بسمه تعالی

پروژه پیشنهادی و فرم تخصیص پروژه

نام و نام خانوادگی : غزال لباف راد | شماره دانشجویی: ۸۹۰۵۵۱۲۵۲ | شماره پروژه :

رشته : مهندسی فناوری اطلاعات | مقطع : کارشناسی پیوسته

زمان اخذ پروژه : نیمسال دوم ۹۲-۹۳ | تاریخ تصویب نهایی :

نام و نام خانوادگی استاد : خانم مهندس مرجان گودرزی

عنوان پروژه : امنیت مسیر یابی در شبکه‌های موردی

اهدف پروژه :

۱) بررسی پروتکل‌های مسیر یابی
۲) تحلیل و تست آن پروتکل‌های مسیر یابی تحت همان پارامترها و سناریوهای شبکه
۳) ارزیابی هر یک از پروتکل‌ها بر مبنای عملکردش
۴) بررسی حملات به شبکه‌های موردی
۵) ارائه الگوریتم مسیر یابی امن
۶) شبیه سازی سه پروتکل **AODV,OLSR,DSR** در نرم افزارهای شبیه ساز شبکه مانند **NS۲**

مقدمه پروژه:

شبکه‌های موردی شبکه‌هایی هستند که برای مسیریابی از هیچ عنصر کمکی شبکه ای استفاده نمی‌کنند. بلکه در این شبکه‌ها خود گره‌های شرکت کننده در شبکه وظیفه مسیریابی شبکه را به عهده دارند. امنیت در شبکه-های موردی از وضعیت ویژه‌ای برخوردار است. زیرا دراین شبکه‌ها علاوه بر تمامی مشکلات موجود در شبکه‌های با سیم، با مشکلات امنیتی همچون سادگی شنود و تغییر اطلاعات در حال انتقال، امکان جعل هویت افراد، شرکت نکردن و یا تخریب عملیات مسیریابی، عدم امکان استفاده از زیرساخت‌های توزیع کلید رمزنگاری و غیره مواجه می شویم. یکی از مهم‌ترین موارد امنیتی در شبکه‌های موردی، ارائه یک الگوریتم مسیریابی امن در این شبکه‌ها است. در چند سال اخیر تلاش زیادی برای ارائه یک الگوریتم مسیریابی امن در شبکه‌های موردی انجام شده است. از این میان می‌توان به پروتکل‌های **SEAD**، **Ariadne**، **SRP**، **SAODV**،**ARAN** و غیره اشاره کرد. ولی هر کدام از آن‌ها دارای مشکلات خاص مربوط به خود می‌باشند و همچنان کمبود یک الگوریتم که هم از لحاظ امنیت و هم از لحاظ کارایی شبکه در حد قابل قبولی باشد احساس می‌شود. در این پایان نامه به بررسی شبکه‌های موردی و موارد امنیتی مربوط به آن می‌پردازیم. و در ادامه الگوریتم‌های مسیر یابی را در این شبکه

مورد بررسی قرار می‌دهیم ودر ا نتها به ارزیابی پروتکل‌های مسیر یابی بر مبنای نتایج استخراج شده ازشبیه ساز **ns۲** می‌پردازیم.

مراحل انجام پروژه:

۱. بررسی شبکه‌های موردی و مشکلات امنیتی این شبکه‌ها
۲. بررسی انواع الگوریتم‌ها و پروتکل‌های مسیر یابی در شبکه‌های موردی
۳. ارزیابی دو پروتکل مسیر یابی AODV,DSR و یک پروتکل پیشتاز OLSR بر مبنای نتایج شبیه سازی با شبیه ساز شبکه NS۲
۴. ارائه الگوریتم مسیر یابی امن

شرح پروژه:

شبکه‌های موردی به علت عدم استفاده از زیر ساخت از پیش بنا شده می‌توانند استفاده‌های گوناگونی داشته باشند. این شبکه‌ها می‌توانند به راحتی راه اندازی شوند، مورد استفاده قرار بگیرند و نهایتا از میان بروند. از موارد استفاده شبکه‌های موردی می‌توان به کاربردهای شخصی مانند اتصال لپ تاپ‌ها به یکدیگر، کاربردهای عمومی مانند ارتباط وسایل نقلیه و تاکسی‌ها،کاربردهای نظامی مانند ارتش و ارتباط ناوگان جنگی و کاربردهای اضطراری مانند عملیات امداد و نجات اشاره کرد. از آنجا که عمل مسیریابی در شبکه‌های موردی به عهده خود گره‌های شرکت کننده در شبکه است امنیت مسیریابی در این شبکه‌ها بیش از دیگر شبکه‌ها خود را نشان می‌دهد.

شبکه موردی شبکه ای است که توسط **host** های بی سیم که می‌توانند سیار هم باشند تشکیل می‌شود در این شبکه لزوما از هیچ زیر ساخت پیش ساخته ای استفاده نمی‌شود. بدین معنا که هیچ زیر ساختی مانند یک ایستگاه مرکزی، مسیر یاب، سوییچ و یا هر چیز دیگری که در دیگر شبکه‌ها از آن‌ها برای کمک به ساختار شبکه استفاده می‌شود، وجود ندارد. بلکه فقط تعدادی گره بی سیم هستند که با کمک ارتباط با گره‌های همسایه، به گره‌های غیر همسایه متصل می‌گردند.

در شبکه‌های موردی، سیار بودن گره‌ها ممکن است باعث تغییر مسیر بین دو گره شود. همین امر است که باعث تمایز این شبکه‌ها از دیگر شبکه‌های بی سیم می‌شود. با وجود تمامی این مشکلات، از شبکه‌های موردی در موارد بسیاری استفاده می شود. دلیل این امر سرعت و آسانی پیاده سازی این شبکه و همچنین عدم وابستگی آن به ساختارهای از پیش بنا شده است.

مشکلات امنیتی در شبکه‌های موردی:

مشکلات امنیتی در شبکه‌های موردی از آن جهت خاص شده و جداگانه مورد بررسی قرار می‌گیرد که در این شبکه‌ها، علاوه بر این که تمامی مشکلات موجود در یک شبکه با سیم و یا یک شبکه بی سیم ولی با زیر ساخت با سیم وجود دارد، بلکه مشکلات بیشتری نیز دیده می شود. مانند اینکه از آنجا که تمامی ارتباطات به صورت بی سیم انجام می‌شود،می‌توان آن‌ها را شنود کرد و یا تغییر داد. همچنین ازآن‌جایی که خود گره‌ها در عمل مسیریابی شرکت می‌کنند، وجود یک گره متخاصم می‌تواند به نابودی شبکه بیانجامد. همچنین در این شبکه‌ها تصور یک واحد توزیع کلید و یا زیر ساخت کلید عمومی و غیره مشکل است. زیرا این شبکه‌ها اغلب بدون برنامه ریزی قبلی ایجاد می‌شوند و برای مدت کوتاهی نیاز به برقراری امنیت دارند از این رو امنیت در این شبکه‌ها به صورت جداگانه مورد بحث و بررسی قرار می‌گیرند. در مجموع می توان موارد امنیتی در شبکه‌های موردی را به

صورت زیر دسته بندی کرد.

۱. مدیرت کلید
۲. مسیر یابی امن
۳. تصدیق اصالت
۴. جلوگیری از حملات ممانعت از سرویس
۵. تشخیص نفوذ و...

موارد ذکر شده هریک به صورت خاص برای شبکه‌های موردی مورد بررسی قرار می‌گیرند. هر کدام از این مواد زمینه بحث گسترده ای دارند و به علت جدید بودن شبکه‌های موردی، میدان فعالیت در آن‌ها بسیار زیاد است. در این پایان نامه ما تنها به مورد دوم یعنی امنیت مسیر یابی می‌پردازیم.

مشکلات امنیتی در مسیر یابی شبکه‌های موردی:

حملات علیه شبکه های موردی را می‌توان از چند دیدگاه دسته بندی نمود. در دیدگاه اول دسته بندی می‌تواند به صورت حملات داخلی و خارجی باشد. حملات داخلی حملاتی است که توسط گره‌های مجاز داخل شبکه انجام می‌شود و غالبا جلوگیری از آن‌ها کاری مشکل است. حملات خارجی حملاتی هستند که توسط یک یا چند گره از خارج شبکه انجام می‌شود و و اکثر اقدامات امنیتی در مقابل این‌گونه حملات اعمال می‌شوند. دیدگاه دیگر دسته بندی بر حسب فعال و یا غیر فعال بودن حمله است. حملات غیر فعال حملاتی هستند که در آن‌ها حمله کننده به داده‌های عبوری گوش داده و آن‌ها را استراق سمع می‌کند ولی در حملات فعال کننده این داده‌ها را به نفع خود تغییر می‌دهد. دیدگاه بعدی دسته بندی از جهت لایه‌های شبکه ای مورد حمله می‌باشد یعنی حمله می‌تواند بر روی لایه‌های فیزیکی شبکه،**MAC** ، شبکه و یا کاربرد صورت می‌گیرد.

مشکلات امنیتی در مسیر یابی در شبکه‌های موردی به سه دسته عمده تقسیم می‌شود تغییر، جعل هویت، و جعل.البته گونه های دیگری از حملات که منجر به ممانعت از سرویس می‌شوند مانند شرکت نکردن در عملیات مسیر یابی یا قطع ارتباط وجود دارند که در تمامی پروتکل‌های مسیر یابی وجود دارند و تنها راه جلوگیری از آنها پیدا کردن گره متخاصم می باشد.

در این پایان نامه انواع پروتکل‌ها و الگوریتم‌های مسیر یابی و مشکلات آن‌ها را بررسی و با نرم افزار**ns۲** شبیه سازی می‌کنیم و با استفاده از نتایج به دست آمده به ارزیابی هر یک از پروتکل‌ها می‌پردازیم.

خروجی پروژه:

در این پایان نامه بر مبنای کیفیت اندازه گیری در مطابقت با **[RFC ۲۵۰۱]** سه پروتکل مسیریابی **OLSR** و**AODV** و**DSR** برای شبیه سازی و ارزیابی انتخاب شده است. برای شبیه سازی از شبیه ساز **ns۲** استفاده می شود. در پایان با ارزیابی هریک از این پروتکل ها به نقاط ضعف و قوت هر یک از این پروتکل ها پی برده و پروتکلی که دارای عملکرد بالاتری می باشد برای مسیریابی در شبکه ارائه می شود.

نظـــــــــــر شـــــــورای تخصصی	نظر اول :	امضا مدیرگروه :