافتی همانگونه که در شکل ۲-۷ نشان داده شده است، با توجه به متریک و شماره مسلسل پیام صورت میگیرد. در واقع گیرنده با انجام Hashهای متوالی بر روی مقدار دریافتی می تواند به مقدار اولیه در انتهای زنجیره اعداد درهم خود برسد که تعداد عملهای Hashی لازم برای این کار را با توجه به روابط زیر انجام می دهد.



$$H:\{0,1\}^{*}\rightarrow\{0,1\}^{\rho}$$
$$generate->h_0,h_1,\ldots,h_n$$
$$h_0=x,h_i=H(h_{i-1}):0<i\leq n$$
$$then->h_{i+j}=H^{j}(h_i)$$
$$seq-num=i$$
$$metric=j$$
$$k=\frac{n}{m}-i$$
$$\ldots,h_{km},h_{km-1},\ldots,\mathbf{h_{km-j}},\ldots,h_{km+m-1},\ldots$$

شکل ۲-۷

۲-۲۲-۱-۱-زنجیره اعداد درهم

از زنجیره اعداد درهم علاوه بر احراز اصالت به روز رسانیهای مسیریابی می توان برای تثبیت باند پایین متریک هم

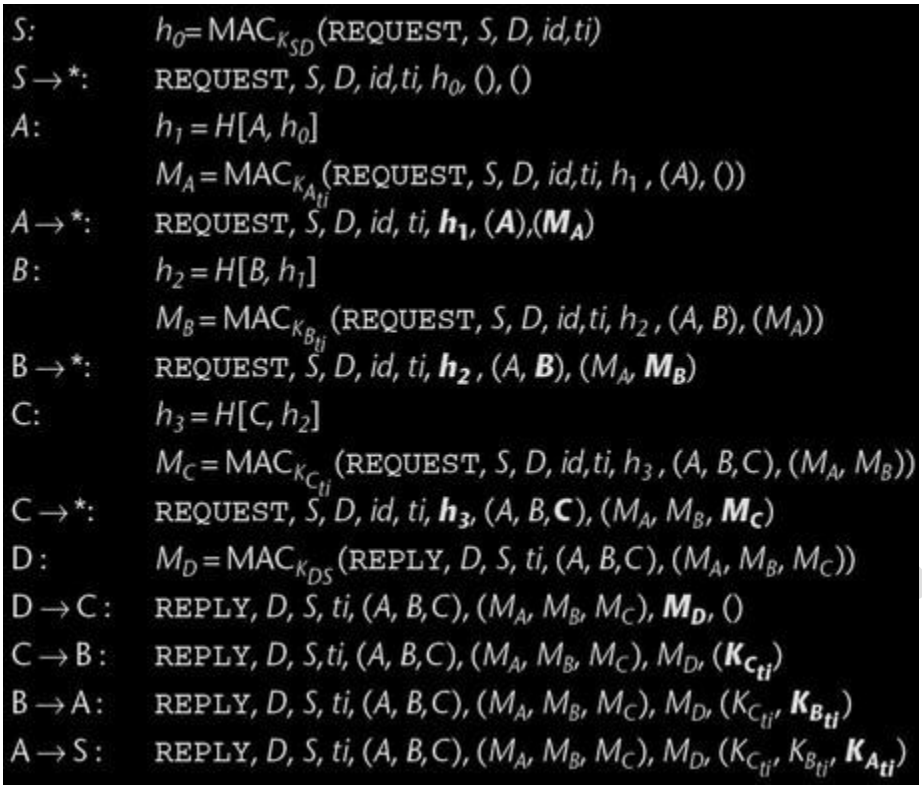
استفاده کرد، چرا که مهاجم هرگز نمی تواند مقدار متریک داخل کد احراز پیام درهم شده را کاهش دهد، زیرا باید معکوس تابع درهم ساز را بدست آورد! ولی با قراردادن گره های مجازی می تواند مقدار متریک مسیر را بزرگتر نشان دهد . لذا شبکه باید یک باند بالا برای متریک مسیرهای ممکن در شبکه تعیین کند که این کار خود بسیار مشکل است چرا که توپولوژی شبکه دائم در حال تغییر می باشد.

۲-۲۲-۲-پروتکل مسیریابی امن برحسب نیاز به نام ARIADNE

پروتکل مسیریابی امن برحسب نیاز *ARIADNE* در برابر مصالحه گره ها ایستادگی میکند و بر مبنای رمزنگاری متقارن بهینه عمل میکند. احراز اصالت پیامها توسط کلید مشترک بین هر جفت گره یا کلید مشترک بین گره های مرتبط با احراز جزئی در میان مسیر و یا امضای دیجیتال صورت میگیرد که در اینجا امضای دیجیتال انکارناپذیری را تامین نمی کند و تنها احراز هویت را انجام می دهد. برای احراز اصالت از مدل پروتکل *TESLA* استفاده می شود و همگام سازی گره ها به صورت آزاد انجام می شود. در نتیجه باید هزینه بیشتری برای آرایش کلید بپردازیم.

برای مسیریابی و نگهداری مسیر از پروتکل *DSR* ایده گرفته شده است. ولی با این وجود به حمله مهاجمی که در مسیر کشف شده پنهان شده است، آسیب پذیر می باشد لذا تصمیم گیری بر اساس سابقه عملکرد گره ها صورت میگیرد که همانطور که در ابتدای بحث بیان شد این تصمیم گیریها نسبی است.

مدل پروتکل *ARIADNE* را در شکل ۲-۸مشاهده میکنید. مقادیر پررنگ توسط همان گره ای که نامش پررنگ شده و همچنین توسط مبدا (*Source*) و مقصد (*Destination*) قابل احراز اصالت هستند. کلید مشترک *Ksd* بین مبدا و مقصد مشترک است. در مسیر بازگشت پیام *RRep* با عبور از هر گره احراز اصالت می شود و در نهایت نیز توسط مبدا قابل احراز است، اگر مهاجم فرضی آن را تغییر نداده باشد. چنین مهاجمی می تواند در میان مسیر قرار گرفته و با مسکوت گذاردن عمل مسیریابی حمله *DoS* را پیاده سازی کند.



شکل ۲-۸ پروتکل مسیریابی امن برحسب نیاز ARIADNE

۲-۲۲-۳-پروتکل مسیریابی ARAN

۲-۲۲-۳-۱-خصوصیات پروتکل مسیریابی *ARAN* را می توان به صورت زیر برشمرد:

- استفاده از رمزنگاری کلید-عمومی
- مسیریابی بر اساس *AODV*

- هر گره گواهینامه امضا شده توسط TA دارد.

- آدرس IP بر اساس کلید عمومی ($SUCV$)

در پروتکل مسیریابی $ARAN$ هر گره جواب مسیر ($RRep$) را $unicast$ میکند به گره پیشینی که از آن درخواست مسیر ($RReq$) را دریافت کرده است و هر گره جدول مسیریابی خود را بر اساس جواب مسیر ($RRep$) به گره مقصد به روز رسانی میکند. اگر گره ای بمیرد، گره های همسایه به دیگران با ارسال پیام خطای مسیر ($Route\ Error$) اطلاع می دهند . این پروتکل به حمله DoS بر مبنای $flooding$ی اطلاعاتی که باید امضای آن تایید شود، آسیب پذیر است . نمونه مدل پروتکل $ARAN$ را در شکل 2- ۹مشاهده میکنید.

$S \rightarrow *$: (ROUTE REQUEST, D, $cert_S$, N, $t)_{K_S^-}$

$A \rightarrow *$: ((ROUTE REQUEST, D, $cert_S$, N, $t)_{K_S^-})_{K_A^-}$, $cert_A$

$B \rightarrow *$: ((ROUTE REQUEST, D, $cert_S$, N, $t)_{K_S^-})_{K_B^-}$, $cert_B$

$C \rightarrow *$: ((ROUTE REQUEST, D, $cert_S$, N, $t)_{K_S^-})_{K_C^-}$, $cert_C$

$D \rightarrow C$: ((ROUTE REPLY, S, $cert_D$, N, $t)_{K_D^-}$

$C \rightarrow B$: ((ROUTE REPLY, S, $cert_D$, N, $t)_{K_D^-})_{K_C^-}$, $cert_C$

$B \rightarrow A$: ((ROUTE REPLY, S, $cert_D$, N, $t)_{K_D^-})_{K_B^-}$, $cert_B$

$A \rightarrow S$: ((ROUTE REPLY, S, $cert_D$, N, $t)_{K_D^-})_{K_A^-}$, $cert_A$

شکل 2- ۹پروتکل مسیریابی ARAN

۲-۲۲-۴-پروتکل مسیریابی SAODV

پروتکل مسیریابی SAODV مشابه ARAN از رمزنگاری کلید-عمومی استفاده میکند و مسیریابی را بر اساس پروتکل AODV انجام می دهد. از پسوند تک امضایی برای احراز اصالت بیشتر قسمتهای RReq یا RRep

استفاده میکند. از زنجیره اعداد (Hash Chains) برای احراز اصالت متریک (hop-count)ی مسیر استفاده میکند. در واقع پروتکل مسیریابی SAODV یک الحاق امضا به پروتکل مسیر یابی AODV است، با قابلیت امکان استفاده از پسوند دوامضایی مشابه ARAN. ولی هزینه محاسباتی آن مشابه ARAN است چون تنها یک امضا در هر دو پروتکل تایید می شود.

۲-۲۳-مسائل قابل بحث در آینده بر روی امنیت شبکه های اقتضایی

- بدست آوردن مدلی برای مشکلات امنیتی مسیریابی امن
- ارزیابی و مقایسه علمی بین انواع پروتکلها
- روشهای استاندارد برای بررسی و طراحی امن شبکه
- طراحی بهینه پروتکل مسیریابی با توجه به بده-بستان بین امنیت و عملکرد
- منطق طراحی یک پروتکل امن برای شبکه های بی سیم *Ad-hoc*