نشریه علمی‌ترویجی محاسبات نرم

سال ششم/ شمارهٔ اول/ بهار و تابستان ۱۳۹۶/ صفحهٔ ۳۸ـ۴۷

دریافت مقاله: ۱۳۹۳/۹/۹

پذیرش مقاله: ۱۳۹۶/۷/۱

ارائهٔ یک راهکار جدید در تکنیک به کار گرفته شده در پروتکل ARAN برای بهینه نمودن و افزایش کارایی مسیریابی امن در شبکه‌های سیار موردی

اعظم دوه لی[1*]، احمد شریف[2]

[1] باشگاه پژوهشگران جوان و نخبگان، واحد قم، دانشگاه آزاد اسلامی، قم، ایران

Davahli@qom-iau.ac.ir

[2] گروه کامپیوتر، آموزشکده فنی حرفه‌ای سما، دانشگاه آزاد اسلامی واحد قم، قم، ایران

Sharif12@hotmail.com

چکیده

برای برقراری امنیت در مسیریابی در شبکه‌های موردی، پروتکل‌های مسیریابی امن متفاوتی ارائه شده‌اند. اما متأسفانه روش به کار گرفته شده در برخی از این پروتکل‌ها ناکارآمد بوده و برخلاف افزایش امنیت، باعث کاهش کارایی و بهینگی شده و یا اشکالات و نواقصی را به دنبال داشته‌اند. با مطالعهٔ پروتکل‌های مسیریابی امن بسیاری، نتایج حاصل از مطالعات نشان داد که ARAN نسبت به اکثر آن‌ها سرویس‌های امنیتی تشخیص هویت و عدم انکار را با استفاده از تصدیق‌های رمزنگاری به‌صورت مطمئن و امن‌تری ایجاد کرده است و همچنین در برابر حملات گره‌های بدخواه مقاوم می‌باشد. در نتیجه به‌طور کلی امنیت خوبی را اعمال نموده است. اما تکنیک به کار گرفته شده در آن برای برقراری امنیت، علاوه بر مصرف انرژی زیاد (که یکی از محدودیت‌های اصلی شبکه‌های بی‌سیم است) با افزایش سایز بسته‌های مسیریابی، نرخ سربار را نیز افزایش داده و در نتیجه افزایش تأخیر و کاهش سرعت را نیز به دنبال داشته است. بنابراین ما در این مقاله ابتدا به معرفی ARAN پرداخته و سپس نشان داده‌ایم که اگرچه این پروتکل در عملیات مسیریابی در شبکه‌های موردی، امنیت را ایجاد نموده است، تکنیک به کار گرفته شده در آن برای برقراری امنیت علاوه بر مصرف انرژی زیاد با افزایش سایز بسته‌های مسیریابی، نرخ سربار را نیز افزایش داده و در نتیجه افزایش تأخیر و کاهش سرعت را نیز به دنبال داشته است. ما در این مقاله با ارائهٔ راهکاری جدید به‌جای تکنیک به کارگرفته شده در ARAN، سعی در برطرف نمودن مشکلات و ناکارآمدی آن نموده و آن را بهینه و کارآمدتر کرده‌ایم، به‌طوری که نتایج حاصل از شبیه‌سازی نشان می‌دهد که اعمال روش پیشنهادی ما در این الگوریتم با کاهش اندازهٔ بسته‌های مسیریابی و نرخ سربار حاصل از آن باعث کاهش میزان مصرف انرژی شده و همچنین زمان احراز هویت و به‌دنبال آن زمان مسیریابی را نیز کاهش داده است.

واژه‌های کلیدی: شبکه‌های سیار موردی، امنیت، پروتکل ARAN، احراز هویت، افزایش کارایی.

۱. مقدمه

شبکه‌های سیار موردی به‌علت ویژگی‌های خاصی [۱] که در انجام عملیاتشان دارند و نیز نحوهٔ قرارگیری‌شان، اغلب به شبکه‌های بدون ساختار، خودکار و خود سازمان‌دهنده معروف‌اند. شبکهٔ سیار موردی شامل تعدادی گره سیار بی‌سیم است که می‌توانند بدون استفاده از زیرساختار یا هر مدیریت مرکزی با همدیگر ارتباط برقرار کنند. به‌طور کلی می‌توان تمامی وسایلی را که به‌صورت بی‌سیم و بدون هیچ ایستگاه مرکزی به هم متصل شده‌اند، به‌عنوان گره‌های شبکه‌های سیار در نظر گرفت. به‌دلیل متحرک بودن گره‌ها، مسیریاب‌ها در این گونه شبکه‌ها نیاز دارند که به‌طور خودکار تغییرات توپولوژی را منعکس کنند. همچنین، ممکن است در هر لحظه گره‌های جدیدی به شبکه اضافه یا گره‌هایی از شبکه حذف شوند یا اینکه بعضی از گره‌ها خود را به حالت خاموشی درآورند. بنابراین در شبکه‌های سیار موردی، توپولوژی شبکه به‌طور مداوم در حال تغییر است. به‌دلیل این ویژگی‌های خاص، شبکه‌های سیار موردی علاوه بر مواجهه با مشکلاتی از قبیل منابع انرژی، محدودیت پردازش و محدودهٔ ارتباطی محدود با مشکل اصلی مسیریابی پویا مواجه‌اند. طراحی پروتکل‌های مسیریابی امن برای چنین شبکه‌هایی [۲] چالش بیشتری نسبت به شبکه‌های سیمی دارد. بنابراین در این شبکه‌ها به شدت نیاز به استفاده از پروتکل‌های مسیریابی کارآمد و بهینه برای انتقال اطلاعات به‌صورت مؤثر و بهینه در شبکه احساس می‌شود [۱ و ۳]. در این شبکه‌ها به‌منظور گسترش محدودهٔ ارتباطی گره‌ها (فراتر از یک گام)، از الگوریتم‌های مسیریابی پیکربندی‌شده استفاده می‌شود [۴]. ویژگی اساسی این الگوریتم‌ها، قابلیت تشکیل مسیر با وجود توپولوژی پویاست. چون در این شبکه‌ها گره‌ها به‌صورت مسیریاب عمل می‌کنند، این پروتکل‌ها روی بسته‌های داده‌ای که از آن‌ها عبور می‌کنند، کنترل کامل دارند [۵]. اکثر پروتکل‌های مسیریابی امن [۶ و ۷] ارائه‌شده، برای پاسخ به نیازمندی‌های امنیتی [۸ و ۹] از الگوریتم‌های رمزنگاری [۱۰] استفاده می‌کنند. یکی از این پروتکل‌ها ARAN[1] [۱۱] می‌باشد که در جهت برقراری امنیت در پروتکل‌های مسیریابی ناامن AODV[2] [۱۲ـ۱۴] و DSR[3] [۱۴ـ۱۶] ارائه شده است. ARAN برای ایجاد امنیت از تصدیق رمزنگاری استفاده می‌کند. این پروتکل شامل یک فرایند تصدیق اولیه است که تشخیص هویت را به‌صورت انتها به انتها تضمین می‌کند. کشف مسیر را با پخش همگانی نمودن پیام کشف مسیر (RDP) از یک گره مبدأ که با تک‌پخشی گره مقصد، پاسخ (REP) داده می‌شود، انجام می‌دهد. بنابراین پیام‌های مسیریابی در هر گام از مبدأ تا مقصد تشخیص هویت می‌شوند که این خود باعث شناسایی و مقابله با گره‌های بدخواه [۱۷ و ۱۸] می‌گردد. اما نتایج آزمایش‌ها نشان داده که این پروتکل برای اعمال احراز هویت، مراحل تصدیق رمزنگاری طولانی و بسته‌های مسیریابی بزرگی دارد که این‌ها باعث افزایش زمان مسیریابی شده و نرخ سربار مسیریابی را نیز افزایش داده است که به‌معنای کاهش بهینگی و کارایی است. ازاین‌رو ما در این پروتکل برای اعمال احراز هویت، به‌جای استفاده از تکنیک تصدیق رمزنگاری طولانی در مسیریابی، از یک روش جدید استفاده کرده‌ایم که سعی کرده است عملیات تکراری و طولانی و زمان مصرفی را کاهش و از طرف دیگر نرخ ارسال، بهینگی و کارایی را افزایش دهد. راهکار ارائه‌شده مبتنی بر یک جدول است که برای مسیریابی از تصدیق‌های (مسیرهای) ذخیره‌شده (به‌جای انجام مراحل تصدیق در هر مرحله از مسیریابی) استفاده می‌کند. در روش ارائه‌شده برای تمام مسیرهای موجود، جدول مسیریابی نیز بروزرسانی می‌شود تا در صورت اضافه شدن یا حذف گره‌ها (تغییر مسیر) عمل تصدیق و مسیریابی دچار خطا یا اشتباه نگردد. از آنجایی که عملیات احراز هویت بدین صورت است که با ورود هر گره و درخواست تصدیق از سرور T، سرور T ابتدا گره درخواست‌نموده را احراز هویت کرده و سپس در صورت تشخیص بدخواه نبودن آن، تصدیق و کلیدی را به آن گره تخصیص داده و در نهایت آن گره را به همراه

1. A Secure Routing Protocol for Ad Hoc Networks
2. Ad hoc On-Demand Distance Vector
3. Dynamic Source Routing Protocol

پارامترهایش، در رکوردی از جدول (۱) ثبت می‌کند، این امکان که گرهی بدخواه بتواند جدول را به‌صورت نامعتبر بروزرسانی نماید، وجود ندارد.

در این جدول، هر گره که بعد از احراز هویت توسط سرور نگهداری می‌شود تا برای ارسال بسته به گرهی در یک محدودهٔ خاص، نیاز به احراز هویت بسته در هر بار مسیریابی نباشد. نتایج حاصل از پیاده‌سازی این روش نشان می‌دهد که با اعمال این تکنیک و کاهش تعداد مراحل تصدیق و اندازهٔ بسته‌های مسیریابی علاوه بر کاهش مصرف انرژی و نرخ سربار، سرعت مسیریابی را نیز افزایش داده است. سازمان‌دهی این مقاله به این صورت است که ابتدا در بخش دوم به معرفی و بررسی برخی از پروتکل‌های مسیریابی امن در شبکه‌های سیار موردی پرداخته و سپس در بخش سوم به‌طور مختصر، پروتکل ARAN را مورد مطالعه و بررسی قرار داده و به معرفی مشکلات، معایب و مزایای روش مورد استفاده در آن پرداخته و سپس در مرحلهٔ چهارم، تکنیک پیشنهادی خود را برای بهینه‌تر و کارآمدتر نمودن مسیریابی امن در ARAN ارائه نموده‌ایم. در بخش پنجم نتایج حاصل از شبیه‌سازی را برای مقایسهٔ بین روش قبلی و روش پیشنهادی ارائه داده و نتایج و ارزیابی‌های به‌دست‌آمده از به‌کارگیری روش پیشنهادی در ARAN را نشان داده‌ایم. در انتها نیز نتیجه‌گیری کلی را ارائه کرده‌ایم.

۲. پروتکل‌های مسیریابی امن

دو گروه مهم از پروتکل‌های مسیریابی در شبکه‌های سیار موردی شامل پروتکل‌های امن و ناامن هستند. اکثر پروتکل‌های مسیریابی مانند AODV و DSR و DSDV[1] [۱۹] بدون در نظر گرفتن امنیت طراحی شده‌اند. اما به‌دلیل مشکلات و محدودیت‌های ذکرشده، مسیریابی در شبکه‌های سیار موردی با دو مشکل مواجه است: اول آنکه باید تضمین شود که داده‌ها به‌طور امن از طریق گره‌های معتمد مسیریابی می‌شوند و دوم امنیت پیغام پروتکل‌های مسیریابی است. بنابراین از آنجایی که امنیت پروتکل‌های مسیریابی در سراسر شبکهٔ موردی امری ضروری است، پروتکل‌های مسیریابی امن متفاوتی برای استفاده در شبکه‌های موردی ارائه شده‌اند [۲۰ و ۲۱] و هریک از آن‌ها نیازمندی‌های امنیتی متفاوتی را ارائه نموده‌اند که ما در اینجا به معرفی برخی از آن پروتکل‌های مسیریابی پرداخته‌ایم. پروتکل ROS[2] [۲۲] یک بستهٔ بدخواه [۱۹ و ۲۰] را برحسب یک پارامتر جدید (T_{UTI}) که یک فاصلهٔ زمانی بین بروزرسانی‌های متوالی در جدول مسیریابی برای همان مقصد است تشخیص می‌دهد. و آن بستهٔ مشکوک را به‌جای آنکه با همهٔ بسته‌های مسیریابی دریافتی‌اش چک کند، با گام قبلی یا با همسایگان محلی‌اش چک می‌کند و به موجب آن نرخ سربار مسیریابی برای ارتقای کارایی شبکه کاهش می‌یابد. پروتکل SEAD[3] [۲۳] از زنجیرهای درهم یک‌طرفهٔ کارا و درخت‌های درهم Markle [۲۴] استفاده می‌کند. برای اجتناب از حلقه‌های مسیریابی با مدت حیات طولانی در SEAD از شماره‌های ترتیب مقصد استفاده شده است. همچنین از این شماره‌های ترتیب مقصد برای محافظت در برابر حملات Replay در پیام‌های بروزرسانی مسیریابی در SEAD استفاده می‌شود. در پروتکل SEAD از پارامتری به نام Average weighted settling time در ارسال رکوردهای بروزرسانی‌های شده مورد استفاده قرار گرفته است. همچنین در این پروتکل وقتی یک گره تشخیص می‌دهد که اتصال گام بعدی تا مقصد قطع شده است، شماره ترتیب را برای آن مقصد با تنظیم مقدار متریک به بی‌نهایت در آن ورودی در جدول مسیریابی‌اش افزایش نمی‌دهد. بدین صورت از مشکل «شمارش تا بی‌نهایت» نیز جلوگیری می‌شود. در پروتکل SAODV[4] [۲۵] مزایای خلاصه پیام با کلید رمز برای مخفی نگه داشتن اطلاعات همهٔ فیلدهای پیام‌ها با استفاده از وظایف خلاصه پیام‌های متفاوت در نظر گرفته شده است که خیلی مؤثر است و یک راه حل امنیتی با مصرف انرژی کمتر برای شبکه‌های موردی می‌باشد. این پروتکل مبتنی بر این فرض است که هر گره دارای کلید عمومی تأییدشده توسط تمام گره‌های شبکه است. مالک کلیدهای عمومی تأییدشده، گره‌های میانی را برای تصدیق تمام بسته‌های

1. Destination-Sequenced Distance Vector

2. Resiliency Oriented Secure
3. Secure Efficient Ad hoc Distance vector
4. Secure Ad hoc On-Demand Distance Vector

مسیریابی در حال ارسال، فعال می‌سازد. همچنین این گره‌ها نیازمند استفاده از روش مدیریت کلید[۱] است. MAODV[۲] [۲۶] نیز یکی دیگر از پروتکل‌های مسیریابی امن در شبکه‌های موردی می‌باشد که از الگوریتم SHA-1 [۲۷] استفاده کرده است و براساس ارتباطات گروهی و استفاده از روش پخش همگانی [۲۸ـ۳۰] عمل می‌کند و انتقال و مسیریابی بسته‌ها به چندین مقصد با منابع شبکه‌ای کمتر را مجاز می‌دارد. این پروتکل بیشتر به مسئله افزایش نرخ اتصال توجه کرده است. در این پروتکل، حرکت گره‌ها براساس سرعت و مکان پیش بینی می‌شود و قبل از آنکه اتصالی قطع گردد، گره‌ها مسیر رو به بالای خود را با دیگر مسیرهای موجود جایگزین می‌کنند. پروتکل SDSDV[۳] [۳۱] نیز مثل SEAD از روش زنجیر در هم استفاده می‌کند. اما در SDSDV هر گره دو زنجیر درهم یک‌طرفه را برای ارتباط با گره دیگر در شبکه نگهداری می‌کند و همچنین دو فیلد اضافه در آن به نام‌های AL و AC وجود دارد که به‌ترتیب یکی برای حفاظت در برابر حمله کاهش متریک[۴] [۳۱] و دیگری برای حفاظت از حمله افزایش متریک[۵] [۳۱] استفاده می‌شود. بنابراین برای یک سیستم با n گره، هر گره شامل 2n زنجیر درهم است. این‌ها به هر ورودی از بسته‌های بروزرسانی اضافه می‌شوند که مقادیر درهم[۶] [۳۱] را حمل می‌کنند. با استفادهٔ مناسب از عناصر زنجیره‌های درهم، شمارهٔ ترتیب و مقادیر متریک در یک مسیر، از تحریف شدن جلوگیری می‌شود. در پروتکل SecMR[۷] [۳۲] مجموعه کاملی از مسیرهای موجود node-disjoint , non-syclic را بین یک گره مبدأ و یک گره مقصد کشف می‌کند. این پروتکل در دو فاز کار می‌کند: در فاز اول احراز هویت همسایگی را انجام می‌دهد که شامل احراز هویت بحرانی غیر همزمان گره‌های همسایه است و در فاز دوم، عمل کشف مسیر و نگهداری مسیر صورت می‌گیرد که ایجاد و نگهداری مسیرهای فعال را شامل می‌شود. در پروتکل SDAR[۸] [۳۳]، هدف اصلی پروتکل SDAR آن است که با استفاده از رهیافت مسیریابی onion و سیستم مدیریتی اعتبار به گره‌های میانی قابل معتمد اجازه دهد که در پروتکل ساخت مسیر، بدون به مخاطره انداختن گمنامی گره‌های ارتباطی شرکت کنند. این پروتکل، زمانی رفتاری را به‌صورت بدخواهانه تشخیص می‌دهد که یک گره بدون آنکه بسته‌ای را ارسال کند، آن را حذف نماید یا به‌صورت بدخواهانه بروزرسانی کند [۳۳]. در این پروتکل برای ارسال داده‌ها به‌طور گمنام به گره گیرنده (R) یک گره فرستنده (S) یک مسیر قابل معتمد و گمنام را کشف و ایجاد می کند که دو گره را به هم متصل می‌کند. هر دو پروسهٔ کشف مسیر و ایجاد مسیر باید به‌صورت محرمانه و بدون به خطر انداختن گمنامی گره‌های ارتباطی انجام شوند.

۳. بررسی روش و تکنیک به کار گرفته شده در پروتکل ARAN

۳ـ۱. تصدیق نمودن سرور و جزئیات چگونگی تصدیق

پروتکل ARAN نیازمند استفاده از یک سرور T با تصدیق مورد اطمینان است که کلید عمومی شناخته شده برای همه گره‌های معتبر است. قبل از ورود به شبکه Ad hoc هر گره باید یک درخواست تصدیق از T داشته باشد و هر گره دقیقاً یک تصدیق را بعد از تعیین هویتش از T دریافت می‌کند.

S ↔ A ↔ B ↔ M ↔ C ↔ D ↔ X

شکل (۱) [۸]: یک نمونه از شبکهٔ موردی

گره A، تصدیق را از T دریافت می‌کند:

$$T \rightarrow A: CERT_A = [IPA, K_{A+}, t, e]\ K_{T-} \qquad (۱)$$

تصدیق شامل پارامترهای IP_A که آدرس ip مربوط به A و K_A که کلید عمومی A و t که مهر زمانی و زمان انقضای تصدیق e می‌باشد.

۱. در پروتکل‌ها و الگوریتم‌های رمزنگاری برای عملیات رمزنگاری و رمزگشایی نیازمند استفاده از یک کلید رمز هستیم. در نتیجه امنیت الگوریتم‌ها وابسته به پنهان و مخفی نگه داشتن همین کلید رمز است. بنابراین در الگوریتم‌های مسیریابی‌ای که از رمزنگاری استفاده می‌کنند نیازمند مدیریت کلید برای مخفی و پنهان نگه داشتن آن می‌باشیم.

2. Multicast Ad hoc On-Demand Distance Vector
3. Secure Destination-Sequenced Distance Vector
4. Decreasing metric attack
5. Increasing metric attack
6. Hash values
7. Secure multipath routing
8. Secure Distributed Anonymous Routing

۳ـ۲. کشف مسیر تصدیق‌شده

گره مبدأ A با پخش همگانی کردن یک بسته کشف مسیر به همسایگانش مسیر تا مقصد X را معرفی می‌کند:

$$A\rightarrow \text{brdcast: } [RDP, IP_x, CERT_A, N_A, t]\ K_A- \quad (۲)$$

RDP شامل یک بسته شناسه نوع ("RDP")، IP آدرس مقصد (IPx) ، تصدیق مربوط به گره A ($CERT_A$) و یک nonce (N_A) و یک زمان جاری t می‌باشد که همگی با کلید اختصاصی A علامت‌گذاری شده‌اند. وقتی یک گره پیام RDP را دریافت می‌کند، از نقطهٔ دریافت پیام، یک مسیر معکوس به‌سمت مبدأ ایجاد می‌کند. گره دریافت‌کننده از یک کلید عمومی A برای اعتبار دادن به امضا و بررسی کردن تصدیق مربوط به A استفاده می‌کند. گره دریافت کننده همچنین چندتایی (N_A,IP_A) را برای بازبینی اینکه آیا RDP را پردازش نکرده است، استفاده می‌کند. در غیر این صورت گره محتوای پیام را علامت می‌زند و تصدیق خودش را به آن اضافه نموده و پیام را رو به جلو به همه گره‌های مجاورش پخش همگانی می‌کند. امضا از حملهٔ جعل هویت که ممکن است مسیر را تغییر دهند یا حلقه‌هایی را ایجاد کنند، جلوگیری می‌کند. B همسایه‌ای است که پخش همگانی مربوط به RDP را از گره A دریافت نموده است و دوباره پخش همگانی را انجام می‌دهد:

$$B\rightarrow \text{brdcast: } [[RDP, IP_x, CERT_A, N_A, t]\ K_A\text{ -}]\ KB\text{ - },\ CERT_B \quad (۳)$$

به محض دریافت RDP همسایه B یعنی C امضا را با تصدیق معین تأیید می‌کند و امضای B را حذف می‌کند و B را به‌عنوان گره قبلی خود ثبت می‌کند و علامت می‌زند و محتوای پیام پخش همگانی‌شده را در آغاز کار توسط A اضافه می‌کند. تصدیق خود را به آن اضافه نموده و پیام را رو به جلو پخش همگانی می‌کند. سپس گره C نیز مجدداً RDP را پخش همگانی می‌کند. هر گره در امتداد مسیر این مرحله از معتبرسازی امضای گره قبلی را تکرار می‌کند و تصدیق و امضای گره قبلی را حذف می‌کند و IP آدرس گره قبلی را ثبت می‌کند و محتوای اصلی پیام را علامت‌گذاری می‌کند و تصدیق خودش را اضافه نموده و پیام را به سمت رو به جلو پخش همگانی می‌کند:

$$C\rightarrow \text{brdcast: } [[RDP, IP_x, CERT_A, N_A, t]\ K_A\ –]\ KC\text{ - },\ CERT_C \quad (۴)$$

۳ـ۳. ایجاد مسیر بررسی‌شده و تعیین هویت شده

سرانجام پیامی که توسط مقصد X دریافت می‌شود به اولین RDP که آن را دریافت می‌کند برای یک مبدأ و nonce معین پاسخ می‌دهد. به‌دلیل اینکه RDP شامل یک شماره hop یا مسیر مبدأ ثبت‌شدهٔ مشخص نیست و به‌علت اینکه پیام‌ها در هر hop علامت‌گذاری می‌شوند، گره‌های بدخواه فرصتی برای هدایت تغییر مسیر مجدد ترافیک از طریق بهره‌برداری ندارند. بعد از دریافت RDP مقصد یک بسته پاسخ REP را به‌سمت عقب در طول مسیر معکوس و به‌سمت مبدأ تک‌پخشی می‌کند. اولین گرهی که REP ارسال‌شده توسط گره X را دریافت می‌کند، گره D می‌باشد.

$$X\rightarrow D: [REP, IP_A, CERT_x, N_A, t]\ K_x- \quad (۵)$$

REP شامل یک شناسه نوع بسته ("REP")، IP آدرس A (IPa) ، تصدیق متعلق به X (CERTx) و nonce ، timestamp مربوطه است که توسط A ارسال می‌شود. گره‌هایی که REP را دریافت می‌کنند، بسته را از مکانی که آن‌ها RDP اصلی را دریافت کرده‌اند به‌سمت عقب و گره‌های قبلی ارسال می‌کنند. هر گره در طول مسیر برگشت به مبدأ، قبل از ارسال REP به hop بعدی، REP را علامت‌گذاری می‌کند و تصدیق خودش را به آن اضافه می‌کند.

$$D\rightarrow C: [[REP, IP_A, CERT_x, N_A, t]\ K_x\text{-}]\ K_D\text{- },\ CERT_D \quad (۶)$$

C امضای D را روی پیام‌های دریافت‌شده تأیید می‌کند. امضا و تصدیق را حذف می‌کند و سپس محتوای پیام را علامت می‌زند و تصدیق خودش را قبل از تک‌پخشی نمودن REP به B به آن اضافه می‌کند.

$$C\rightarrow B\text{:s } [[REP\ ,\ IPa\ ,\ CERT_X\ ,N_A\ ,t\ ]K_x\text{- }]K_C\text{-},CERT_C \quad (۷)$$

هر گره هنگامی که REP به مبدأ باز می‌گردد، nonce و امضای hop قبلی را چک می‌کند که این اجتناب می‌کند از حملات گره‌های بدخواه که باعث ایجاد مسیرهایی با جعل

هویت می‌شود و دوباره ارسال شدن (replay) پیام‌های X. وقتی که مبدأ REP را دریافت می‌کند، امضای مقصد و nonce را که توسط مقصد برگردانده می‌شود، بررسی می‌کند.

۴ـ۳. بررسی کارایی و سرویس‌های امنیتی ایجادشده توسط پروتکل ARAN

نتایج نشان داده است که نرخ تحویل داده و بارگذاری مسیریابی در ARAN خیلی بیشتر از حالت ناامن این پروتکل [۳] می‌باشد که این منجر به امنیت داده می‌شود. ARAN در مقایسهٔ با پروتکل مسیریابی ناامنش یعنی AODV [۱۰ و ۱۱] دارای این مزیت است که از حملات جعل هویت و جعل شدن هریک از گره‌های مبدأ یا مقصد جلوگیری می‌کند و مشخص می‌کند که همهٔ فیلدهای بسته‌های RDP و REP بین مبدأ و مقصد بدون تغییر باقی می‌مانند. گره‌های بدخواه [۱۵ و ۱۶] در پروتکل AODV سعی می‌کنند که مسیریابی را از میان خود عبور دهند؛ یعنی جریان مسیر را طوری تغییر می‌دهند تا بتوانند بسته‌های داده را شنود نموده یا اینکه دور بریزند، در حالی که این بهره‌برداری‌ها با استفاده از پروتکل ARAN امکان‌پذیر نیست. از جمله سرویس‌های امنیتی دیگر که این پروتکل علاوه بر احراز هویت ارائه کرده، سرویس عدم انکار و جامعیت است. در واقع پروتکل مسیریابی امن ARAN یک پروتکل ساده است که نیازی به کار اضافی مهمی از گره‌ها ندارد و حملات را محدود نموده، اما هزینهٔ تأخیر در کشف مسیر در این پروتکل به‌دلیل محاسبات رمزنگاری بیشتر است که این خود، اشکالات و ناکارآمدی‌های دیگری را به‌دنبال دارد.

۴. اشکالات و معایب پروتکل ARAN

چون این پروتکل از روش رمزنگاری استفاده می‌کند و مبتنی بر تصدیق است، هر گره در ارسال بسته‌های RDP,REP,REE باید آن‌ها را علامت‌گذاری کند. بدین صورت که ابتدا تصدیق و کلید عمومی گره قبلی را که ارسال‌کنندهٔ آن بسته است، بررسی نموده آنگاه در صورت مجاز بودن آن را حذف کرده، سپس تصدیق و کلید عمومی خودش را به بسته اضافه کند و در هر مرحله از ارسال نیز، محتوای اصلی پیام ([RDP, IP_X, $CERT_A$, N_A, t]KA-) را به آن بسته اضافه کند که این در مراحل قبلی نیز تکرار شده است. بنابراین تعداد گام و مراحلی را که هر گره با استفاده از روش به کار گرفته شده در ARAN، باید در امتداد مسیر طی نماید عبارت‌اند از:

۱. اعتبارسنجی امضای گره قبلی
۲. برداشتن امضا و تصدیق گره قبلی
۳. ضبط آدرس IP گره قبلی
۴. علامت‌گذاری محتوای اصلی پیام
۵. اضافه کردن تصدیق خودش
۶. جلورانی کردن پخش پیام

نتایج حاصل از پیاده‌سازی ARAN، نشان داده که این مراحل طولانی باعث مصرف انرژی زیادی می‌شود که درخصوص شبکه‌های موردی که با محدودیت انرژی مواجه‌اند ناخوشایند است. و همچنین درج سرآیندهای مختلف به بستهٔ ارسالی در هر گام، موجب افزایش سایز بسته‌های مسیریابی و سربار می‌شود. بنابراین به‌طور کلی می‌توان بیان کرد که تکنیک رمزنگاری و انجام محاسبات طولانی به کار گرفته شده در این پروتکل، نه فقط موجب افزایش هزینه تأخیر در کشف مسیر شده است، بلکه تخصیص کلید به گره‌ها، سربار کنترلی را هم افزایش داده است، و در نهایت تمامی این موارد علی‌رغم اعمال نیازمندی‌های امنیتی در طول کشف مسیر، موجب ناکارآمدی‌هایی از جمله تأخیر در عملیات مسیریابی و افزایش افزونگی و نیز افزایش مصرف انرژی شده است. لذا برای رفع مشکلات مذکور و بهینه نمودن عملیات مسیریابی توسط ARAN، در بخش بعدی به ارائهٔ تکنیکی مؤثر و کارآمد پرداخته‌ایم.

۵. ارائهٔ راهکار پیشنهادی در پروتکل ARAN

در این روش فرض می‌کنیم که سرور T که وظیفهٔ تخصیص تصدیق به گره‌ها را زمانی که آن‌ها وارد شبکه شده و درخواست تصدیق می‌نمایند بر عهده دارد، دارای یک جدول نیز می‌باشد. بنابراین این سرور در هنگام اختصاص تصدیق به هر گره، آن را به همراه تصدیقش درون یک رکورد از این جدول نیز ثبت می‌کند. در واقع هر رکورد از این جدول که درون سرور T قرار دارد، متعلق به یک گره است که توسط

سرور تصدیق شده است. جدول و شرح هریک از فیلدهای مربوط به آن در زیر نشان داده شده است.

جدول (۱): جدول پیشنهادی درون سرور T

NODE	$NONCE_X$	IP_X	K_X	t_X	e_X
A	$NONCE_A$	IP_A	KA+	t_A	e_A
B	$NONCE_B$	IP_B	KB+	t_B	e_B
C	$NONCE_C$	IP_C	KC+	t_C	e_C
D	$NONCE_D$	IP_D	KD+	t_D	e_D

NODE: گرهی که تصدیق را توسط سرور T دریافت نموده و از نظر سرور گرهی معتبر است.

$NONCE_X$: nonce x می‌باشد که هروقت گره فرایند کشف مسیر را اجرا می‌کند، به‌طور یکنواخت آن را افزایش می‌دهد. (به‌ازای هر رجوع به گره A در جدول یک واحد به آن اضافه می‌شود).

IP-ADDRESS: آدرس IP مربوط به گره X را نشان می‌دهد.

KEY (K_X): کلید عمومی تخصیص‌یافته به گره X را نشان می‌دهد.

Timestamp (t_x): زمانی که تصدیقی برای گره X ایجاد می‌شود.

تصدیق expire(e_x): زمانی که تصدیق ایجادشدهٔ گره X منقضی می‌شود.

(N_A, IP_A): برای بازبینی اینکه آن هنوز RDP را پردازش نکرده است.

۵ـ۱. شرح عملکرد روش پیشنهادی با استفاده از جدول۲

عملیات احراز هویت بدین صورت است که با ورود هر گره و درخواست تصدیق از سرور T، سرور T ابتدا گره درخواست‌نموده را احراز هویت کرده و سپس در صورت تشخیص بدخواه نبودن آن گره، تصدیق و کلیدی را به آن گره تخصیص داده و در نهایت آن گره را به همراه پارامترهای شرح داده شده در بالا، در رکوردی از جدول (۲) ثبت می‌کند. گره‌های درج‌شده در جدول، از این تصدیق‌ها برای احراز هویت خودشان در شبکه استفاده می‌کنند؛ مثلاً وقتی که گره مبدأ A با پخش همگانی نمودن یک بسته کشف مسیر RDP به همسایه‌هایش مسیر تا مقصد X را معرفی می‌کند:

A ⟶ پخش همگانی [RDP]

(بستهٔ درخواست RDP شامل بسته‌ای با آدرس IP مبدأ و مقصد و ID درخواست و شماره‌های ترتیب و تعداد گام است.) در این هنگام ابتدا همسایهٔ A به سرور رجوع نموده تا اینکه تصدیق مربوط به A را بررسی کند. آنگاه اگر تصدیق مربوط به A را در جدول نیابد، این بدان معناست که گره A یک گره نامعتبر بوده است. در نتیجه بستهٔ دریافتی از A را دور می‌اندازد، در غیر این صورت این بسته را دوباره به همسایه‌هایش پخش همگانی نموده و IP آدرس گره قبلی را نیز ثبت می‌کند (برخلاف روش قبل که در آن بعد از آنکه گره معتبر شناخته شد، تصدیق گره قبلی را حذف کرده و تصدیق خودش را به آن اضافه می‌کند و IP آدرس گره قبلی را هم ثبت می‌کند.) و این روال ادامه می‌یابد تا اینکه بسته به مقصد برسد. سرانجام پیامی که توسط مقصد X دریافت می‌شود، به اولین RDP که آن را دریافت نموده برای یک مبدأ معین پاسخ می‌دهد بدین صورت که بعد از دریافت RDP مقصد یک بسته پاسخ REP را به‌سمت عقب و در طول مسیر معکوس به‌سمت مبدأ تک‌پخشی (ارسال توسط مبدأ فقط برای یک مقصد) می‌کند. همچنین در این ارسال/پاسخ برخلاف روش قبلی، دیگر نیازی به اضافه نمودن محتوای اصلی پیام ([REP, I_{Pa}, $CERT_x$, $N_{A,t}$]) نیست.

در واقع اولین گرهی که REP ارسال‌شده توسط گره X را دریافت می‌کند، گره D می‌باشد:

X ⟶ D: [REP]

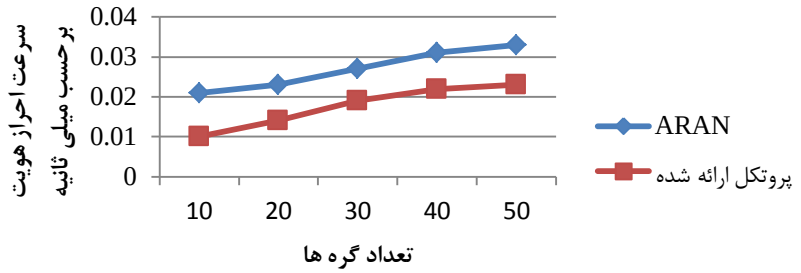
و C فقط امضای D را از طریق جدول موجود در سرور تأیید می‌کند و دیگر نیازی به عمل حذف نمودن امضا و تصدیق‌های مربوط به D و اضافه نمودن تصدیق و امضای خود قبل از تک‌پخشی کردن REP به گره B بر روی محتوای پیام را ندارد:

C ⟶ B: [REP]

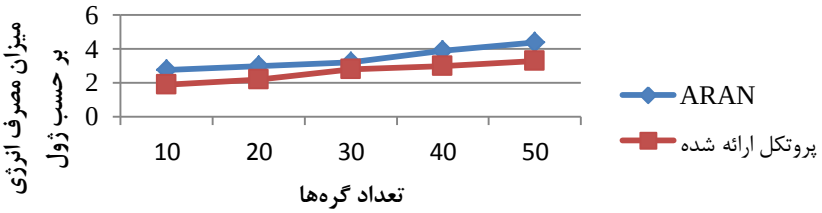
هر گره هنگامی که REP به مبدأ باز می‌گردد، nonce و امضای گام قبلی را از طریق جدول سرور چک می‌کند که این باعث ایجاد مسیرهایی با جعل هویت می‌شوند، و در نهایت

نیز هنگامی که مبدأ REP را دریافت کرد، امضای مقصد و nonce برگردانده‌شده توسط مقصد را بررسی می‌کند.

در این بهبود با اینکه همچنان این پروتکل از رمزنگاری استفاده می‌کند، دیگر لازم نیست که هر گره در ارسال بسته‌های RDP, REP,ERR آن‌ها را علامت‌گذاری کند و نیز نیازی به الحاق محتوای اصلی پیام که شامل نوع پیام و آدرس مقصد و اعتبار گره مبدأ و... نیست. بنابراین همان طور که نتایج حاصل از شبیه‌سازی در شکل‌های (۲) و (۳) نشان داده شده، این روش با کاهش عملیات مورد نیاز جهت تصدیق هویت، علاوه بر اعمال امنیت در مسیریابی، باعث افزایش سرعت مسیریابی و صرفه‌جویی در مصرف انرژی (که یکی از مهمترین دغدغه‌ها در شبکه‌های موردی می‌باشد) شده است.



شکل (۲): مقایسهٔ زمان مصرفی بین تکنیک قبلی و روش پیشنهادی اعمال‌شده در ARAN

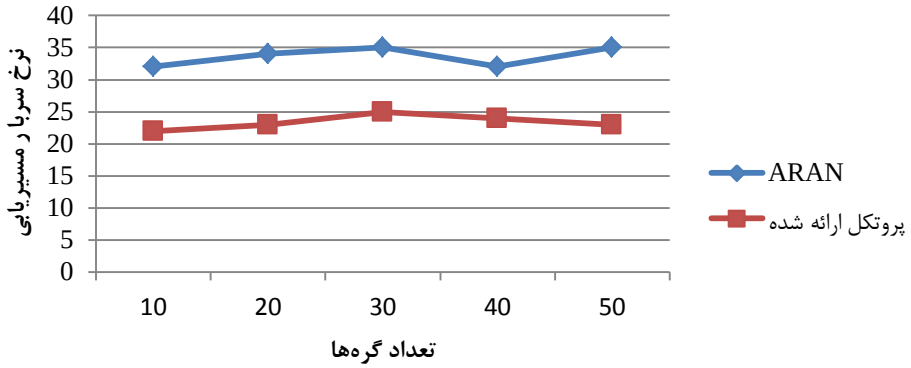


شکل (۳): مقایسهٔ انرژی مصرفی بین تکنیک قبلی و روش پیشنهادی اعمال شده در ARAN

از آنجایی که پروتکل ARAN نیازمند استفاده از یک سرور T با تصدیق مورد اطمینان می‌باشد که کلید عمومی شناخته‌شده برای همه گره‌های معتبر است، قبل از ورود به شبکهٔ Ad hoc هر گره باید یک درخواست تصدیق از T داشته باشد و هر گره دقیقاً یک تصدیق را بعد از تعیین هویتش از T دریافت می‌کند. بنابراین نه تنها هزینه‌های ارتباطی هر نود با سرور برای تأیید اصالت مورد بررسی در روش پیشنهادی نسبت به روش قبلی افزایشی نیافته، بلکه هزینه‌های ارتباطی‌ای که روش پیشنهادی به شبکه تحمیل می‌کند (به دلایل اینکه با کاهش اندازهٔ بسته‌های مسیریابی و نرخ سربار حاصل از آن باعث کاهش میزان مصرف انرژی شده و همچنین زمان احراز هویت و به‌دنبال آن زمان مسیریابی را نیز کاهش داده است، نسبت به روش قبلی بسیار کمتر شده است.

همچنین قابل ذکر است که با وجود اینکه جدول ارائه‌شده در سرور، خود دارای سربار می‌باشد، این سربار به چند دلیل نسبت به روش قبلی بسیار ناچیز است: ابتدا آنکه سرور در روش قبلی نیز موجود است فقط در این روش جدولی در آن درج می‌گردد؛ دوم آنکه همیشه با افزایش قابلیتی ممکن است قابلیتی دیگر را از دست بدهیم یا کاهش بیابد که این امر کاملاً واضح است و سوم آنکه پروتکل ARAN، سرویس‌های امنیتی، تشخیص هویت و عدم انکار را با استفاده از تصدیق‌های رمزنگاری از پیش تعیین‌شده فراهم می‌کند و همچنین در برابر حملات گره‌های بدخواه مقاوم بوده و نرخ تحویل را نیز افزایش می‌دهد. اما علی‌رغم سرویس‌های امنیتی‌ای که توسط این پروتکل ارائه شده است، تکنیک طولانی و ناکارآمد به کار گرفته شده در آن، باعث مصرف انرژی زیادی شده و سایز بسته‌های مسیریابی را نیز افزایش می‌دهد و به‌دلیل محاسبات و

رمزنگاری، هزینهٔ تأخیر در کشف مسیر و نیز سربار کنترلی نسبت به روش پیشنهادی بسیار افزایش می‌یابد و در نهایت زمان به‌دست‌آوردن مسیر نیز طولانی‌تر می‌شود.



شکل (۴): مقایسهٔ نرخ سربار بین تکنیک قبلی و روش پیشنهادی اعمال‌شده در ARAN

۵. نتیجه‌گیری و آینده کاری

پروتکل‌های مسیریابی زیادی در شبکه‌های سیار موردی معرفی شده‌اند که به‌دلیل امن نبودن آن‌ها، شبکه‌های موردی با انواع حملات مواجه بودند. برای رفع این مشکلات و برخورد با برخی از این حملات، پروتکل‌های امن مختلفی طراحی شده‌اند. از آنجایی که نتایج حاصل از مطالعات پروتکل‌های مسیریابی امن بسیار، نشان داد که ARAN نسبت به اکثر آن‌ها، سرویس‌های امنیتی تشخیص هویت و عدم انکار را با استفاده از تصدیق‌های رمزنگاری به‌صورت مطمئن و امن‌تری ایجاد کرده است و همچنین در برابر حملات گره‌های بدخواه مقاومت مناسب‌تری دارد و به‌طور کلی امنیت خوبی را ارائه نموده است اما تکنیک به کار گرفته‌شده در آن برای برقراری امنیت علاوه بر مصرف انرژی زیاد که یکی از محدودیت‌های اصلی شبکه‌های بی سیم می‌باشد، با افزایش سایز بسته‌های مسیریابی، نرخ سربار را نیز افزایش داده و در نتیجه افزایش تأخیر و کاهش سرعت را نیز به‌دنبال داشته است. بنابراین در این مقاله، به مطالعه و بررسی یکی از این پروتکل‌های امن پرداخته ایم و تکنیکی را در جهت بهبود و افزایش بهره‌وری و کارایی آن ارائه نموده‌ایم. این پروتکل امن سرویس‌های امنیتی تشخیص هویت و عدم انکار را با استفاده از تصدیق‌های رمزنگاری از پیش تعیین‌شده فراهم می‌کند و همچنین در برابر حملات گره‌های بدخواه مقاوم بوده و نرخ تحویل را نیز افزایش می‌دهد. اما علی‌رغم سرویس‌های امنیتی‌ای که توسط این پروتکل ارائه شده است، تکنیک طولانی و ناکارآمد به کار گرفته شده در آن، باعث مصرف انرژی زیادی شده و سایز بسته‌های مسیریابی را نیز افزایش می‌دهد و به‌دلیل محاسبات و رمزنگاری، هزینهٔ تأخیر در کشف مسیر و نیز سربار کنترلی افزایش می‌یابد و در نهایت زمان به‌دست‌آوردن مسیر نیز طولانی‌تر می‌شود. بنابراین در این مقاله، تکنیکی را در جهت بهبود و افزایش بهره‌وری و کارایی این پروتکل ارائه نموده‌ایم.

مراجع

[1] S. Corson and J. Macker, Mobile ad-hoc networking MANET: Routing Protocol Performance Issues and Evalution Consideration, IETF MANET, 1999.

[2] A. Khurram, Proposed Protocol for Secured Multi Path Routing in Ad hoc Networks, International Journal of Latest Trends in Engineering and Technology (IJLTET), vol. 5, 2015.

[3] R. Menchaca-Mendeza, J.J. Garcia-Luna-Aceves,Hydra: Efficient multicast routing in MANETs using sender-initiated multicast meshes, Pervasive and Mobile Computing, vol. 6, pp. 144-157, 2010.

[4] H. Al Amri, M. Abolhasan, T. Wysocki, Scalability of MANET routing protocols for heterogeneous and homogenous networks, Computers and Electrical Engineering vol. 36, pp.752–765, 2010.

[5] M. Abolhasan, T.Wysocki, E.Dutkiewciz, A review of routing protocols for mobile ad hoc networks, Elsevier J Ad Hoc Networks, vol. l2(1), pp.1–22, 2004.

[6] R. S. Lakshan, U. Madhur, J.K Kamran, Review of Security in Routing Protocols on Ad-Hoc Networks, SSRG International Journal of Mobile Computing & Application (SSRG-IJMCA), vol. 2 Issue pp.15-19, 2015.

[7]N. Arora1, K. Kishore Arora, P. Vyas, Survey of Security Enhancements in MANET Routing Protocols for Networking, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, 2016.

[8] S. Carter and A. Yasinsac, Secure Position Aided Ad hoc Routing Protocol, In Proceeding of the IASTED Conference on Communication and computer Network, 2002.

[9] Y. Desmedt, Some recent Aspect Of Threshold Cryptography, In Proceeding of the First
International Workshop on Information Security, springer-Verlag, pp. 158-173, 1998.

[10] M. Burmester and Y. Desmedt, Secure communication in an unknown network using certificates, Advances in Cryptology - Asiacrypt '99, Lecture Notes in Computer Science1716, pp. 274-287, 1999.

[11] K. sanzgiri, B. Dehill, B. Neil Levin, C. Shields, E. M.Belding-Royer,A Secure Routing Protocol for Ad hoc Networks.

[12] C.E. Perkins and E.M. Royer, Ad-Hoc On-Demand Distance Vector Routing, In Proceedings of IEEE WMCSA'-99, New Orleans, LA, Feb, pp.99-100,1999.

[13] C. Perkins, E. Belding-Royer, and S. Das, RFC 3561 - Ad hoc On-Demand Distance Vector
(AODV) Routing, Network Working Group, Request for Comments: 3561, 2003.

[14] H. Sharma, Analysis of Security Issues, Challenges and Current Trends in AODV and DSR, International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering Vol. 3, Issue 10, 2015.

[15]Johnson DB, Moltz DA, Brach J, The dynamic source routing protocol for multi-hop wireless Ad Hoc networks, In: EPC, editor, Ad Hoc Networking. Boston: Addison-wesley, PP.72 -139, 2001.

[16] Johnson D, Hu Y, Maltz D. The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4, RFC Editor, 2007.

[17] G. Padmavathi, D. Shanmugapriya, A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,(IJCSIS) International Journal of Computer Science and Information Security,2009.

[18] B. Sun, L. Osborne, Y. Xiao, S. Guizani, Intrusion Detection Techniques in Mobile Ad hoc AND WIRELESS SENSOR NETWORKS, IEEE Wireless Communications,5663,2007.

[19] C. E. Perkins and P. Bhagwat. Highly dynamic Destination-Sequenced Distance-Vector Routing DSDV for mobile Computers. In Precedings of the SIGcomm Conference on Communication, Architectures, Protocols and Application, 1994.

[20] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne, A secure on-demand routing protocol forad hoc networks. Proceedings of MOBICOM, vol 5.1, 2002.

[21] S. Carter and A. Yasinsac. Secure Position Aided Ad hoc Routing Protocol. In Proceeding of the IASTED Conference on Communication and computer Network, 2002.

[22] L. Mnickam J. Martin, S.Shanmugavel, Providing Routing security Using ROS Protocol in MANET and Performance Comparision AODV",Information Technology Journal 5(5), pp.656-663,2007.

[23] Ch. Hu Yih, B.Johnson David , P. Adrin, Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Elsevier Ad Hoc Netorks 175-192, 2003.

[24] R. Merkle, Protocols for public key cryptosystems, IEEE Symposium on Security and Privacy, 1980.

[25] K. Lakhtaria and B. N.Patel, S. G.prajapati and N.N.Jani,Security AODV for MANETsUsing Message Digest with Secret Key, International Journal of Network Security & Its Applications(IJNSA),Vol.1, No.3, 2009.

[26] M. Zhong, Y. Fu, X. Jia, MAODV multicast routing protocol based on node mobility prediction, In proceedings of International Conference on E -Business and E -Government (ICEE), pp. 1-4, 2011.

[27]N.Shanth and L.Ganesan, Security in Multicast Mobile Ad Hoc Networks, Ijcscsns Internatonal Journal of Compter Science and Network Security,Vol. 8, No.7, 2008.

[28] S.S. Manvi, M.S. Kakkasageri, Multicast routing in mobile ad hoc networks by using a multiagent system, International Journal of Information Science, Vol. 178, pp. 1611-1628, 2008.

[29] N.Fareena, A.S. Mala , k.Ramar, Mobility based energy efficient multicast protocol for MANET, In proceedings of ICMOC, vol. 38, pp. 2473 – 2483, 2012.

[30] J. Huang and Y. Liu, MOEAQ:A QoS-Aware Multicast Routing algorithm for MANET, Expert Systems with Applications, Vol. 37, No. 2, pp. 1391-1399, 2010.

[31] Jyu-Wei Wang and Hsing-Chung Chen and Yi-Ping Lin,A Secure DSDV Routing Protocol for Ad Hoc MobileNetworks, Fifth International Joint Conference on INC,IMS and IDS, 2009.

[32] R. Mavropodi and P. Kotzankolau and Ch Douligeris, a Secure Multipath Routing Protocol for Ad Hoc Networks, Vol. 5, pp.87-99, 2007.

[33] A. Boukerche,KH. EL-Khatib and Li Xu and L. Korba,A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks.