مجلهٔ علمی- پژوهشی
«مهندسی برق مدرس»
دورهٔ دهم، شمارهٔ ٤، زمستان ۱۳۸۹

طراحی، شبیه‌سازی و ارزیابی پروتکل وفقی امن مبتنی بر الگوی چندمسیریابی در شبکهٔ بی‌سیم سیار

منصور نجاتی جهرمی[1*]، علیرضا رضایی[2]

۱- استادیار، دانشگاه علوم و فنون هوائی شهید ستاری، تهران، ایران

۲- دانشجوی کارشناسی ارشد مخابرات رمز، دانشگاه علوم و فنون هوائی شهید ستاری

Nejati@aut.ac.ir

(دریافت مقاله: آبان ۱۳۸۹، پذیرش مقاله: اسفند ۱۳۸۹)

چکیده- در هر شبکه بی‌سیم سیار ایدئال، ویژگی‌هایی مانند توانایی کشف چندین مسیر برای تبادل اطلاعات، قابلیت اطمینان بالا، وقوع کمترین خطا، مقابله با تلاش مهاجرین برای شناخت و کشف مسیر، مورد توجه است. نزدیک شدن به این اهداف منجر به افزایش کارایی و ارتقای شبکه خواهد شد.

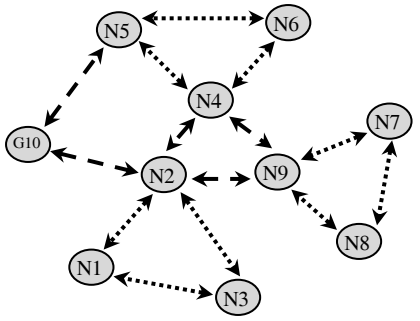
در این مقاله، پروتکلی طراحی و معرفی می‌شود که توانایی کشف چند مسیر برای تبادل اطلاعات با قابلیت اطمینان بالا را دارد. همچنین، شبکه طراحی شده مزیت‌هایی مانند مقاومت در برابر ایجاد خطا و کاهش اثر مهاجمان در طول فرایند شناخت و کشف مسیر و انتقال داده نیز دارد. این پروتکل امنیت شبکه را به‌روش کدگذاری، رمزنگاری و بارگذاری وفقی تأمین می‌کند. طرح ارائه شده منجر به افزایش سرعت تحرک شبکه، بالا رفتن کارایی و کاهش ضعف سیستم امنیتی می‌شود. در روش پیشنهادی با افزایش سرعت گره‌ها و تراکم شبکه، با ثابت بودن درصد گره‌های مهاجم و سرعت متغیر گره‌ها، نرخ دریافت بسته‌ها در حدود ٤٪ و با متغیر بودن درصد گره‌های مهاجم نرخ دریافت یا سرعت انتقال بسته‌ها در حدود ۱٪ افزایش می‌یابد. با افزایش درصد مهاجمان، علاوه بر برقراری امنیت، سربار اضافی نیز همزمان به‌طور میانگین ۱۲٪ کاهش می‌یابد.

کلیدواژگان: شبکه‌های بی‌سیم سیار اقتضایی، امنیت شبکه، بارگذاری وفقی، چند مسیریابی.

۱- مقدمه

در شبکه‌های بی‌سیم سیار هر گره می‌تواند به‌طور پویا در هر نقطه‌ای از فضای شبکه، حضور یافته و آزادانه بر اساس مقتضیات، جابه‌جا شده و به‌عنوان میزبان برای تبادل فرامین یا به‌عنوان مسیریاب، فعالیت کند. در شکل ۱ طرحی از چنین شبکه‌ای با چند گره ارتباطی نشان داده شده است. در این مقاله، پروتکلی پیشنهاد می‌شود که بخشی از آن شامل مسیریابی مبتنی بر مبدأ یا DSR[1]، چندمسیریابی[2] و بارگذاری وفقی غیریکنواخت[3] و بخش دیگری از آن شامل کانال امن با رمزنگاری بسته‌های ارسالی است که در ادامه به توضیح آنها می‌پردازیم.

1. Dynamic Source Routing
2. Multipath
3. Non-uniform Adaptive Loading



شکل ۱ شمای شبکه بی‌سیم سیار با چند گره ارتباطی

۲- مسیریابی مبتنی بر مبدأ

مسیریابی مبتنی بر مبدأ در شبکه‌های بی‌سیم سیار توسط جانسون و مالتز در سال ۱۹۹٦ در الگوریتم مسیریابی DSR مطرح شد [۱]. ایدهٔ اصلی این روش چنین است که در هر بسته مسیر، فهرستی از نشانی‌ها توسط مبدأ مشخص می‌شود و هر گره میانی با دریافت بسته، در صورتی که عضو مسیر باشند، بسته را به گره بعدیی که در فهرست نشانی‌ها آمده ارسال می‌کنند و در غیر این‌صورت بسته را دور می‌ریزد. بدین ترتیب، مسیر به‌طور دقیق توسط مبدأ تعیین شده و گره‌های میانی فقط وظیفه پیش‌راندن بسته‌ها را بر عهده دارند که این یکی از مهمترین مزایای پروتکل DSR به‌شمار می‌رود. از دیدگاه امنیتی، آگاهی مبدأ از کل مسیر، امکان انتخاب مسیرهای بدون گره مشترک را به مبدأ می‌دهد که یکی دیگر از نقاط قوت این روش محسوب می‌شود. در برابر این، وجود اطلاعات تمام مسیر در سرایند بسته[1]های تبادل داده (قطعه‌ای از بسته داده که عموماً برای اعلام وصول داده‌ها و پیام‌های کنترلی کاربرد دارند)، به‌ویژه در شرایطی که مسیر طولانی باشد، سربار قابل ملاحظه‌ای را به شبکه تحمیل می‌کند.

۳- پروتکل چندمسیریابی

آن دسته از پروتکل‌های شبکه که به کشف یک یا چند مسیر فعال برای انجام عملیات پیش‌رانی بسته‌های تبادل داده اقدام می‌کنند، پروتکل‌های چند مسیریابی نامیده می‌شوند و می‌توانند با توجه به شرایط کاری مانند انباشتگی[2]، محدودیت توان ارسال، حملات و غیره خود را با شرایط وفق دهند و مسیر جانشین بهتری را با توجه به شرایط جایگزین کنند؛ برای مثال پروتکل‌های AOMDV[3] [۲]، SMR[4] [۳] و MDSR[5] [٤] جزو پروتکل‌های چند مسیریابی به‌شمار می‌روند.

٤- بارگذاری غیریکنواخت وفقی بهینه

در این الگوریتم، نخست بهترین مسیرهای دارای امتیاز بیشینه شناخته شده و بر اساس فاصله و به‌ترتیب نزولی مرتب می‌شوند. لذا اگر مجموعه مسیرهای انتخاب شده R باشد و به‌صورت زیر تعریف شود:

$$R=\{r/p_r=\max p_i\ \} \qquad (۱)$$

p_i احتمال موفقیت ارسال هر بسته در هر مسیر و p_r بیشینه p_i است. طول مسیرهای انتخابی D_{Ri}، با رابطه زیر به‌ترتیب نزولی مرتب می‌شود:

$$D_{R1} \le D_{R2} \le \ldots \le D_{RR} \qquad (۲)$$

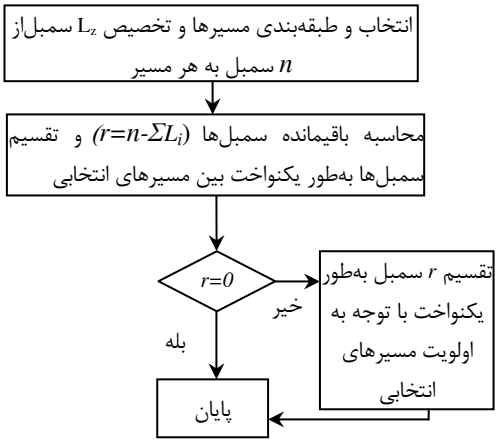
اکنون از رابطه (۱) مسیرهایی که امتیاز S_i بیشتری دارند (p_r بیشینه) انتخاب شده و از رابطه (۲) مسیرهای انتخابی که طول کمتری دارند به‌ترتیب نزولی مرتب می‌شوند. سپس از n سمبل، L_z سمبل‌به هر مسیر تخصیص داده شده و سمبل‌ها بین این مسیرها به‌طور یکنواخت توزیع می‌شود.

از آنجا که ممکن است در تقسیم n بر تعداد مسیرها (/R/)، باقیمانده مخالف صفر باشد، سمبل‌های باقیمانده r

1. Packet Overhead

2. Congestion
3. Ad hoc On-Multipath Distance Vector
4. Split Multipath Routing
5. Multipath Dynamic Source Routing

نامیده می‌شود [۵]. سپس بررسی می‌شود که آیا r صفر شده یا خیر. اگر r صفر باشد، بارگذاری وفقی به‌صورت بهینه پایان می‌یابد و در غیر این صورت با توجه به صحیح بودن تعداد سمبل‌ها، لازم است بعضی از مسیرها تعداد سمبل بیشتری دریافت نمایند. به این منظور سمبل‌های باقی مانده بار دیگر به‌طور یکنواخت و با توجه به اولویت بین مسیرها توزیع می‌شود [٦].



شکل ۲ روندنمای الگوریتم بارگذاری مسیرها به‌صورت وفقی غیر یکنواخت بهینه (ONA)

در شکل ۲، روندنمای الگوریتم بارگذاری وفقی غیریکنواخت بهینه یا ONA[1] نشان داده شده است. مهمترین دلیل برای توزیع یکنواخت بین مسیرهای بهینه، بیشینه‌سازی بهره‌گیری از مسیرهای بهینه و برقراری توازن بار در شبکه است.

۵- اجزای الگوریتم پیشنهادی

روش پیشنهادی بر انتقال اطلاعات کد شده به‌طور همزمان و استفاده از مسیرهای متعدد متکی است. ایده اصلی روش پیشنهادی مطابق شکل ۳ چنین است که پس از رمز شدن بسته‌های داده به کمک کلید مشترک از روش RS[2] [۷] به‌منظور گسترش هر یک از بسته‌ها به چند بسته کد شده استفاده می‌شود و سپس بر مبنای نوعی الگوریتم بارگذاری وفقی غیریکنواخت بهینه، به هر یک از مسیرها تعداد مناسبی بسته کد شده تخصیص می‌یابد. مقصد، بسته‌هایی را که از مسیرهای متعدد دریافت کرده، بازبینی می‌کند و سپس پیام‌ها کدگشایی و رمزگشایی می‌شوند.

معیار تخصیص بسته‌های کد شده در الگوریتم مزبور اطلاعات وضعیت مسیر است که نقشی کلیدی در عملکرد سیستم دارد.

علاوه بر وجود بارگذاری وفقی غیریکنواخت، زیر ساخت روش پیشنهادی برای برقراری ارتباط امن، دو جزء اصلی زیر را دارد:

۱- مسیریابی و تشکیل کانال امن.

۲- انتقال داده امن و مقاوم نسبت به بدرفتاری گره‌ها با استفاده از کانال امن ایجاد شده.

نخست از ایدهٔ پراکندگی اطلاعات، افزونگی اطلاعات به کمک کدگذاری و استفاده از مسیرهای متعدد استفاده می‌شود. سپس، به‌طور همزمان به امن‌سازی هر یک از مسیرها پرداخته و در نهایت از سیستم بازخورد همزمان استفاده می‌شود تا روشی مقاوم در برابر حملات متعارف به‌دست آید. با به‌کارگیری افزونگی اطلاعات و استفاده از مسیرهای مختلف در ارسال بسته داده، تأثیر حملات گره‌های مهاجم کاهش می‌یابد. این روش در شرایطی که تعداد گره‌های بدرفتار کم باشد بدون هیچ تأثیر اضافی، کیفیت و امنیت ارتباط را تضمین می‌کند. در کنار این روش تخمین وضعیت مسیرها و تخصیص بهینه بسته‌ها به مسیرها به‌صورت وفقی، بر مبنای اطلاعات وضعیت مسیر (به‌کمک حلقه بازخورد) نقش مؤثری در امنیت انتقال داده دارد.

1. Optimum Non-Uniform Adaptive Loading

2. Read-Solomon

روش انتقال داده امن و قابل اطمینان چند مسیری اجزایی به شرح زیر دارد:

الف- رمزنگاری بسته‌ها با کلید مشترک و کدگذاری هر بسته رمز شده به روش RS به n بسته کد شده که k تا از آنها برای بازسازی داده‌های اصلی کافی است [۸].

ب- معرفی مفهوم اطلاعات وضعیت مسیر یا PSI به‌عنوان قالب کلی، تطبیق این مفهوم برای تخمین امنیت و قابلیت اطمینان مجموعه مسیرها و ارائه روشی مبتنی بر بازخورد برای تخمین اطلاعات وضعیت مسیر

پ- ارائه الگوریتم‌های وفقی برای به‌کارگیری اطلاعات وضعیت مسیر برای تخصیص بهینه بسته‌های کد شده به مسیرهای موجود.

شبکه‌های بی‌سیم سیار با چالش‌های مختلفی روبه‌رو هستند و برای بهبود امنیت در این شبکه‌ها نکات مهمی را باید مد نظر داشت. در طراحی پروتکل ارائه شده در این مقاله که SMPDSR[1] نام دارد، به‌منظور دستیابی به عملکرد بهینه، نکات کلیدی زیر را باید درنظر گرفت [۹].

الف- برای کاهش تداخل مسیرها و کم‌کردن توانایی مهاجمان، مسیرهای انتخاب شده باید تا حد ممکن بدون گره مشترک باشند.

ب- با به‌کارگیری زیر مجموعه‌ای از بهترین مسیرها (از رابطهٔ ۱ و۲) می‌توان در استفاده از مسیرهای با کیفیت و امنیت پایین که موجب افزایش سربار و احتمالاً تأخیر می‌شود جلوگیری کرد.

پ- برای کاهش حجم سربار تحمیل شده به شبکه، ناشی از به‌کارگیری مسیرهای متعدد، لازم است از الگوریتم کدگذاری بهینه نظیر کدهای RS استفاده شود.

ت- سیستم باید بتواند رفتار متفاوت مسیرهای مختلف را تشخیص داده و از هر مسیر به نحو مقتضی استفاده کند. به بیانی دیگر، احتمال خراب یا گم شدن بسته در مسیرهای مختلف باید متفاوت فرض شود.

ج- در صورتی که گره‌های نامطلوب در سیستم وجود نداشته باشد روش پیشنهادی باید به مسیرهای بهینه همگرا شود.

د- خواص شبکه‌های بی‌سیم سیار و رفتار متغیر با زمان گره‌های بدرفتار و مهاجمان، باعث می‌شود که کیفیت مسیرها در طول زمان تغییر کند. روش ارائه شده باید توانایی تعقیب رفتار مسیرهای مختلف را داشته و خود را با آن وفق دهد.

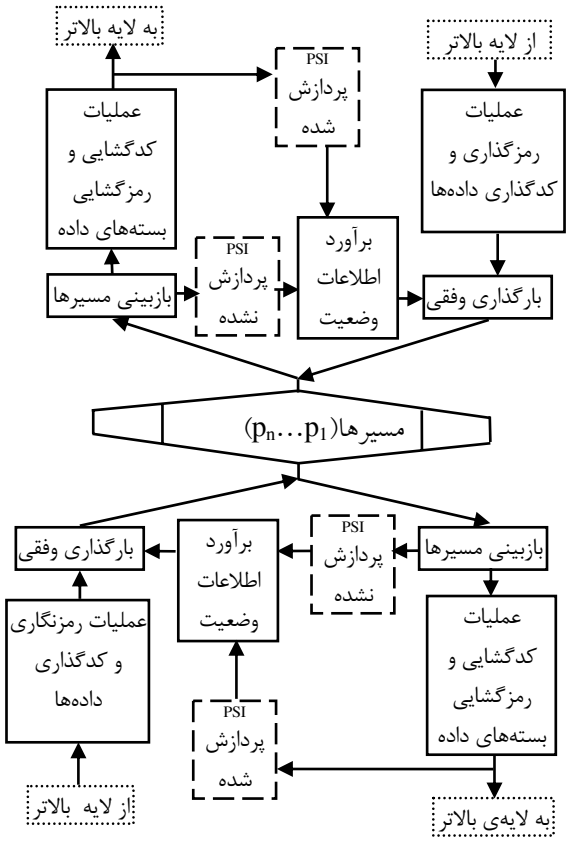
ر- از آنجا که روشهای چندمسیری مانند APSL[2] [۱۰] به‌تنهایی نمی‌توانند محرمانگی اطلاعات را حتی با به‌کارگیری کدگذاری در پروتکل‌های چند مسیری تأمین نمایند[3]، بنابراین به‌منظور تأمین محرمانگی و یکپارچگی اطلاعات، لازم است از رمزنگاری نیز استفاده شود.

گسترش داده‌ها به مجموعه‌ای از بسته‌ها که حد مشخصی از کل آنها برای بازسازی داده‌ها کافی است، یک مزیت جانبی نیز دارد: در روشهای معمولی، هنگامی که بسته با موفقیت دریافت نمی‌شود معمولاً به ارسال مجدد نیاز است و کل داده‌ها باید دوباره فرستاده شود. با استفاده از روش گسترش داده به اجزای دارای افزونگی، می‌توان به جای ارسال مجدد کل داده‌ها، فقط به مقدار نیاز (برای رسیدن به آستانه لازم برای کد گشایی) ارسال دوباره را انجام داد و به این ترتیب در پهنای باند صرفه‌جویی کرد. این ایده، به ارسال مجدد جزئی موسوم است [۸].

1. Secure Multipath and Dynamic Source Routing

2. Adaptive Path Selection and Loading

۳. زیرا گره‌هایی که در نزدیکی مبدأ و مقصد قرار دارند، حتی اگر روی هیچ یک از مسیرها نیز نباشند توانایی شنیدن بسته‌های کد شده مختلف را داشته و لذا توانایی بازسازی داده‌های اصلی را دارند.



شکل ۳ عملکرد کلی روش پیشنهادی

در شکل ۳، عملکرد کلی روش پیشنهادی چنین است. با فرض برقراری یک دسته مسیر فاقد گره مشترک و یک کلید مشترک بین مبدأ و مقصد، ابتدا هر بسته به کمک کلید مشترک رمزگذاری شده و سپس به روش RS به n بسته تبدیل می‌شود؛ برای بازسازی اطلاعات، K بسته از این بسته‌ها مورد نیاز است. سپس به هر بسته کد شده، کد تشخیص یکپارچگی که با استفاده از کلید مشترک محاسبه می‌شود - اضافه شده و توسط الگوریتمی تطبیقی یا بر مبنای تخمین موجود از وضعیت مسیرها، به هر مسیر تعداد مناسبی بسته کد شده تخصیص یافته و بسته‌های مزبور ارسال می‌شوند.

در ارتباط بین گره‌ها، به دلیل وجود گره‌های بدرفتار[1] و مهاجمان، برخی از بسته‌های داده، حذف و برخی دیگر تغییر داده می‌شوند. بنابراین تعدادی بسته کد شده به مقصد خواهند رسید. مقصد نخست درستی آنها را به کمک کدهای تشخیص یکپارچگی می‌سنجد و با دریافت K بسته رست، به کمک الگوریتم کدگشایی RS بسته رمز شده را بازسازی کرده و با استفاده از کلید مشترک رمزگشایی می‌کند [۱۱] و بسته داده را به لایه‌های بالاتر تحویل می‌دهد. مقصد مدت زمان مشخصی را پس از موفقیت در بازیابی بسته، در انتظار دریافت بسته‌های مسیرهای مختلفی که با تأخیر می‌رسند، می‌ماند و سپس با توجه به این‌که کدام بسته‌ها صحیح رسیده، کدام در راه تغییر یافته و کدام گم‌شده یا اساساً نرسیده‌اند، به کمک الگوریتم تخمین سطح قابلیت اطمینان و امنیت مسیر، اطلاعات وضعیت مسیر را به‌روز می‌کند.

در صورتی که پیام‌های ACK[2] از طرف مبدأ درخواست شده باشد یا بسته‌ای به سوی مقصد در حال ارسال باشد، مقصد، اطلاعات آخرین تغییر وضعیت مسیر را نیز برای مبدأ ارسال می‌کند. این روند به‌طور متناوب و دوطرفه برای انتقال تمامی بسته‌های داده به‌کار می‌رود. مهمترین نکته در روش انتقال داده امن و قابل اطمینان چندمسیری، رویکرد اثر محور در طراحی آن است. به این معنا که با در نظر گرفتن این نکته که مستقل از علت، برای بسته‌های داده در شبکه‌های بی‌سیم سیار، دو حالت ناخواسته گم شدن و تغییر محتوا را می‌توان در نظر گرفت، هدف روش پیشنهادی کاهش این دو اثر است.

به بیانی دیگر، هدف ما، افزایش μ در رابطه زیر است:

$$\mu=\frac{p_c}{p_t} \qquad (۳)$$

۱. گره‌هایی که فقط از سایر گره‌ها برای انتقال بسته‌های خود استفاده کرده و بسته‌های دیگران را انتقال نمی‌دهند؛ یا اقدام به قرارگیری در مسیر بسته‌ها کرده و این بسته‌ها را تغییر داده یا به‌طور تصادفی انتقال می‌دهند

2. Acknowledgement

در این رابطه، p_c تعداد بسته‌های تحویل شده صحیح در مقصد و p_t تعداد بسته‌های ارسالی است.

گم‌شدن بسته‌ها، ناشی از رفتار خودخواهانه گره‌های میانی و تغییر بسته‌ها، ناشی از تهاجم گره‌های بدخواه است که به قصد تغییر آنها و به مخاطره انداختن امنیت ارتباط از دیدگاه محرمانگی، یکپارچگی و دسترسی‌پذیری داده‌های انتقالی انجام می‌شود.

روش ارائه شده با توجه به ساختار آن، نسبت به گم‌شدن یا تغییر تصادفی بسته‌ها به دلایل مختلفی مانند تحرک، تداخل در کانال بی‌سیم و تراکم، مقاوم است.

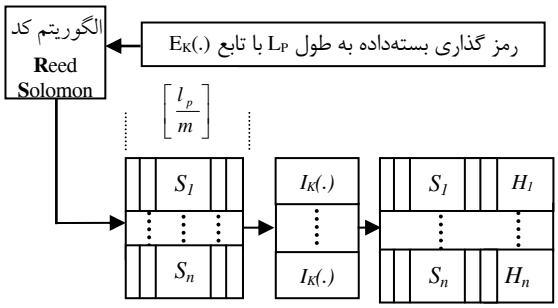
٦- کدگذاری و رمزنگاری داده‌ها

در شبکه‌های بی‌سیم سیار به‌منظور استفاده بهینه از افزونگی مسیر یا عدم قطعیت موجود در این شبکه‌ها، لازم است افزونگی اطلاعات به نحو مقتضی مدنظر قرار گیرد.

شکل ٤ ساختار کدنگاری (کدگذاری-کدگشایی) و رمزنگاری سیستم طراحی شده یا SMPDSR ارائه شده است.

همان‌طور که در شکل ٤ می‌بینیم، نخست بسته‌ای با طول L_P به کمک الگوریتم رمزنگاری متقارن $E_k(.)$ نظیر AES[1] [١٢] رمز می‌شود. سپس بسته رمز شده توسط کدگذار RS به n بسته با طول l_P/m تبدیل می‌شود که m تعداد بسته‌های مورد نیاز برای بازسازی اطلاعات است. سپس به کمک الگوریتم تولید امضای دیجیتال یا کلید متقارن مانند AES در حالت CBC[2]، کدهای تشخیص صحت یا به‌اصطلاح خلاصه رمزنگاری (اطلاعات رمز شده برای تشخیص صحت هر بسته دریافتی در مقصد) برای هر بسته به‌دست آمده و به آن افزوده می‌شود.

1. Advanced Encryption Standard
2. Cipher Block Chaining



شکل ٤ طرحوارهٔ بخش رمزنگاری و کدگذاری

در شکل ٤ تابع $I_k(.)$ عمل تولید کد تشخیص صحت به کمک کلید مشترک k[3] است و S_i بسته‌های کد شده و H_i کد تشخیص صحت است. همان‌طور که دیده می‌شود به هر بسته کد شده، کد تشخیص صحت اضافه شده و بسته آماده ارسال می‌شود [٥].

رمزنگاری در سطح بسته اصلی و تولید کدهای تشخیص صحت، روشی بهینه را از نظر حفظ محرمانگی به‌دست می‌دهد، زیرا مجزا بودن کدهای تشخیص صحت، به مقصد این امکان را می‌دهد که رفتار مسیرها را برای تک‌تک بسته‌های کد شده و محافظت شده (سمبل‌ها) بررسی کند. بررسی رفتار مسیرهای مختلف، به دقت تخمین در مورد سطح امنیت مسیرها کمک می‌نماید. دریافت K بسته از n بسته در مقصد کافی است تا به‌توان بسته اصلی را بازسازی کرد.

٧- ایجاد کلید رمزنگاری

الگوریتم دیفی هلمن DH[4] [١٣] در برابر حملات غیر فعال مقاوم است، اما در برابر حمله مردمیانی[5] (حمله‌ای که در

٣. نحوه به‌دست آوردن کلید مشترک k برای رمزنگاری در شکل ٥ نشان داده شده است.

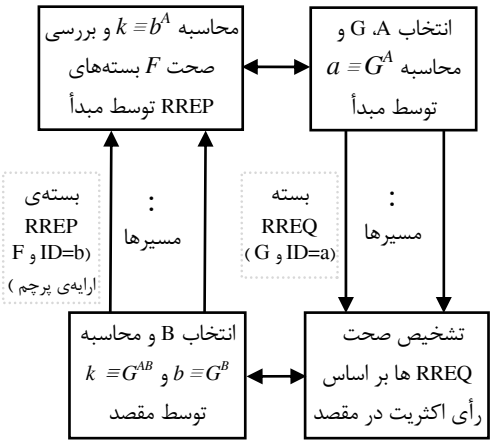
4. Diffie-Hellman
5. The Man in the Middle

آن مهاجم کنترل فعالی بر لایه ارتباطی بین دو گره دارد) آسیب‌پذیر است [١٤]. در روش پیشنهادی، از پروتکل‌های چند مسیریابی استفاده می‌شود و برای جبران کاستی بالا و کاهش سربار کلید (سرباری که برای به‌دست آوردن کلید به شبکه داده می‌شود)، الگوریتم دیفی هلمن به‌صورت زیر در نظر گرفته می‌شود:

الف- فرایند مسیریابی و تأسیس کانال امن را همزمان می‌کنیم.

ب- به کمک این روش، تخمینی از امنیت و قابلیت اطمینان مسیرها را به‌دست خواهیم آورد.

در این روش، با توجه به شکل ٥، در ابتدا مبدأ عدد تصادفی A و پایه G را که عددی بزرگ است، انتخاب کرده و سپس $a \equiv G^A$ را محاسبه می‌کند.



شکل ٥ روندنمای تبادل کلید

سپس یک بسته درخواست مسیر یا RREQ[1]، شامل سرایند معمولی، نشانی مبدأ و نشانی مقصد (شامل ID = a و G) تولید شده و برای گره‌های همسایه ارسال می‌شود و سرانجام بسته‌های RREQ به مقصد می‌رسد. مقصد با دریافت بسته‌های RREQ علاوه بر به‌دست آوردن مسیرهای متعدد، به‌کمک رأی اکثریت می‌تواند به تشخیص تغییر احتمالی بسته‌های RREQ بپردازد. بنابراین امنیت مسیرهای دریافتی را می‌تواند تخمین بزند. مقصد عددی تصادفی مانند B را انتخاب کرده و با استفاده از پایه ارائه شده توسط مبدأ یعنی G، $b \equiv G^B$ و $k \equiv a^B \equiv G^{AB}$ را محاسبه می‌کند. سپس مقصد بسته RREP را تولید می‌کند و ID آن را برابر b قرار می‌دهد. مقصد برای هر مسیر یک آرایه پرچم (F) را تشکیل می‌دهد که طول این آرایه برابر تعداد مسیرهای کشف شده است. در این آرایه، برای مسیرهای ناامن مقدار یک"1" و برای مسیرهای امن مقدار صفر"0" در نظر گرفته می‌شود که این مقادیر، با استفاده از کلید مشترک رمز شده و به بسته RREP افزوده می‌شود سپس بسته RREP از تمامی مسیرهای موازی، کشف شده و به سمت مبدأ ارسال می‌شود. مبدأ به‌کمک b، کلید مشترک را به‌صورت $k \equiv (b)^A$ محاسبه کرده و با آن آرایه پرچم را رمزگشایی کرده و امنیت مسیرهای یافته شده را ارزیابی می‌کند [١٥].

با فرض اینکه سربار محاسباتی الگوریتم دیفی هلمن، برابر با سایر الگوریتم‌های کلید عمومی باشد، این الگوریتم فقط یک بار در زمان تأسیس کلید به‌کار می‌رود و بقیه عملیات رمزنگاری به‌صورت متقارن انجام می‌شود و سربار محاسباتی تحمیل شده به گره‌ها در برابر امنیت به‌دست آمده ناچیز است [١٦].

٨- شبیه‌سازی و تحلیل نتایج

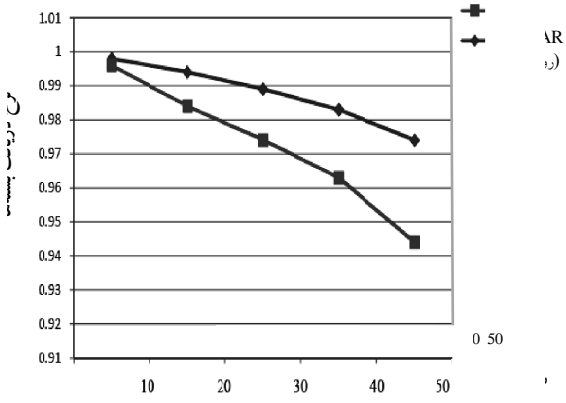
در شبیه‌سازی الگوریتم‌ها، از شبیه‌ساز NS2[2] [١٧] استفاده شده و محیط شبیه‌سازی با وسعت ٣٠٠٠×٣٠٠٠ متر مربع (٩کیلومتر مربع) در نظر گرفته شده است.

نتایج شبیه‌سازی روش پیشنهادی SMPDSR و APSL، چگونگی نرخ دریافت بسته‌ها در شرایطی که درصد گره‌های مهاجم ثابت و شبکه دارای ١٥٠ و ٢٥٠

1. Route Request

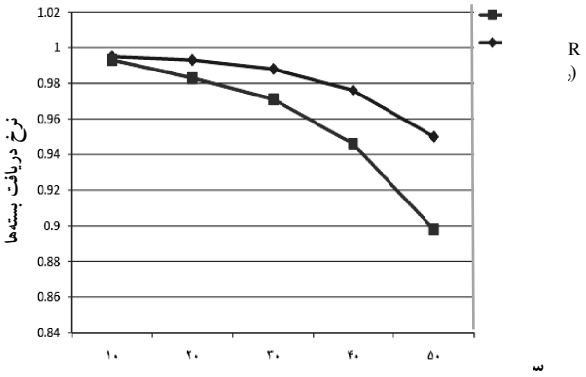
2. Network Simulation 2

گره است و سرعت گره‌های شبکه افزایش می‌یابد در دو شکل ٦ و ٧ نشان داده شده است.



شکل ٦ نرخ دریافت بسته‌ها در الگوریتم SMPDSR و APSL (١٥٠ گره)

در SMPDSR وقتی سرعت گره‌ها افزایش می‌یابد، قطع و وصل شدن مسیرها افزایش می‌یابد. تحرّک یکی از عوامل مهمی است که باعث می‌شود کارایی شبکه افزایش یابد زیرا در شرایط سخت (ترافیک سنگین یا نقص در شبکه) تحرک و انعطاف‌پذیری یکی از عوامل مهم موفقیت است. لذا اگر به‌منظور تأمین ارتباط و امنیت در ارتباط گره‌ها پیش‌بینی‌های لازم انجام نشود، افزایش سرعت، خود به نقطه ضعف تبدیل می‌شود. در SMPDSR برای جلوگیری از سوء استفاده از این ضعف و شنود همسایه‌های مبدأ و مقصد، از رمزنگاری استفاده شده است. همچنین بین تحویل بسته و سربار رابطه‌ای بسیار قوی وجود دارد. موفق نشدن در انتقال داده‌ها به ارسال مجدد منجر می‌شود که باعث افزایش سربار و حتی منجر به عدم موفقیت در انتقال بسته، افت در عملکرد شبکه و جستجو برای دسته مسیر جدید نیز خواهد شد.

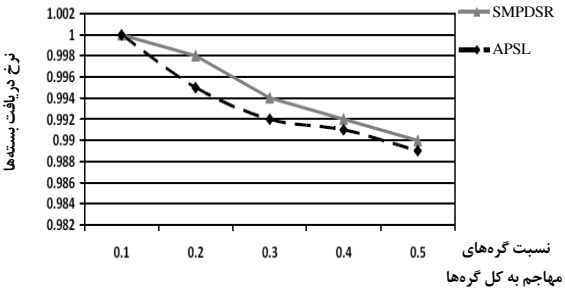


شکل ٧ نرخ دریافت بسته‌ها در الگوریتم SMPDSR و APSL (٢٥٠ گره)

یکی از مهمترین نقاط قوت روش پیشنهادی مقاومت بالای آن در برابر مهاجمانی است که سعی می‌کنند در سرعتهای بالا از قطع و وصل مسیرها به نفع مقاصد خود استفاده کنند. اما این روش حتی با وجود شنود در همسایه‌های مبدأ و مقصد و قطع و وصل شدن ارتباطات در سرعت بالای گره‌های شبکه، امکان کشف پیام را از میان می‌برد و در حین مسیریابی نیز بیشتر مسیرهایی که گره‌های مهاجم دارند از مسیرهای بهینه حذف می‌شوند. در شکل‌های ٦ و ٧ دیده می‌شود که در حالت کلی، با افزایش سرعت گره‌های شبکه، نرخ دریافت بسته‌ها کاهش می‌یابد؛ اما در محدوده سرعت ٤٠، شیب کاهش سرعت زیاد و غیر عادی می‌شود. زیرا سرعت بالای گره‌ها و تراکم زیاد گره‌های شبکه، باعث ایجاد اختلال در ارتباطات، کم شدن تعداد مسیرهای انتقال داده و افزایش ترافیک می‌شود. در سرعتهای بالا، تعداد مسیرهای انتقال داده به کمترین تعداد می‌رسند (فرض بر این است که حداقل یک مسیر سالم وجود دارد) و کل ترافیک از این مسیرها عبور می‌کند، لذا سربار افزایش می‌یابد. زیرا داده‌ها برای انتقال باید منتظر بمانند تا نوبت به آنها برسد. همچنین افزایش سرعت گره‌ها، باعث افزایش قطع و وصل ارتباطات و ایجاد اختلال در عملکرد شبکه می‌شود.

برای انتقال داده در شبکه‌ای با ۱۵۰ گره، نرخ دریافت بسته‌ها با افزایش سرعت گره‌های شبکه به‌طور عادی کاهش می‌یابد. زیرا با توجه به برد انتقال بی‌سیم و وسعت شبکه، تعداد گره‌ها، مناسب است. افزایش گره‌های شبکه به ۲۵۰ گره، نرخ دریافت بسته‌ها را کاهش می‌دهد، زیرا مبدأ باید اطلاعات بیشتری از مسیرها را در حافظه خود نگاه دارد و با افزایش گره‌ها، طول گام مسیرها افزایش می‌یابد. همچنین مبدأ باید تلاش بیشتری در تفکیک مسیرهای مجزا انجام دهد و یافتن مسیرهایی که گره‌های مجزایی داشته باشند، به پردازش بیشتری نیاز دارد. در این حالت گره‌های مهاجم می‌توانند اطلاعات بیشتری را از همسایه‌های خود کسب کنند و شناخت آنها نیز مشکل‌تر می‌شود. می‌توان نتیجه گرفت که اگر چه سرعت گره‌های شبکه تأثیر به‌سزایی بر عملکرد شبکه دارد؛ اما نسبت وسعت شبکه به تعداد گرها را نیز باید در نظر گرفت.

در پروتکل پیشنهادی مانند سایر روشها، با افزایش درصد گره‌های مهاجم، نرخ دریافت بسته‌ها کاهش می‌یابد؛ اما مهمترین نکته در این روش، به‌کارگیری رمزنگاری است، به‌گونه‌ای که فقط در ابتدای ارتباط، با تبادل یک کلید، می‌توان پیام‌ها را رمز کرد. پیام‌های رمزشده، به‌صورت پیام‌هایی کد شده در آمده و در صورت شناسایی روش کدگذاری، توسط مهاجمان، به علت به‌کارگیری رمزنگاری قابل کشف نیستند. در روش APSL گره‌های همسایه مبدأ و مقصد پیام‌های کد شده زیادی را دریافت می‌کنند و مهاجمان از این ضعف امنیتی استفاده کرده و می‌توانند پیام‌ها را شنود و کشف کنند. نتایج شبیه‌سازی SMPDSR و APSL و چگونگی نرخ دریافت بسته‌ها در شرایطی که نسبت گره‌های مهاجم به کل گره‌ها در شبکه، افزایش می‌یابد در شکل ۸ نشان داده شده است.



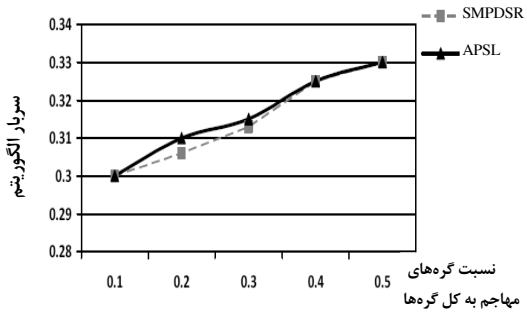
شکل ۸ متوسط تحویل بسته‌ها در SMPDSR و APSL

در APSL، شنود همسایه‌های مبدأ و مقصد باعث می‌شود که پیام‌های کدشده زیادی را دریافت کنند و امنیت پیام‌ها به خطر می‌افتد. روش پیشنهادی ضمن برتری کارایی و استحکام امنیتی، ضعف امنیتی روش APSL را نیز پوشش می‌دهد.

در شکل ۹ نتایج شبیه‌سازی SMPDSR و APSL و سربار الگوریتم در شرایطی که نسبت گره‌های مهاجم به کل گره‌ها در شبکه افزایش می‌یابد نشان داده شده که سربار روش پیشنهادی تا نسبت ۰/٤ بیشتر و بعد از آن با روش APSL برابر می‌شود.

در SMPDSR برای جلوگیری از شنود همسایه‌های مبدأ و مقصد، از رمزنگاری استفاده شده که موجب ایجاد سربار اضافی برای شبکه می‌شود. اما با افزایش درصد مهاجمان در روش پیشنهادی، سربار اضافی جبران می‌شود. در روش پیشنهادی با به‌کارگیری الگوریتم ساده‌ای که در شکل ۲ نشان داده شده، پیام‌ها بر روی مسیرها بارگذاری می‌شوند. اساساً بین تحویل بسته و سربار رابطه‌ای بسیار قوی وجود دارد. موفق نبودن در انتقال داده‌ها، به ارسال مجدد منجر می‌شود که باعث افزایش سربار و حتی ناموفقیت در انتقال بسته، افت در عملکرد شبکه و جستجو برای دسته-مسیر جدید نیز می‌شود. یکی از مهمترین نقاط قوت روش پیشنهادی مقاومت بالای آن در برابر مهاجمان

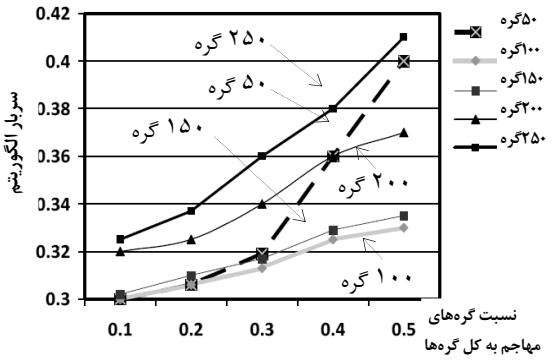
است. حتی با وجود شنود در همسایه‌های مبدأ و مقصد، امکان کشف پیام وجود ندارد و در حین مسیریابی نیز بیشتر مسیرهایی که دارای گره‌های مهاجم هستند از میان مسیرهای بهینه حذف می‌شوند.



شکل ۹ سربار الگوریتم در SMPDSR و APSL

در شکل ۱۰ دیده می‌شود در حالت کلی، با افزایش نسبت گره‌های مهاجم به کل گره‌ها در شبکه، سربار شبکه افزایش می‌یابد. زیرا گره‌های نامطلوب با ایجاد اختلال در ارتباطات و کم کردن مسیر انتقال داده، باعث افزایش ترافیک می‌شوند.

شبکه ۵۰ گرهی در جایی که نسبت گره‌های مهاجم به کل، از ۰/۱۰ به ۰/۳۰ می‌رسد، به علت کم شدن تعداد مسیرهای سالم، سربار با شیب خطی ملایمی افزایش می‌یابد و زمانی که به ۰/۳۰ می‌رسد، سربار به‌طور ناگهانی افزایش می‌یابد. دلیل این پدیده آن است که با توجه به وسعت شبکه و درصد گره‌های مهاجم، مسیرهای انتقال داده به کمترین تعداد می‌رسند (فرض بر آن است که حداقل یک مسیر سالم وجود دارد) و کل ترافیک از این مسیرها عبور می‌کند، لذا سربار افزایش می‌یابد زیرا داده‌ها برای انتقال باید منتظر بمانند تا نوبت‌به آنها برسد.



شکل ۱۰ سربار الگوریتم SMPDSR با تعداد گره‌های مختلف

همچنین افزایش گره‌های نامطلوب، باعث افزایش اختلال در عملکرد شبکه می‌شود. برای انتقال داده در شبکه‌ای با ۱۰۰ یا ۱۵۰ گره، سربار الگوریتم با افزایش درصد گره‌های مهاجم به‌طور عادی افزایش می‌یابد، زیرا با توجه به برد انتقال بی‌سیم و وسعت شبکه، تعداد گره‌ها مناسب است. افزایش تعداد گره‌های شبکه به ۲۰۰ و ۲۵۰، سربار را افزایش می‌دهد زیرا مبدأ باید اطلاعات بیشتری از مسیرها را در حافظه خود نگاه دارد، زیرا با افزایش تعداد گره‌ها، طول گام مسیرها افزایش می‌یابد و همچنین مبدأ باید تلاش بیشتری برای تفکیک مسیرهای مجزا انجام دهد.

گره‌های نامطلوب نیز می‌توانند این سربار را با اخلال در انتقال داده‌ها افزایش دهند. مشکل‌ترین حالت شبکه‌ای با ۲۵۰ گره است، زیرا افزایش تعداد گره‌ها تعداد گام‌های بین مبدأ و مقصد را افزایش می‌دهد و یافتن مسیرهایی که گره‌هایی مجزا داشته باشند، به پردازش بیشتری نیاز دارد. با توجه به تراکم گره‌های شبکه، گره‌های مهاجم می‌توانند اطلاعات بیشتری را از همسایه‌های خود کسب کنند و شناخت آنها نیز مشکل‌تر می‌شود. می‌توان نتیجه گرفت که اگر چه

درصد گره‌های مهاجم تأثیر به‌سزایی بر سربار دارند، اما نسبت وسعت شبکه با تعداد گره‌ها را نیز باید در نظر گرفت.

۹- نتیجه‌گیری

در سیستم‌های ارتباطی بی‌سیم از پروتکل‌هایی استفاده می‌شود که بتوانند ارتباط بی‌سیم را با بیشترین بهره به‌کار گیرند. شبکه بی‌سیم سیار(اقتضایی) مدلی برای سیستم‌های ارتباطی بی‌سیم است که در آنها گره‌ها به‌طور آزادانه و با سرعت دلخواه جابه‌جا شده و به‌عنوان میزبان تبادل فرامین یا به‌عنوان مسیریاب، فعالیت می‌کنند.

برای داشتن شبکه‌ای امن و با قابلیت اطمینان بالا، و با کمترین خطا، مقابله با تأثیر مهاجمان در شناخت و کشف مسیر در انتقال داده و پیشگیری از هر گونه اختلال در تبادل اطلاعات و جلوگیری از اختلال توسط دشمن، به پروتکل‌های ارتباطی مناسب و امنی نیاز است. در اینجا پروتکل SMPDSR پیشنهاد و ارزیابی و با پروتکلAPSL که در شبکه‌ای مشابه کاربرد دارد، شبیه‌سازی و مقایسه شد. اگرچه اصول عملکرد دو پروتکل SMPDSR و APSL، یکسان است اما پروتکل SMPDSR، در حفظ محرمانگی به‌کمک رمزنگاری متقارن با کلید مشترک و نیز الگوریتم بارگذاری، با پروتکل APSL متفاوت است. در این پروتکل با به‌کارگیری سیستم بازخورد به‌کمک تخمین PSI، تعقیب وضعیت مسیرها به‌خوبی انجام شده و حتی در شرایط سخت نیز با موفقیت عمل می‌کند. از سوی دیگر با استفاده از کدگذاری داده‌ها و استفاده از چند مسیر، توانایی آزمودن مسیرهای مختلف را به‌صورت سریع و موازی دارد که این یکی از مزیت‌های مستقیم ناشی از انتقال چند مسیری، علاوه بر مسیریابی چندمسیری است. یکی از نواقص بسیاری از پروتکل‌ها، امکان شنود توسط همسایه‌های مبدأ و مقصد است که می‌توانند پیام‌های کد شده زیادی را دریافت کنند. برای حل این مشکل، از رمزنگاری استفاده کرده‌ایم که باعث افزایش سربار می‌شود و برای جبران این سربار، روشی پیشنهاد شده است. با شبیه‌سازی SMPDSR و APSL، نرخ دریافت بسته‌ها و سربار الگوریتم در شرایطی که درصد گره‌های مهاجم در شبکه افزایش می‌یابد نمایش داده شد و همچنین نرخ دریافت بسته‌ها در شرایطی که سرعت گره‌های شبکه افزایش می‌یابد ارائه شد که برتری روش پیشنهادی را تأیید می‌کند. نشان دادیم که یکی از مهمترین نقاط قوت روش پیشنهادی، مقاومت بالای آن در برابر مهاجمان و انعطاف‌پذیری در برابر افزایش تحرک شبکه است.

۱۰- منابع

[1] A.F, Abidin, and M.K, Yusof. " Ad Hoc On-Demand Distance Vector Routing, Dynamic Source Routing and Destination-Sequenced Distance-Vector", International Journal on Computer Science and Engineering (IJCSE), (2010).

[2] N.Jaisankar and R.Saravanan. "AOMDV: On-Demand Multipath Routing for Mobile AD Hoc Networks" , IACSIT International

Journal of Engineering and Technology, August 2010 ISSN: 1793-8236.

[3] S. Lee, M. Gerla. "SMR: Split Multipath Routing with Maximally Disjoint Paths in AD HOC Networks", Proc. Of IEEEICC, Vol.10, (2001), pp.3201-3205.

[4] A. Nasipuri, R. Castaneda, S.R. Das. "MDSR: Performance of route caching strategies in dynamic source routing for on demand protocols in mobile ad hoc networks", ACM/Kluwer Mobile Networks and Application (MONET), (2001), 6(4): 339-349.

[۵] علیرضا رضائی ، " طراحی و شبیه‌سازی یک کانال امن و مقاوم در برابر حملات متعارف در شبکه‌های بی‌سیم سیار بر اساس چند مسیریابی مبتنی بر مبدا" ، پایان‌نامه کارشناسی ارشد دانشگاه علوم و فنون هوائی شهید ستاری. (۱۳۸۹)

[6] V. Vetriselvi and R. Parthasarathi. "Secure communication for multipath ad hoc network", TENCON 2003. Conference on Convergent Technologies for Asia-Pacific Region, (2003), 1086-1090.

[7] I.S. Reed, G. Solomon. "Polynomial Codes over Certain Finite Fields," SIAM Journal of Applied Math, (1960), pp. 300-304.

[8] E. Ayanoglu, I. Chih-Lin, R.D. Gitlin, J.E. Mazo. "Diversity Coding for Transparent Self-Healing and Fault-Tolerant Communication Networks", Communications, IEEE Transactions on, Vol.41, (1993), pp. 1677-1686.

[9] L. Wenjing, W. Yuguang."SPREAD: Enhancing Data Comfidentiality in The Mobile Ad-hoc Network", IEEE INFOCOM 2004, Hang Kong, China.

[10] Kh. Ahmad. and S. Ghassem."Misbehavior Resilient Multipath Data Transmission in Mobile Ad hoc Networks". Institute for Studies in Theoretical Physics and Mathematics (IPM), (2006).

[11] A. Balasubramanian, S. Mishra, R. Sridhar. "Analysis of a Hybrid Key Management Solution for Ad hoc Networks", IEEE Wireless Communications and Networking Conference, (2005), PP.2082-2087.

[12] R.Stinson , "Cryptography theory and practice", university of Waterloo Ontario, Canada.

[13] Diffie, W. and Hellman, M.E.(1976), "New Directions in Cryptography", IEEE Transactions on Information Theory, (2006), pp. 644-654.

[14] S.Convery. "Network security rchitectures", (2004)

[15] Shoup, Victor. "A Computational Introdution to Number Theory and Algebra (Version 1)", Cambridge University Press, (2005).

[16] Diffie, W. and Hellman, M.E. “New Directions in Cryptography”, IEEE Transactions on Information Theory, Vol. 22, (1976), pp. 644-654.

[17] FJ, Arbona "Simulation of Routing Protocol for Ad-hoc networks in NS- 2", (2006).