نشریه علمی- پژوهشی مهندسی هوانوردی
سال دوازدهم، شماره دوم، پاییز 89

طراحی، شبیه‌سازی و ارزیابی یک سامانه هدایت و ناوبری امن هوایی بر اساس شبکه چند مسیری مبتنی بر مبدأ و بارگذاری وفقی

نجاتی جهرمی، منصور*[1]، رضایی، علیرضا[2]
1- دکترا و مدرس دانشگاه، دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران
2- دانشجوی کارشناسی ارشد، دانشگاه علوم و فنون هوایی شهید ستاری، تهران، ایران
(دریافت مقاله: 1389/5/24 تاریخ پذیرش: 1389/9/15)

چکیده

سامانه هدایت و ناوبری شبکه‌ای، بستر ارتباطی کارآمدی را برای تحقیق اهداف و هدایت عملیات فراهم می‌آورد. در این الگو، عملیات هوایی گسترده با مجموعه‌ای از صدها پرنده پشتیبانی هوایی و جنگنده، انجام می‌شود. این شبکه با توجه به تحرک پرنده‌ها به‌صورت الگویی خاص از شبکه بی‌سیم سیار طراحی شده که ضمن داشتن مزیت‌هایی از قبیل: تحمل‌پذیری در برابر خطا، کاهش تأثیر مهاجمین در طول فرایند شناخت و کشف مسیر و انتقال داده، از توانایی کشف چندین مسیر نیز برخوردار است و امکان تبادل اطلاعات و افزایش قابلیت اطمینان در شبکه را فراهم می‌آورد. در این مقاله، پروتکل طراحی شده ضمن برخورداری از مزیت‌های فوق، از کدبندی، رمزنگاری، الگوریتم چند مسیریابی و بارگذاری وفقی، نیز استفاده می‌نمایدکه منجر به افزایش کارایی و امنیت و نهایتاً، افزایش نسبت تحویل سالم بسته‌ها به کل بسته‌های ارسالی خواهد شد. نتایج شبیه‌سازی نشان می‌دهد در روش پیشنهادی، به‌طور متوسط نرخ دریافت یا سرعت انتقال بسته‌ها، حدوداً 1% افزایش پیدا می‌کند و با افزایش درصد مهاجمین ضمن برقراری امنیت، هم‌زمان سربار اضافی به‌طور متوسط 12% کاهش می‌یابد.

واژه‌های کلیدی: *شبکه هدایت و ناوبری، شبکه‌های بی‌سیم سیار، امنیت، امنیت بر مبنای مسیریابی مبتنی بر مبدأ*

مقدمه

در مدل پیشنهادی برای هدایت و تحقق اهداف هواپیماها در طرح عملیاتی، الگویی از شبکه هدایت و ناوبری گسترده در کنار شبکه بی‌سیم سیار بسیار خاص ارائه شده است. مدل مذکور از تعداد زیادی از پرنده‌ها و هواپیماهای مختلف پشتیبانی و رزمی تشکیل می‌شود. در این مدل، هر هواپیما و پرنده، به‌صورت یک گره بی‌سیم سیار است که می‌تواند به‌طور پویا در هر نقطه از فضای عملیاتی، بدون استفاده از ساختار مرکزی و زمینی، عملیات ارتباط، هدایت و ناوبری را انجام دهد و به‌طور آزادانه بر اساس مقتضیات عملیات، جابه‌جا شده و در حکم میزبان برای تبادل فرامین یا در نقش مسیریاب، فعالیت کند. ساختار شبکه‌ای موجود در هدایت و ناوبری بین رادارهای زمینی و برج‌های مراقبت و پرنده‌ها و هواپیماهاست که از استانداردهای مرتبط پیروی می‌کند. ساختار پیشنهادی در مقاله در شبکه‌ای مستقل و بین پرنده‌هاست.

در این مقاله ابتدا الگوی شبکه مورد نظر معرفی می‌شود سپس ضمن توصیف پروتکل پیشنهادی و اجزای آن، زیرساخت طراحی شبکه تبیین می‌شود و سرانجام نتایج به‌دست آمده شبیه‌سازی و تحلیل خواهد شد.

الگوی شبکه هدایت و ناوبری

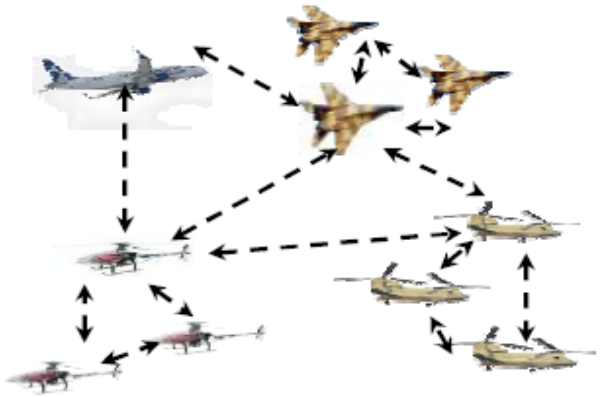
در این الگو مجموعه‌ای از هواپیما و پرنده‌ها مطابق شکل (1) که در یک گروه پروازی و عملیاتی قرار دارند در نظر گرفته می‌شود.

در این مدل، هر پرنده، به‌صورت یک گره بی‌سیم سیار به‌طور پویا در هر نقطه از فضای عملیاتی، توانایی عملیات ارتباط، هدایت و ناوبری را دارد و بر اساس مقتضیات عملیات،

* نویسنده پاسخگو، پست الکترونیک: nejati@aut.ac.ir

در حکم میزبان برای تبادل فرامین یا در نقش مسیریاب، فعالیت می‌کند. در شکل (2) شبکه معادل طرح عملیات هوایی با 10 گره ارتباطی، آورده شده است. بر این اساس مدل ارتباطی به‌صورت یک شبکه بی‌سیم سیار خاص‌منظوره خواهد بود که متناسب با آن پروتکل‌های لازم در نظر گرفته می‌شود و از این به بعد در متن شبکه هدایت و ناوبری شبکه بی‌سیم سیار خاص‌منظوره و به اختصار شبکه بی‌سیم نامیده می‌شود.

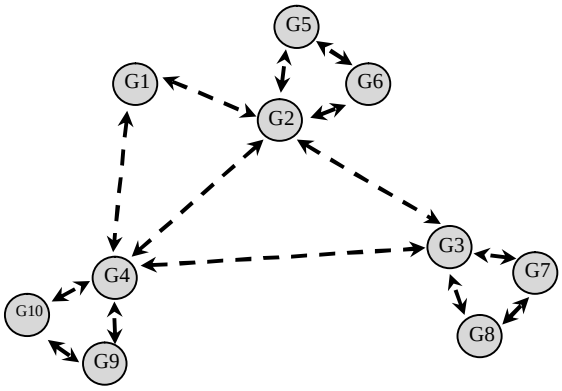
اجزاء پروتکل پیشنهادی که در شکل (3) شمای اجزاء کلی آن نشان داده شده است بر اساس مسیریابی مبتنی بر مبدأ یا DSR[1][1]، چندمسیریابی[2] و بارگذاری وفقی غیریکنواخت[3] در شبکه، همچنین تشکیل کانال امن با رمزنگاری بسته‌های ارسالی است، در ادامه توضیح داده خواهد شد.



شکل 1- شبکه ارتباطی هدایت و ناوبری در یک طرح عملیاتی

مسیریابی مبتنی بر مبدأ

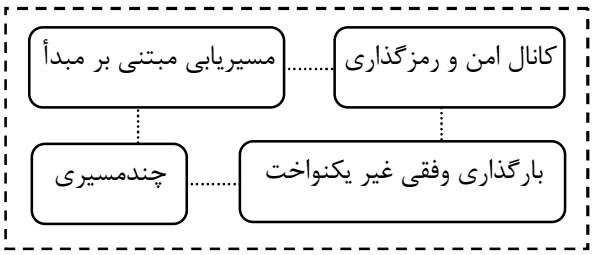
ایده مسیریابی مبتنی بر مبدأ در شبکه‌های بی‌سیم سیار را جانسون و مالتز در سال 1996 در الگوریتم مسیریابی DSR مطرح نمودند [1]. ایده اصلی این روش به این صورت است که در هر بسته مسیر، فهرستی از آدرس‌ها توسط مبدأ مشخص می‌گردد و گره‌های میانی به مجرد دریافت بسته، در صورتی‌که عضو مسیر باشند، بسته را به گره بعدی که در فهرست آدرس‌ها آمده است ارسال می‌کنند و در غیر این صورت بسته را دور می‌ریزد. بدین ترتیب، مسیر به‌صورت مشخص از مبدأ تعیین می‌شود و گره‌های میانی تنها وظیفه پیش‌راندن بسته‌ها را به‌عهده دارند که این مسئله یکی از مهم‌ترین مزایای پروتکل DSR به شمار می‌رود. علاوه بر آن، از دیدگاه امنیتی، آگاهی مبدأ از کل مسیر، قدرت انتخاب مسیرهای فاقد گره مشترک را به مبدأ می‌دهد، که از نقاط قوت این روش محسوب می‌شود. در برابر این، وجود تمام مسیر در سرایند بسته[4]های تبادل داده (قطعه‌ای از بسته داده که عموماً برای اعلام وصول داده‌ها و پیام‌های کنترلی کاربرد دارد)، خصوصاً در شرایطی که مسیر طولانی باشد، سربار قابل ملاحظه‌ای به شبکه تحمیل می‌کند.



شکل 2- شبکه معادل هدایت و ناوبری در یک طرح عملیاتی با 10 گره ارتباطی

الگوریتم چند مسیریابی

پروتکل‌های چند مسیریابی آن دسته از پروتکل‌های شبکه هستند که به کشف یک یا چند مسیر فعال برای انجام عملیات جلورانی بسته‌های تبادل داده، اقدام می‌کنند. پروتکل‌های چند مسیریابی قادر هستند با توجه به شرایط محیطی همچون ازدحام[5]، محدودیت توان ارسال، حملات و غیره خود را با شرایط وفق دهند و مسیر جانشین بهتری را با توجه به شرایط جایگزین کنند به عنوان نمونه پروتکل‌های AOMDV[6] [2]، SMR[7] [3] و MDSR[8] [4] جزو پروتکل‌های چند مسیریابی به‌شمار می‌آیند.



شکل 3- اجزاء کلی پروتکل پیشنهادی

الگوریتم بارگذاری غیریکنواخت وفقی بهینه

در این الگوریتم، ابتدا بهترین مسیرها با امتیاز بیشینه شناخته شده و بر اساس فاصله و به ترتیب نزولی مرتب می‌شوند لذا اگر مجموعه مسیرهای انتخاب شده، Z باشد و به‌صورت رابطه (1) تعریف شود:

$$Z=\{z/p_z=\max p_i\} \quad (1)$$

P_i احتمال موفقیت تک‌بسته‌های داده هر مسیر است و طول مسیرهای انتخابی D_{zi}، با رابطه (2) به ترتیب نزولی مرتب و تعریف می‌شود:

$$D_{Z1} \le D_{Z2} \le .. \le D_{ZZ} \quad (2)$$

حال از رابطه (1) مسیرهایی که امتیاز S_i بیشتر دارند انتخاب شده و از رابطه (2) مسیرهای انتخابی که طول کمتری دارند به ترتیب نزولی مرتب می‌شوند، سپس از n سمبل، L_z سمبل به هر مسیر تخصیص داده می‌شود و سمبل‌ها بین این مسیرها به‌طور یکنواخت توزیع می‌گردد.

چون ممکن است از تقسیم n بر تعداد مسیرها ($/z/$)، باقیمانده ایجاد شود، سمبل‌های باقیمانده، r نامیده می‌شود [5] حال بررسی می‌شود که آیا r صفر شده یا خیر، اگر $r=0$ باشد، بارگذاری وفقی به‌صورت بهینه پایان می‌یابد، در غیر این صورت با توجه به صحیح بودن تعداد سمبل‌ها، لازم است که بعضی مسیرها تعداد سمبل بیشتری دریافت نمایند. به این منظور سمبل‌های باقی‌مانده مجدداً به‌طور یکنواخت با توجه به اولویت بین مسیرها توزیع می‌گردد [6].

در شکل (4)، فلوچارت الگوریتم بارگذاری وفقی غیریکنواخت بهینه یا ONA[9] نشان داده شده که مطابق توصیف فوق است.

مهمترین دلیل برای توزیع یکنواخت بین مسیرهای بهینه، بیشینه‌سازی بهره‌گیری از مسیرهای بهینه و برقراری توازن بار در شبکه است.

توصیف اجزاء الگوریتم و روش پیشنهادی

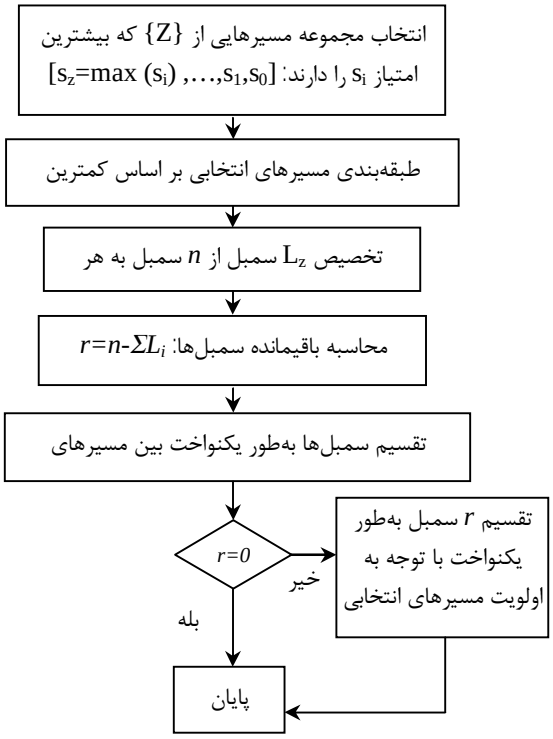
روش پیشنهادی از اجزای گوناگونی تشکیل شده است که بر مبنای انتقال اطلاعات کدشده به‌طور هم‌زمان و استفاده از مسیرهای متعدد است. ایده کلی روش پیشنهادی مطابق شکل (5) به این شرح است که پس از رمز شدن بسته‌های داده به کمک کلید مشترک از روش کدبندی RS[10][7] به‌منظور گسترش هر یک از بسته‌ها به چند بسته کدشده استفاده می‌گردد، سپس بر مبنای یک الگوریتم بارگذاری وفقی غیریکنواخت بهینه، به هر یک از مسیرها تعداد مناسبی بسته کدشده، تخصیص می‌یابد. مقصد، بسته‌هایی را که از مسیرهای متعدد دریافت کرده است بازبینی می‌کند. سپس پیام‌ها کدگشایی و رمزگشایی می‌شود.

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

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

1) مسیریابی و تشکیل کانال امن.

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



شکل 4- روندنمایی الگوریتم بارگذاری مسیرها به‌صورت بارگذاری وفقی غیر یکنواخت بهینه‌ی ONA

در ابتدا از ایده تفرقی اطلاعات، افزونگی اطلاعات به کمک کدبندی و استفاده از مسیرهای متعدد در کنار امن‌سازی

تک‌تک مسیرها و در نهایت یک سیستم بازخورد هم‌زمان در کنار هم استفاده شده است تا در نهایت 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 متد در شرایطی که تعداد گره‌های بدرفتار کم باشند بدون هیچ تاثیر اضافی کیفیت و امنیت ارتباط را تضمین می‌کند. در کنار این روش تخمین وضعیت مسیرها و تخصیص بهینه بسته‌ها به مسیرها به صورت وفقی، بر مبنای اطلاعات وضعیت مسیر (به کمک حلقه بازخورد) نقش موثری در امنیت انتقال داده دارد.

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

الف) رمزنگاری بسته‌ها با کلید مشترک و کدبندی هر بسته رمز شده با روش RS به n بسته کدشده که k عدد از آنها برای بازسازی داده‌های اصلی کافی است [8].

ب) معرفی نمودن "مفهوم اطلاعات وضعیت مسیر" یا PSI[11] در حکم قالب کلی، تطبیق دادن این اطلاعات برای تخمین امنیت و قابلیت اطمینان مجموعه مسیرها، ارائه کردن یک روش مبتنی بر بازخورد برای تخمین اطلاعات وضعیت مسیر

پ) ارائه الگوریتم‌های وفقی برای به‌کارگیری اطلاعات وضعیت مسیر برای تخصیص بهینه بسته‌های کدشده به مسیرهای موجود.

شبکه‌های بی‌سیم سیار با چالش‌های مختلفی مواجه هستند که برای بهبود امنیت در این شبکه نکات مهمی را باید مد نظر داشت. در طراحی پروتکل ارائه شده در این مقاله که SMPDSR[12] نام‌گذاری می‌شود به‌منظور دست‌یابی به عملکرد بهینه، باید نکات کلیدی زیر را درنظر گرفت [9].

الف) برای کاهش تداخل مسیرها و کم‌کردن توانایی مهاجمین، باید مسیرهای انتخاب شده حتی‌الامکان فاقد گره مشترک باشند.

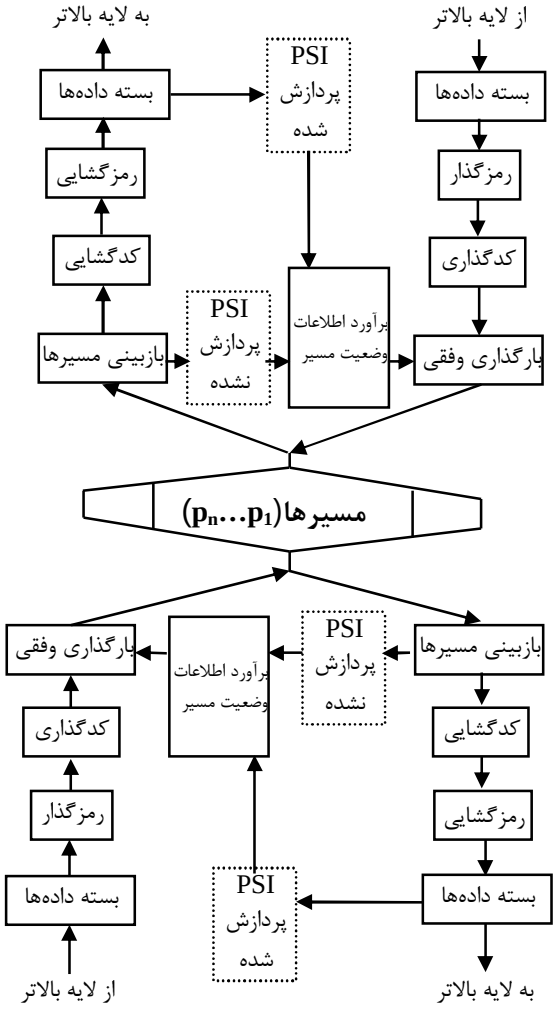
ب) با به‌کارگیری زیرمجموعه‌ای از بهترین مسیرها (از رابطه 1 و 2) می‌توان استفاده از مسیرهای با کیفیت و امنیت پایین که موجب افزایش سربار و احتمالاً تاخیر می‌گردد جلوگیری کرد.

پ) برای کنترل سربار تحمیل شده به شبکه، ناشی از به‌کارگیری مسیرهای متعدد لازم است از الگوریتم کدبندی بهینه نظیر کدهای RS استفاده نمود.

ت) سامانه باید بتواند رفتار متفاوت مسیرهای مختلف را تشخیص داده و از هر مسیر به نحو مقتضی استفاده نماید به عبارت دیگر احتمال خراب شدن یا گم شدن بسته در مسیرهای مختلف باید متفاوت در نظر گرفته شود.

ج) در صورتی که گره‌های نامطلوب در سیستم نباشد روش پیشنهادی باید به مسیرهای بهینه همگرا شود.

د) خواص شبکه‌های بی‌سیم سیار و رفتار متغییر با زمان گره‌های بدرفتار و مهاجمین، باعث می‌گردد تا کیفیت مسیرها در طول زمان تغییر نماید. روش ارائه شده باید توانایی تعقیب رفتار مسیرهای مختلف را داشته باشد و خود را با آن وفق دهد.



شکل 5 - عملکرد کلی روش پیشنهادی

از آنجا که روش‌های چند مسیری مانند APSL[13] [10] به‌تنهایی نمی‌توانند محرمانگی اطلاعات را حتی با به‌کارگیری کدبندی در پروتکل‌های چند مسیری تأمین نمایند. چون

گره‌هایی که در نزدیکی مبدأ و مقصد قرار دارند، حتی اگر روی هیچ‌یک از مسیرها نباشند نیز توانایی شنیدن بسته‌های کدشده مختلف را داشته و لذا توانایی بازسازی داده‌های اصلی را دارند. بنابراین به‌منظور تامین محرمانگی و یکپارچگی اطلاعات، لازم است از رمزنگاری هم استفاده شود.

گسترش داده‌ها، به مجموعه‌ای از بسته‌ها که حد مشخصی از کل آنها برای بازسازی داده‌ها کافی است، از یک مزیت جانبی نیز برخوردار است. در روش‌های معمولی هنگامی که بسته با موفقیت دریافت نمی‌گردد معمولاً نیاز به ارسال مجدد وجود دارد و تمام داده باید مجدداً فرستاده شود. با استفاده از روش گسترش داده به اجزای دارای افزونگی، می‌توان به جای ارسال مجدد کل داده‌ها تنها به مقدار نیاز برای رسیدن به آستانه لازم برای کدگشایی، ارسال مجدد را انجام داد و به این ترتیب در عرض باند صرفه‌جویی نمود. این ایده، به ارسال مجدد جزئی موسوم است [10].

بر اساس شکل (5)، عملکرد روش پیشنهادی به این شرح است که، 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، سپس به کمک روش RS به n بسته تبدیل می‌شود که برای بازسازی مجدد اطلاعات k بسته از بسته‌های مزبور مورد نیاز هستند.

سپس به هر بسته کدشده، کد تشخیص یکپارچگی که با استفاده از کلید مشترک محاسبه می‌گردد، اضافه می‌شود و توسط یک الگوریتم تطبیقی و یا بر مبنای تخمین موجود از وضعیت مسیرها، به هر مسیر تعداد مناسبی بسته کدشده تخصیص می‌یابد و بسته‌های مزبور ارسال می‌گردند.

در ارتباط بین گره‌ها، به دلیل وجود گره‌های بدرفتار (گره‌هایی که تنها به استفاده از دیگر گره‌ها برای انتقال بسته‌های خود پرداخته ولی در عوض بسته‌های دیگران را انتقال نمی‌دهند یا اقدام به، قرارگیری در مسیر بسته‌ها نموده و این بسته‌ها را تغییر داده یا به‌طور تصادفی انتقال می‌دهند) و مهاجمین برخی بسته‌های داده، حذف و برخی دیگر تغییر داده می‌شوند. در نهایت تعدادی بسته کدشده داده، به مقصد خواهند رسید، که مقصد ابتدا درستی آنها را به کمک کدهای تشخیص یکپارچگی می‌سنجد و به مجرد دریافت k بسته درست، به کمک الگوریتم کدگشائی RS بسته رمزشده را بازسازی نموده و با استفاده از کلید مشترک رمزگشایی می‌نماید [11] و در نهایت بسته داده را به لایه‌های بالاتر تحویل می‌دهد. علاوه بر این، مقصد مدت زمان مشخصی را پس از موفقیت در بازیابی بسته، منتظر بسته‌های مسیرهای مختلف که با تأخیر می‌رسند، می‌ماند سپس بر مبنای اینکه کدامیک از بسته‌ها صحیح رسیده‌اند، کدامیک در راه تغییر یافته و کدامیک گم‌شده و اصلاً نرسیده‌اند به کمک یک الگوریتم تخمین سطح قابلیت اطمینان و امنیت مسیر، اطلاعات وضعیت مسیر را به‌روز می‌نمایند.

در صورتی که پیام‌های ACK[14] از طرف مبدأ درخواست شده باشد یا بسته‌ای به مقصد در حال ارسال باشد، مقصد اطلاعات آخرین تغییرات وضعیت مسیر را برای مبدأ نیز ارسال می‌دارد. این فرایند به طور متناوب و دو طرفه برای انتقال تمامی بسته‌های داده به‌کار گرفته می‌شود. مهمترین نکته در روش انتقال داده امن و قابل اطمینان چند مسیری، رویکرد اثر محور در طراحی آن است. به این معنی که با در نظر گرفتن این نکته که صرف‌نظر از علت، برای بسته‌های داده در یک شبکه بی‌سیم سیار دو حالت ناخواسته گم شدن و تغییر محتوی را می‌توان متصور شد، در روش پیشنهادی هدف کاهش این دو اثر است.

به عبارت دیگر، هدف روش پیشنهادی، بهبود نسبت بسته‌های تحویل شده صحیح به بسته‌های ارسالی در مقصد است. فرض اصلی گم‌شدن بسته‌ها، به دلیل رفتار خودخواهانه گره‌های میانی و تغییر بسته‌ها به دلیل تهاجم گره‌های بدخواه و به قصد تغییر بسته‌های داده برای به مخاطره انداختن امنیت ارتباط از حیث محرمانگی، یکپارچگی و دسترسی‌پذیری داده‌های منتقل شده است که ساختار ارائه شده با پیش‌بینی چند مسیری انتقال داده‌ها و رمزنگاری در آن نسبت به گم‌شدن یا تغییر تصادفی بسته‌ها مقاوم است.

کدبندی و رمزنگاری داده‌ها

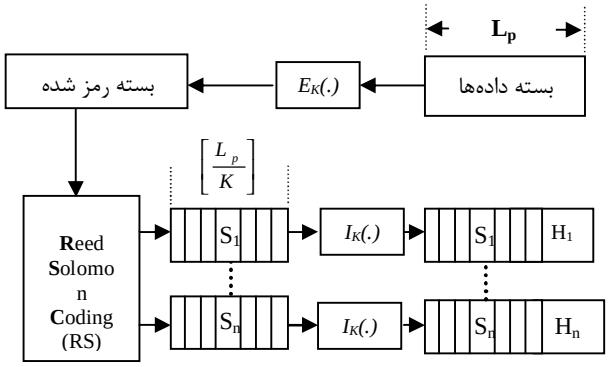
مطابق شکل (6) کدبندی (کدگذاری-کدگشایی) از اجزاء سامانه طراحی شده است و در شبکه‌های بی‌سیم سیار به منظور استفاده بهینه از افزونگی مسیر و با عدم قطعیت‌های موجود در این شبکه‌ها، لازم است افزونگی اطلاعات به نحو مقتضی مورد استفاده قرار گیرد.

در روش ارائه شده مقاله یا SMPDSR، به‌منظور استفاده بهینه از مسیرها و متناظر با امنیت آنها، پیش از ارسال بسته،

ابتدا آن را به کمک کلید مشترک رمز نموده، سپس بسته رمزشده را به کمک کدهای خطی RS(n,k) کدبندی می‌کنیم که در نتیجه بسته مزبور به n بسته، تبدیل می‌شود که طول هر بسته k/n برابر طول بسته اولیه است.

بنابر خواص کدهای RS(n,k)، برای بازسازی مجدد داده‌های اصلی (بسته رمزشده) k بسته از n بسته کدشده، کافی است. به عبارت دیگر کد RS(n,k) توانایی تصحیح n-k بیت حذف شده و $t = [(n-k)/2]$ بیت تغییر یافته در بسته‌ها را دارد (خاصیت عمومی تمامی کدهای خطی) که در آن [] علامت جزء صحیح است.

پارامتر $r = k/n$ که بیان‌کننده نسبت حجم اطلاعات کدشده است، نیز در اینجا با عنوان بازده تعریف می‌شود.



شکل 6 – طرح‌کلی بخش رمزنگاری و کدبندی

عملکرد بخش رمزنگاری و کدبندی در شکل (6) نمایش داده شده است. همان‌طور که در شکل مشاهده می‌شود، ابتدا بسته‌ای با طول L_P به کمک یک الگوریتم رمزنگاری متقارن $E_K(0)$ نظیر AES[15][12] رمز می‌گردد. سپس بسته رمزشده توسط کدکننده RS به n بسته با طول L_P/K تبدیل می‌شود و به کمک یک الگوریتم تولید امضاء دیجیتال یا با کلید متقارن نظیر به‌کارگیری الگوریتم AES در حالت CBC[16]، کدهای بررسی یکپارچگی یا اصطلاحاً خلاصه رمزنگاری (اطلاعات رمز شده برای تشخیص صحت هر بسته دریافتی در مقصد) برای هر بسته کدشده به‌دست آمده و به آن افزوده می‌شود.

در شکل (6) تابع $I_k(0)$ نشان‌دهنده عمل تولید کد بررسی یکپارچگی به کمک کلید مشترک K است و S_iها نشان‌دهنده بسته‌های کدشده و H_iها نشان‌دهنده خلاصه‌های رمزنگاری شده است. همان‌طور که مشاهده می‌شود به هر بسته کدشده، کد بررسی یکپارچگی اضافه شده و نهایتاً بسته آماده ارسال، به‌دست می‌آید [5].

رمزنگاری در سطح بسته اصلی و تولید کدهای بررسی یکپارچگی روشی بهینه از نظر حفظ محرمانگی ارائه می‌دهد چرا که مجزا بودن کدهای بررسی یکپارچگی، به مقصد امکان می‌دهد، رفتار مسیرها را بر تک‌تک بسته‌های کدشده و محافظت شده (سمبل‌ها) بررسی نماید. مشاهده می‌شود این ریزبینی در بررسی رفتار مسیرهای مختلف به دقت تخمین در مورد سطح امنیت مسیرها کمک می‌نماید. دریافت k عدد از n سمبل فرستاده شده، در مقصد کافی است تا بتوان بسته اصلی را بازسازی کرد.

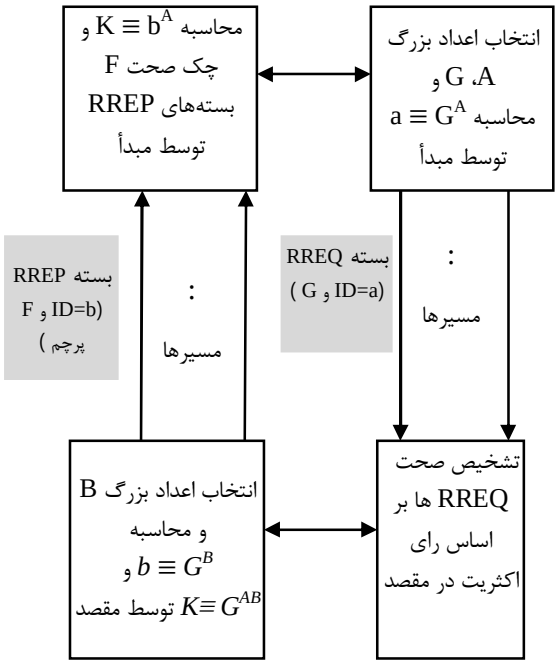
ایجاد کلید برای رمزنگاری

الگوریتم DH[17] در برابر حملات غیر فعال مقاوم، اما این الگوریتم در برابر حمله مردمیانی (حمله‌ای که در آن مهاجم کنترل فعالی بر لایه ارتباطی بین دو قربانی دارد) [13] آسیب‌پذیر است. برای غلبه بر این کاستی و کاهش سربار تأسیس کلید (سرباری که برای بدست آوردن کلید به شبکه تحویل می‌شود) در استفاده از پروتکل‌های چند مسیریابی، در روش پیشنهادی، الگوریتم دیفی و هلمن [14] را به‌صورت زیر در نظر می‌گیریم.

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

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

با توجه به شکل (7)، در این روش، در ابتدا مبدأ عدد تصادفی مانند A و پایه G که یک عدد بزرگ است، انتخاب می‌شود، سپس $a \equiv G^A$ محاسبه می‌شود. حال یک بسته RREQ شامل سرایند معمولی، آدرس مبدأ و آدرس مقصد (شامل ID=a و G) تولید می‌شود. در ادامه، مبدأ بسته RREQ تولیدشده برای گره‌های همسایه ارسال می‌شود و سرانجام بسته‌های RREQ به مقصد می‌رسد. مقصد با دریافت بسته‌های RREQ علاوه بر به‌دست آوردن مسیرهای متعدد، به کمک رای اکثریت قادر به تشخیص تغییرات احتمالی بسته‌های RREQ خواهد بود. بنابراین امنیت مسیرهای دریافتی را می‌تواند تخمین بزند. مقصد یک عدد تصادفی مانند B را انتخاب می‌کند و با استفاده از پایه ارائه شده توسط مبدأ یعنی G می‌تواند $b \equiv G^B$ ، $b \equiv G^{AB}$ و $K \equiv a$ را محاسبه کند.



شکل 7 – طرح کلی تبادل کلید

سپس مقصد یک بسته RREP تولید می‌کند که ID آن را برابر b قرار می‌دهد. مقصد برای هر مسیر یک آرایه پرچم (F) تشکیل می‌دهد که طول این آرایه برابر مسیرهای کشف شده است که برای مسیرهای ناامن مقدار یک "1" و برای مسیرهای امن مقدار صفر در نظر گرفته می‌شود که این مقدار، با استفاده از کلید مشترک استخراج و رمز شده و به بسته RREP افزوده می‌شود.

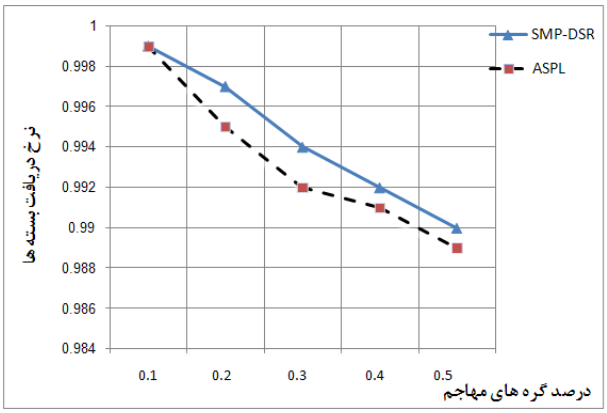
سپس بسته RREP از تمامی مسیرهای موازی، کشف شده و به سمت مبدأ ارسال می‌گردد. مبدأ به کمک b می‌تواند کلید مشترک را به‌صورت $K \equiv (b)^A$ محاسبه نموده و به کمک آن آرایه پرچم را رمزگشایی کند و امنیت مسیرهای یافته شده را ارزیابی کند [15]. این فرایند به‌طور خلاصه در شکل (7) نمایش داده شده است.

با فرض اینکه سربار محاسباتی الگوریتم دیفی و هلمن، معادل دیگر الگوریتم‌های کلید عمومی باشد، این الگوریتم تنها یک‌بار و آن هم در زمان تأسیس کلید به‌کار گرفته می‌شود و بقیه عملیات رمزنگاری به صورت متقارن انجام می‌شود و سربار محاسباتی تحمیل شده به گره‌ها در برابر امنیت به‌دست آمده ناچیز است [16].

شبیه‌سازی و تحلیل نتایج

در شبیه‌سازی الگوریتم‌ها، از ابزار شبیه‌سازی $NS2^{18}$ [17] استفاده شده و محیط شبیه‌سازی در وسعت 3000×3000 متر مربع (9کیلومتر مربع) در نظر گرفته شده است. در پروتکل پیشنهادی با افزایش درصد گره‌های مهاجم نرخ دریافت بسته‌ها کاهش می‌یابد و تقریباً این نرخ با روش APSL در جایی‌که درصد گره‌های مهاجم 0/50 شود، برابر است اما مهمترین نکته در روش پیشنهادی به‌کارگیری رمزنگاری است، به‌گونه‌ای که فقط در ابتدای ارتباط با تبادل یک کلید، می‌توان پیام‌ها را رمز کرد.

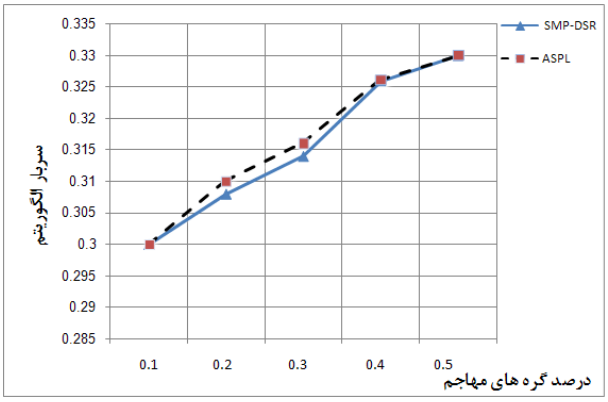
پیام‌های رمزشده، به صورت پیام‌های کدشده در می‌آید و در صورت شناسایی روش کدگذاری، توسط مهاجمین به علت به‌کارگیری رمزنگاری قابل کشف نیستند. در روش APSL گره‌های همسایه مبدأ و مقصد پیام‌های کدشده زیادی را دریافت می‌کنند که مهاجمین از این ضعف امنیتی استفاده کرده و می‌توانند پیام‌ها را شنود و کشف کنند.



شکل 8 - متوسط تحویل بسته‌ها در SMPDSR و APSL

نتایج شبیه‌سازی SMPDSR و APSL که چگونگی نرخ دریافت بسته‌ها در شرایطی که درصد گره‌های مهاجم در شبکه، افزایش می‌یابد در شکل (8) نمایش داده شده است که نشان می‌دهد به‌طور متوسط نرخ دریافت بسته‌ها حدوداً 1% در روش پیشنهادی بیشتر از APSL است گرچه این میزان اندک است اما بهبود در سرعت انتقال را نشان می‌دهد. ساختار APSL باعث می‌شود، همسایه‌های مبدأ و مقصد پیام‌های کد شده زیادی را شنود و دریافت کنند که به این ترتیب امنیت پیام‌ها در خطر می‌افتد این نقص در روش ارائه شده وجود

ندارد. در واقع روش پیشنهادی ضمن برتری در کارایی و سرعت انتقال، با برخورداری از استحکام امنیتی، ضعف امنیتی روش APSL را پوشش می‌دهد. نتایج شبیه‌سازی SMPDSR و APSL که چگونگی سربار الگوریتم در شرایطی که درصد گره‌های مهاجم در شبکه، افزایش می‌یابد در شکل 9 نمایش داده شده است.



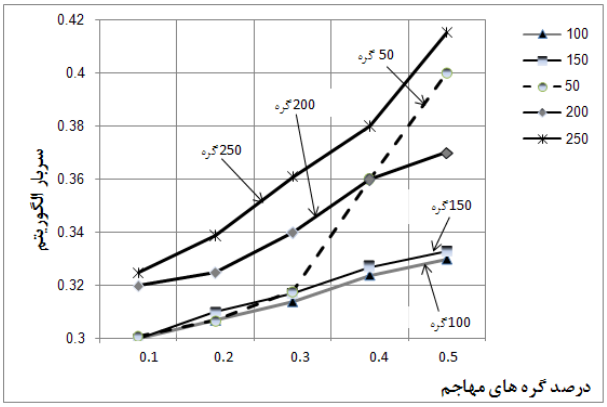
شکل 9 - سربار الگوریتم در SMPDSR وAPSL

در SMPDSR برای جلوگیری از شنود همسایه‌های مبدأ و مقصد، از رمزنگاری استفاده شده است که این موجب ایجاد سربار اضافی برای شبکه می‌شود اما با افزایش درصد مهاجمین در روش پیشنهادی، سربار اضافی جبران می‌شود و به‌طور متوسط 12% سربار کاهش می‌یابد.

در روش پیشنهادی با به‌کارگیری الگوریتم ساده‌ای که در شکل (4) نمایش داده شده است پیام‌ها بر روی مسیرها بارگذاری می‌شوند. اساساً بین تحویل بسته و سربار رابطه‌ای بسیار قوی وجود دارد. طبیعتاً عدم توفیق در انتقال داده‌ها منجر به ارسال مجدد می‌شود که باعث افزایش سربار می‌گردد یا حتی منجر به عدم موفقیت در انتقال بسته، افت در عملکرد شبکه و جستجو برای دسته مسیر جدید نیز می‌گردد.

یکی از مهم‌ترین نقاط قوت روش پیشنهادی مقاومت بالای آن در برابر مهاجمین 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 دسته مسیرهای بهینه حذف می‌شوند.

در شکل (10) دیده می‌شود در حالت کلی، شبکه با افزایش درصد گره‌های مهاجم، سربار آن افزایش می‌یابد زیرا گره‌های نامطلوب با ایجاد اختلال در ارتباطات و کم‌کردن مسیر انتقال داده، باعث افزایش ترافیک می‌شوند. شبکه با داشتن 50 گره در جایی که نسبت گره‌های مهاجم به کل از 0/10 به 0/30 می‌رسد به علت کم شدن مسیرهای سالم سربار آن، با شیب خطی ملایم افزایش می‌یابد و زمانی که به 0/30 می‌رسد سربار آن به‌طور ناگهانی افزایش می‌یابد، دلیل این امر این است که با توجه به وسعت شبکه و درصد گره‌های مهاجم، مسیرهای انتقال داده به کمترین حد ممکن می‌رسند (فرض بر این است که حداقل یک مسیر سالم وجود داشته باشد) و تمام ترافیک از این مسیرها عبور می‌کند پس سربار افزایش می‌یابد زیرا داده‌ها برای انتقال باید منتظر بمانند تا نوبت به آنها برسد. همچنین افزایش گره‌های نامطلوب، باعث افزایش اختلال در عملکرد شبکه می‌شود.



شکل 10 - سربار در الگوریتم SMPDSR با تعداد گره‌های مختلف

برای انتقال داده، شبکه با داشتن 100 یا 150 گره، سربار الگوریتم با افزایش درصد گره‌های مهاجم به‌صورت نرمال افزایش می‌یابد زیرا با توجه به دامنه انتقال بی‌سیم و وسعت شبکه، تعداد گره‌ها مناسب است. افزایش گره‌های شبکه به 200 و 250 گره، سربار را افزایش می‌دهد زیرا مبدأ باید اطلاعات بیشتری از مسیرها را در حافظه خود نگه دارد چون با افزایش گره‌ها، طول گام مسیرها افزایش می‌یابد همچنین مبدأ باید تلاش بیشتری در تفکیک مسیرهای مجزا، انجام دهد. گره‌های نامطلوب هم می‌توانند این سربار را با اخلال در انتقال داده، افزایش دهند. مشکل‌ترین حالت در شبیه‌سازی شبکه، در حالت با 250 گره است زیرا افزایش گره‌ها تعداد گام‌های بین مبدأ و مقصد را افزایش می‌دهد و پیدا کردن مسیرهایی که گره‌های مجزا داشته باشند نیاز به پردازش بیشتری دارد. با توجه به تراکم گره‌ها در شبکه، گره‌های مهاجم می‌توانند

اطلاعات بیشتری از همسایه‌های خود کسب کنند و شناخت آنها نیز مشکل‌تر می‌شود. در نهایت می‌توان نتیجه گرفت که اگر چه درصد گره‌های مهاجم تأثیر به‌سزایی در سربار دارند اما نسبت وسعت شبکه با تعداد گره‌ها را نیز باید در نظر گرفته شود.

نتیجه‌گیری

در مدل پیشنهادی تعداد زیادی از هواپیماهای مختلف، با نوعی شبکه بی‌سیم سیار خاص در قالب طرح عملیاتی ارائه شده است. در این مدل هر هواپیما، به صورت یک گره بی‌سیم سیار است که می‌تواند به‌طور پویا در هر نقطه از فضای عملیاتی، عملیات ارتباط، هدایت و ناوبری را انجام دهد و به طور آزادانه بر اساس مقتضیات عملیات، جابه‌جا شده و در حکم میزبان برای تبادل فرامین یا در نقش مسیریاب، فعالیت کند. برای داشتن یک شبکه امن و پیش‌گیری از هر گونه اختلال در فضای عملیات و جلوگیری از عملیات اختلال توسط دشمن به پروتکل ارتباطی مناسب و امن نیاز است که برای شبکه خاص مورد نظر، پروتکل SMPDSR پیشنهاد و ارزیابی گردید و با پروتکل APSL که در شبکه‌ای مشابه، کاربرد دارد، مقایسه شد. در حالت کلی اصول عملکرد هر دو پروتکل SMPDSR و APSL یکسان است ولی پروتکل SMPDSR در حفظ محرمانگی به کمک رمزنگاری متقارن با کلید مشترک و نیز الگوریتم بارگذاری، با پروتکل APSL متفاوت است. در این پروتکل‌ها با به‌کارگیری سامانه بازخورد برای تعقیب وضعیت مسیرها به کمک تخمین PSI به خوبی عمل نموده و حتی در شرایط سخت موفق عمل می‌نماید. از طرف دیگر با استفاده از کدبندی داده‌ها و استفاده از چندین مسیر، توانایی آزمودن مسیرهای مختلف به صورت سریع و موازی حاصل می‌شود که این مورد از مزیت‌های واضح و مستقیم انتقال داده چند مسیری علاوه بر مسیریابی چند مسیری است. یکی از معایب APSLشنود همسایه‌های مبدأ و مقصد است که می‌توانند پیام‌های کدشده زیادی را دریافت کنند. برای رفع این عیب، از رمزنگاری استفاده می‌شود که باعث افزایش سربار می‌شود، برای جبران سربار تحمیل شده به خاطر رمزنگاری از روش پیشنهادی استفاده می‌شود. نتایج شبیه‌سازی SMPDSR و APSL چگونگی نرخ دریافت بسته‌ها در شرایطی که درصد گره‌های مهاجم در شبکه، افزایش می‌یابد نمایش داده شده، همچنین چگونگی سربار الگوریتم در شرایطی که درصد گره‌های مهاجم در شبکه، افزایش می‌یابد ارائه گردیده است که برتری روش پیشنهادی را تأیید می‌کند و نشان داد که از مهم‌ترین نقاط قوت روش پیشنهادی، مقاومت بالای آن در برابر مهاجمین و سرعت انتقال بهتر در بسته‌هاست.

پی نوشت

1 Dynamic Source Routing
2 Multipath
3 Non-uniform Adaptive Loading
4 Packet overhead
5 Congestion
6 Ad hoc On-Multipath distance vector
7 Split Multipath Routing
8 Multipath Dynamic Source Routing
9 Optimum Non-uniform Adaptive Loading
10 Read-Solomon
11 Path State Information
12 Secure Multipath and Dynamic Source Routing
13 Adaptive Path Selection and Loading
14 Acknowledgement
15 Advanced Encryption standard
16 Cipher Block Chaining
17 Diffie-Hellman
18 Network Simulation 2

منابع و مراجع

[1] Johson, B., Maltz, D., Broch, D., Josh., *"DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks"*, in Ad Hoc Networking, Edited by Charles E. Perkins, Chapter 5, Addison-Wesley, pp. 139-172, 2001

[2] Nasipuri, A., Das., S.R., *"AOMDV: on-demand multipath routing for mobile ad hoc networks"*, Proceedings of the 8th Int. CONF. ON Computer Communications and Networks (IC3N), Boston, MA., 1999

[3] Lee, S., Gerla, M., *"SMR: split multipath routing with maximally disjoint paths in ad hoc networks"*, Proc. Of IEEEICC, Vol.10, pp.3201-3205, 2001

[4] Nasipuri, A., Castaneda, R., Das., S.R., *"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), 6(4): 339-349, 2001

[5] علیرضا رضائی، *" طراحی و شبیه‌سازی یک کانال امن و مقاوم در برابر حملات متعارف در شبکه‌های بی‌سیم سیار بر اساس چند مسیریابی مبتنی بر مبدأ"* ، دانشگاه علوم و فنون هوائی شهید ستاری، 1389

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

[7] Reed, I.S., Solomon, G., *"Polynomial codes over certain finite fields"*, SIAM Journal of Applied Math, pp. 300-304, 1960

[8] Ayanoglu, E., Chih-Lin, I., Gitlin, R.D., Mazo, J.E., *"Diversity coding for transparent self-healing and fault-tolerant communication networks"*, Communications, IEEE Transactions on, Vol.41, pp. 1677-1686, 1993

[9] Wenjing, L., Yuguang, W., *"SPREAD: enhancing data comfidentiality in the mobile ad-hoc network"*, IEEE INFOCOM 2004, Hang Kong, China, 2004

[10] Ahmad, Kh, Ghassem, S., *"Misbehavior resilient multipath data transmission in mobile ad hoc networks"*, Institute for Studies in Theoretical Physics and Mathematics (IPM), 2006

[11] Balasubramanian, A., Mishra, S., Sridhar, R., *"Analysis of a hybrid key management solution for ad hoc networks"*, IEEE Wireless Communications and Networking Conference, 2082-2087, 2005

[12] Stinson, R., *"Cryptography theory and practice"*, university of Waterloo Ontario, Canada, 2006

[13] Convery, S., *"Network security architectures"*, 2004

[14] Diffie, W., Hellman, M.E., *"New directions in cryptography"*, IEEE Transactions on Information Theory, pp. 644-654, 1976

[15] Shoup, Victor, *"A computational introduction to number theory and algebra (version 1)"*, Cambridge University Press, 2005

[16] Diffie, W., Hellman, M.E., *"New directions in cryptography"*, IEEE transactions on Information Theory, Vol. 22, pp. 644-654, 1976

[17] Altman, E., Jimenez, T., *"NS simulator for beginners"*, Lecture Notes. Univ.de Los Andes, Merida, Venezuela and ESSI.Sophia-Antipolis, France, 2003