ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

حمله به سیستم طیف گسترده امن مبتنی بر روش پرش فرکانس تفاضلی متغیر

فرشید فرحت
تهران، دانشگاه صنعتی شریف، دانشکده مهندسی برق
farhat@ee.sharif.edu

چکیده

مخابرات طیف گسترده از لحاظ ایجاد بستر امن برای انتقال داده در لایه فیزیکی بسیار حائز اهمیت است. یکی از روش‌های معمول در طیف گسترده روش پیشرفته پرش فرکانس تفاضلی متغیر است که مزیت‌های متعددی از جمله رهگیری سریعتر، ردگیری بهتر و ضد اختلال مرحله ردگیری دارد. همچنین به دلیل تغییر تابع انتقال فرکانس با توجه به داده ارسالی و ثبات خطی، سیستم مخابراتی مبتنی بر آن حملات شناخته شده تا قبل از خود را دفع می‌کند. در این مقاله حمله جدیدی با توجه به ساختار سیستم، به صورت هوشمند پیشنهاد می‌شود که با پیچیدگی قابل قبول می‌تواند کلید مخفی سیستم مخابراتی را بدست آورد و در نهایت مانع از ایجاد ارتباط مورد نظر بین فرستنده و گیرنده شود. همچنین نکات ضعف سیستم بررسی می‌شود و راه‌کارهایی جهت ایمن‌سازی آن ارائه می‌شود.

واژه‌های کلیدی

مخابرات طیف گسترده، پرش فرکانس تفاضلی متغیر، رهگیری و ردگیری، تابع انتقال فرکانس، حمله شکست کلید سیستم.

۱- مقدمه

توان سیگنال ارسالی در مخابرات کلاسیک به دلیل پهنای باند محدود سیگنال ارسالی بالاتر از سطح توان نویز است، تا گیرنده در پهنای باند مذبور بتواند بسادگی سیگنال را دریافت و آشکارسازی کند. به همین منوال دشمن نیز چنانچه حوزه زمانی، فرکانسی و فضایی سیگنال را کشف کند (یعنی در بازه پوشش آن قرار گیرد)، براحتی قادر است که سیگنال را آشکارسازی کند. در اینجا می‌توان فرض کرد که فرستنده سیگنال ارسالی را رمزنگاری (متقارن یا نامتقارن) کرده و برای گیرنده ارسال می‌کند. با وجود اینکه دشمن نمی‌تواند به محتوای پیام ارسالی دست یابد ولی براحتی با اختلال در باند ارسالی سیگنال قادر است که مانع ارسال پیام از فرستنده به گیرنده شود. این حمله همانند حمله انکارسرویس (Denial of Service) در امنیت شبکه است که در لایه فیزیکی سیستم عمل می‌کند و باعث قطع ارتباط بین فرستنده و گیرنده می‌شود. لذا در مخابرات کلاسیک دشمن با شنود طیف فرکانسی قادر است که باند مربوطه را شناسایی و تخریب کند. در نتیجه باید روش‌هایی اتخاذ گردد که منابع مورد استفاده برای ارسال سیگنال مانند زمان، فرکانس و حتی فضاء از دید دشمن مخفی بماند تا حمله به سیستم عملی نشود.

مخابرات طیف گسترده به عنوان راه‌کار مناسبی در مقابل حملات اختلال دشمن در مقابل مخابرات کلاسیک مطرح شده است. در مخابرات طیف گسترده با گسترش طیف سیگنال ارسالی چگالی طیف توان سیگنال را تا زیر آستانه چگالی طیف نویز سفید کاهش می‌دهند تا احتمال آشکارسازی سیگنال بسیار کاهش یابد. در حالت کلی‌تر با توجه به اطلاعات دشمن در مورد سیستم و هدف او از حمله، می‌توان تقسیم‌بندی دقیق‌تری بر انواع شنود داشت. در واقع تعیین ویژگی‌های سیگنال برای استخراج اطلاعات محتوای آن، مستلزم آن است که ابتدا حوزه زمانی، فرکانسی و فضایی سیگنال کشف شود به این مرحله اصطلاحا مرحله کشف پوشش (Coverage) گفته می‌شود. سپس بایستی حضور سیگنال تشخیص داده شود (مرحله آشکارسازی یا Detection). سپس ویژگی‌های مهم سیگنال مانند فرکانس حامل و مدولاسیون ردیابی شود (مرحله ردیابی یا Interception) و در نهایت در مرحله آخر خصوصیات دقیق سیگنال برای بدست آمدن محتوای آن تعیین می‌شود (مرحله بهره‌برداری یا Exploitation). مراحل ذکر شده به مانند یک زنجیره مارکف بایستی یکی پس از دیگری صورت پذیرد در نتیجه احتمال بهره‌برداری (رابطه ۱) حاصلضرب احتمال‌های شرطی در احتمال کشف پوشش خواهد بود. [۵]

$$Exploitation \leftrightarrow Interception \leftrightarrow Detection \leftrightarrow Coverage \quad (۱)$$
$$Prob(E) = Prob(E|I).Prob(I|D).Prob(D|C).Prob(C)$$

برای کاهش احتمال بهره‌برداری Prob(E) بایستی مولفه‌های احتمال شرطی را حداقل کرد. کاهش احتمال کشف پوشش Prob(C) در اختیار فرستنده نیست و به هوشمندی دشمن بستگی دارد که بر اساس روش‌هایی چون تشخیص جهت دریافت (Direction of Arrival) بتواند محل پوشش را تشخیص دهد. احتمال بهره‌برداری به شرط ردیابی Prob(E|I) نیز تقریبا برابر یک است، زیرا با ردیابی سیگنال تقریبا تمام ویژگی‌های مورد نیاز بدست خواهد آمد. روش کاهش احتمال ردیابی (Interception) مقدار Prob(D|C) را می‌کاهد و روش کاهش احتمال آشکارسازی (Detection) برای کم‌کردن Prob(I|D) مطرح می‌شود. روش‌های هر گروه را با مجزا کردن خصوصیات هدف حمله می‌توان به صورت شرطی مستقل فرض کرد.

برای کاهش احتمال آشکارسازی Prob(D|C) بایستی توان دریافتی در آنتن گیرنده غیرمجاز به حد کافی پایین باشد ولی این توان بایستی درحدی باشد که گیرنده مجاز بتواند سیگنال را دمدوله کند. در نتیجه بر اساس رابطه ۲ با افزایش ضریب "دوره زمانی (T) * پهنای باند (W)" سیگنال می‌توان حاشیه امن احتمال کم آشکارسازی (LPD) را افزایش داد، که Q ضریب کیفیت سیستم است و Q با حاشیه امن احتمال کم آشکارسازی (LPD) رابطه مستقیم دارد [۷].

$$Q = T * W\frac{(SNR)_{Wiretap}}{(SNR)_{Authentic}} \quad (۲)$$

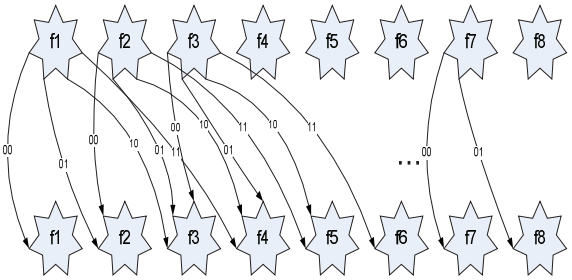
با فرض دوره زمانی و پهنای باند ثابت برای سیگنال ارسالی پارامتر LPD تقریبا تثبیت‌شده است. بر این اساس در این مقاله روش کاهش احتمال ردیابی (LPI) بیان می‌شود. یکی از ایده‌های مطرح شده در این زمینه رمزنگاری در باند میانی است. بدین معنی که با استفاده از الگوریتم‌های رمزنگاری (بخصوص رمزهای متقارن دنباله‌ای) مدولاسیون شبه‌تصادفی (Pseudo Random Modulation) در باند میانی مانند پرش فرکانس تفاضلی متغیر انجام می‌شود.

بر این اساس در بخش بعدی به معرفی روش پرش فرکانس تفاضلی پرداخته می‌شود، سپس مزایا و معایب آن بررسی می‌شود و روش بهبود یافته آن پرش فرکانسی تفاضلی متغیر بیان می‌شود و سیستم طیف گسترده مبتنی بر آن توضیح داده می‌شود. در نهایت ضعف‌های سیستم طراحی شده بررسی می‌شود و حملات خطی کارا بر روی آن انجام می‌شود و در نهایت راه‌کارهایی برای بهبود آن ارائه می‌گردد و در ادامه جمع‌بندی و نتیجه‌گیری از بحث بیان می‌شود.

۲- پرش فرکانس تفاضلی

در پرش فرکانس معمولی [۲و۳] کانال‌های فرکانسی بطور ناهمبسته از داده‌ها انتخاب شده و سیگنال داده در کانال مورد نظر مدوله می‌شود. در سیستم پرش فرکانس تفاضلی (Differential Frequency Hopping) کانال فرکانسی، فرستنده در آغاز ارسال یک کانال فرکانسی را بطور تصادفی اختیار کرده و داده اولیه را در آن کانال مدوله می‌کند. سپس فرکانس کانال پرش بعدی بطور همبسته بر اساس کانال فرکانسی قبلی و داده حاضر تعیین می‌شود. [۶] فرکانس خروجی ترکیب کننده فرکانس (Frequency Synthesizer) تابعی از داده حاضر و کانال فرکانسی قبلی است که معمولا به صورت گراف جهت‌داری بیان می‌شود که رئوس گراف کانال‌های فرکانسی موجود هستند و یال‌های جهت‌دار ارتباط پرش‌های متوالی را بر اساس داده حاضر مشخص می‌کنند.

همانطور که در شکل ۱ نشان داده شده است، ستاره‌های بالایی هشت کانال فرکانسی قبلی‌اند که با ۲بیت داده به همان هشت کانال فرکانسی بعدی نگاشت می‌شوند. در واقع گراف مورد نظر تابع انتقال فرکانس (Frequency Transition Function) را نمایش می‌دهد.



شکل ۱: گراف تابع انتقال فرکانس

گیرنده با استفاده از نمونه‌بردار مبدل آنالوگ به دیجیتال پهنای باند سیگنال را جاروب می‌کند و پس از گرفتن تبدیل فوریه سریع از نمونه‌ها می‌تواند کانال فرکانس حامل بیشترین انرژی را تشخیص دهد و خود را با فرستنده همزمان کند. سپس گیرنده رشته فرکانس‌های ارسالی را دنبال می‌کند و در واحد تصمیم‌گیری نرم با کمک الگوریتم ویتربی بمانند کدگشایی کانولوشن محتمل‌ترین رشته داده ارسالی کدبرداری می‌شود.

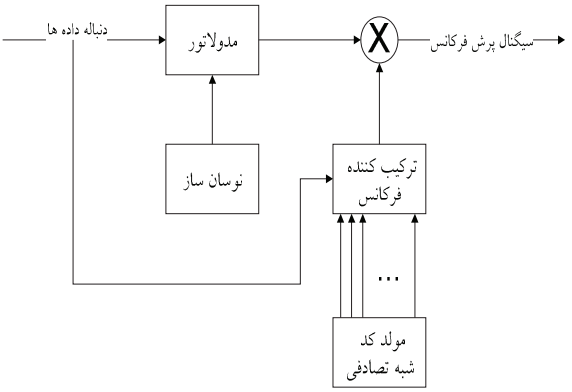
مزیت عمده این روش امکان آشکارسازی به صورت ناهمزمان (Non-Coherent Detection) می‌باشد، زیرا گیرنده بدون نیاز به سیگنال راهنما می‌تواند با جستجو در طیف فرکانسی چنانچه گفته شد با فرستنده همزمان شود، لذا رهگیری در روش پرش فرکانس تفاضلی به راحتی قابل دستیابی است. همچنین اگر تابع انتقال فرکانس همانند کدهای کانولوشن بیشترین فاصله آزاد را دارا باشد [۸]، قابلیت تصحیح خطای سیستم در مقابل نویز و اختلال بسیار بالا می‌رود، لذا سیستم از قابلیت ضداختلال (Anti-Jamming) و احتمال کم آشکارسازی (LPD) خوبی برخوردار است.

از دیدگاه امنیت چنانچه گراف تابع انتقال فرکانس را به عنوان کلید محرمانه در نظرگرفته شود، حجم کلید با تعداد فرکانس‌ها رشد می‌کند که چندان مطلوب نیست. از طرف دیگر اگر گراف‌هایی مطلوب باشند که فاصله آزاد بیشینه دارند، دشمن فضای جستجوی محدودتری برای یافتن گراف خواهد داشت. علاوه بر این دشمن با شنود فرکانس‌های حامل بیشترین انرژی می‌تواند اطلاعاتی در رابطه با گراف (کلید سیستم) دریابد و با تکرار شنود کم‌کم بطور کامل به تابع انتقال فرکانس دست یابد. لذا دشمن هوشمند می‌تواند با احتمال خوبی سیگنال طیف گسترده را ردیابی کرده و از آن بهره‌برداری کند، در نتیجه سیستم پرش فرکانس تفاضلی متغیر [۹] پیشنهاد شد.

۳- پرش فرکانس تفاضلی متغیر

روش پرش فرکانس تفاضلی متغیر (Variable Differential Frequency Hopping) همانطور که در شکل ۲ نمایانده شده است، علاوه بر تابع انتقال فرکانس و داده حاضر از یک مولد کد شبه تصادفی نیز برای انتخاب کانال فرکانسی فعلی بهره می‌گیرد. در واقع ترکیب کننده فرکانس از یک گراف انتقال فرکانس متغیر با زمان استفاده می‌کند. مولد کد شبه‌تصادفی در روش ادعا شده در [۹] یک ثبات خطی (Linear Feedback Shift Register) است.

در ابتدای ارسال پیام فرستنده و گیرنده بایستی بر سر حالت اولیه ثبات خطی توافق کنند. سپس داده ارسالی در فرستنده بر اساس گراف انتقال فرکانس روش DFH مدوله می‌شود، ولی بجای تولید دنباله فرکانس ارسالی دنباله‌ای از شماره گره‌ها تولید می‌شود. سپس در هر پرش شماره گره حاصل از مدولاسیون با حالت فعلی ثبات خطی در آن پرش بیت به بیت باینری جمع می‌شود و عدد حاصل به منزله شماره کانال فرکانس ارسالی محسوب می‌شود. در واقع در هر پرش ستاره‌های بالایی گراف انتقال فرکانس بر اساس حالت فعلی ثبات خطی یک شیفت شبه‌تصادفی داده می‌شوند، در نتیجه این روش بنام پرش فرکانس تفاضلی متغیر خوانده می‌شود.



شکل ۲: سیستم پرش فرکانس تفاضلی در فرستنده

روش پرش فرکانس تفاضلی متغیر مزایای روش پرش فرکانس معمولی را به ارث می‌برد، لذا روش VDFH از ویژگی‌های AJ و LPD برخوردار است. در روش VDFH تابع انتقال فرکانس را می‌توان در اختیار همه قرار داد و در عوض حالت اولیه و چندجمله‌ای اولیه فیدبک ثبات خطی را به عنوان کلید امن سیستم در نظر گرفت. با این ایده دشمن به روش قبل دیگر قادر نخواهد بود که سیگنال طیف گسترده را ردیابی کند. همچنین با غیرخطی کردن ساختار شبه‌تصادفی مولد کد می‌توان امنیت سیستم و خاصیت LPE را بهبود بخشید. مشکل عمده این روش همان توافق اولیه فرستنده و گیرنده است و اینکه چگونه فرآیند رهگیری در گیرنده عملی شود.

۴- سیستم مبتنی بر پرش فرکانس تفاضلی متغیر

سیستم مبتنی بر پرش فرکانس تفاضلی متغیر [۱] تعداد M کانال فرکانسی را به K گروه بر مبنای رابطه ۳ تخصیص می‌دهد، که Si حالت ثبات خطی اول log2M-طبقه‌ای است و Dec(.) نشاندهنده مقدار دهدهی عبارت داخل پرانتز است.

$$\forall i \in \{0,1,\dots,M-2\}: \quad f_{Dec(S_i)} \in Group_{(i \bmod K)} \qquad (۳)$$

همچنین ترتیب فرکانس‌های داخل گروه‌ها با رابطه ۴ تعیین می‌شود.

$$\forall i \in \{0,1,\dots,M-2\}: \quad Order@Group(f_j) = \begin{cases} \left\lfloor \frac{i}{K} \right\rfloor & \text{if } \exists i: j = Dec(S_i) \\ N-1 & \text{if } j = 0 \end{cases} \qquad (۴)$$

الگوی انتخاب گروه‌ها و نوع چیدمان فرکانس‌های آن‌ها توسط حالت ثبات خطی دوم با تعداد طبقات بزرگتر مساوی log2M (با فرض $log_2 L = l > m = log_2 M$ بیت حافظه) صورت می‌گیرد. در واقع log2K بیت اول حالت ثبات خطی دوم مشخص کننده گروه فعال است و log2M-log2K بیت در ادامه نوع چیدمان را تعیین می‌کند. توجه کنید که fM-1 بایستی بطور اجباری در یکی از گروه‌ها قرار گیرد، چون در رابطه ۳ مقداری نمی‌پذیرد. در ابتدای ارسال سمبل‌ها یک گروه از گراف بطور تصادفی توسط فرستنده به عنوان گره اول انتخاب می‌شود ولی در ارسال‌های بعدی با توجه به گروه فعال، نوع چیدمان و سمبل حاضر کانال فرکانسی مشخص می‌شود و داده بر روی مدوله و ارسال می‌شود.

از نظر امنیتی فرض بر این است که گیرنده تنها از حالت و چندجمله‌ای فیدبک ثبات خطی اول (کلید سیستم) مطلع است. گیرنده برای همزمان کردن خود نیاز دارد که دنباله خروجی به طول حافظه ثبات دوم را با کمک اطلاعات ثبات اول (که مشخص کننده گروه‌ها و ترتیب فرکانس‌های داخل گروه‌هاست) بدست آورد. سپس با کمک چندجمله‌ای فیدبک ثبات دوم و حل دستگاه

معادلات خطی حالت اولیه ثبات دوم را بدست آورده و در نهایت می‌تواند خود را با فرستنده همزمان سازد. بعد از این مرحله مشابه آنچه در مورد روش DFH گفته شد، گیرنده با استفاده از الگوریتم گروه‌بندی، نوع چیدمان و الگوریتم ویتربی به دنباله سمبل‌های ارسالی خواهد رسید.

۵- حملات خطی بر سیستم مبتنی بر پرش فرکانس تفاضلی متغیر

حملات خطی بر سیستم معرفی شده در بخش قبلی (سیستم مبتنی بر پرش فرکانس متغیر) براحتی از ساختار خطی سیستم نتیجه می‌شود. این حملات از نوع اول یعنی حمله متن رمزشده تنها است. مهاجم قادر است که طیف گسترده سیگنال را جاروب کند و در هر پرش فرکانس حامل ارسالی را شناسایی نماید، اما تا قبل از شکستن سیستم نمی‌تواند پرش بعدی را حدس بزند و در آن اختلال ایجاد کند. در نتیجه دشمن قادر است که دنباله فرکانس‌های حامل را شنود کند. بدین ترتیب دشمن می‌تواند تخمین مناسبی از تعداد کانال‌های فرکانسی (M) داشته باشد.

کلید سیستم همانطور که گفته شد حالت اولیه و چندجمله‌ای فیدبک ثبات خطی اول است. حملات وقتی قابل پیاده‌سازی خواهد بود که مهاجم به کلید سیستم دست یابد و یا اینکه بتواند فرکانس پرش بعدی را به گونه‌ای با احتمال بالا حدس بزند، که این کار مستلزم بدست آوردن حالت اولیه و چندجمله‌ای فیدبک ثبات خطی دوم هم هست. در واقع ثبات خطی دوم فرکانس‌های حامل را به صورت شبه‌تصادفی از میان گروه‌های تثبیت‌شده توسط ثبات اول انتخاب می‌کند. حملات با توجه به اطلاعات در اختیار دشمن می‌تواند به صورت غیرفعال پیاده‌سازی شود.

۵-۱ حمله خطی به ثبات اول

اگر به نحوه دسته‌بندی کانال‌های فرکانسی (رابطه ۳) توجه شود، می‌توان ماتریس M_{GROUP} را مطابق رابطه ۵ ارائه داد که هر سطر ماتریس نشان‌دهنده اندیس فرکانس‌های یک گروه است، که مطابق رابطه ۴ مرتب شده‌اند و طبیعتا هر ستون اندیس‌های هم-مرتبه گروه‌ها را نشان می‌دهد. نکته جالب دیگر آن است که اندیس‌ها به صورت ستون به ستون در ماتریس پر می‌شوند.

$$M_{GROUP} = \begin{bmatrix} S_0 & S_K & S_{2K} & & S_{M-K} \\ S_1 & S_{K+1} & S_{2K+1} & \cdots & S_{M-K+1} \\ S_2 & S_{K+2} & S_{2K+2} & & S_{M-K+2} \\ & \vdots & & \ddots & \vdots \\ S_{K-1} & S_{2K-1} & S_{3K-1} & \cdots & S_{M-1} \end{bmatrix}_{K*M/K} ; \quad (۵)$$

$$\forall S_i \in GF(M = 2^m)$$

در نگاه ساده شاید چنین به نظر آید که مرتبه پیچیدگی بدست آمدن ماتریس MGROUP برابر با !M است، ولی چنین نیست. در بدترین حالت با فرض اینکه ثبات خطی اول یک دنباله ماکزیمال تولید خواهد کرد، در نتیجه تمام M-1 حالت ممکن در میدان GF(M=2m) تولید خواهند شد. اگر فرض شود که چندجمله‌ای اولیه فیدبک ثابت است، تنها حالت اولیه ثبات خطی اول تعیین کننده محل شروع پرشدن ماتریس MGROUP است و با توجه به نکته گفته شده می‌توان فهمید که بازهم اندیس‌های مشابهی در هر سطر ماتریس MGROUP قرار خواهند گرفت. در واقع با تغییر حالت اولیه ثبات اول تنها سطرها و ستون‌های ماتریس MGROUP شیفت می‌یابند (حتی جابجا نمی‌شوند تنها شیفت می‌یابند). این نکته مرتبه پیچیدگی جستجوی ماتریس گروه‌بندی را به شدت کاهش می‌دهد. توجه کنید که تعداد حالت‌های ممکن شیفت‌یافته ماتریس گروه‌بندی برابر K*M/K یا همان M حالت است.

برای محاسبه مرتبه پیچیدگی توجه کنید که شیفت ستونی جایگشت گروه‌ها را به هم نمی‌زند، لذا در فرآیند حمله برای شکستن ثبات دوم نقشی ندارد. پس تعداد شیفت‌های موثر ماتریس همان K تاست. تعداد چندجمله‌ای‌های اولیه در GF(M) برابر $\frac{\varphi(M-1)}{\log_2 M}$ است (که تابع $\varphi(x)$ تعداد اعداد کوچکتر از x که نسبت به آن اولند را نشان می‌دهد)، که این مرتبه پیچیدگی با توجه به مقدار محدود M چندان هم بزرگ نیست. در نتیجه مرتبه پیچیدگی جستجوی کامل ماتریس گروه‌بندی برابر با $K * \frac{\varphi(M-1)}{\log_2 M}$ خواهد شد.

مهاجم برای پیاده‌سازی حمله خود به خروجی ثبات دوم نگاه می‌کند تا رشته‌ای از گروه‌های فعال را حدس بزند، زیرا ثبات دوم در هر پرش یک گروه فعال به همراه یک فرکانس داخل گروه را برمی‌گزیند. شاید در اینجا به نظر می‌آید که احتمال اینکه در هر پرش گروه فعالی حدس زده شود، برابر تعداد گروه‌ها (K) است و لذا برای حدس دنباله‌ای به طول n از گروه‌های فعال مرتبه پیچیدگی حدس Kn می‌شود. ولی با توجه به ساختار ثبات خطی می‌توان دریافت که اگر در پرشی گروه فعال را درست تشخیص دهیم، در پرش بعدی تنها دو حالت برای گروه فعال بعدی امکان-پذیر است. چون ثبات خطی در هر کلاک حداکثر یک بیت بر سمبل آنتروپی ایجاد می‌کند. برای مثال اگر در پرشی گروه دهم (۱۰۱۰) انتخاب شده باشد در مرحله بعد گروه پنجم (۰۱۰۱) یا گروه سیزدهم (۱۱۰۱) انتخاب می‌شود. توجه کنید که در کلاک بعدی تنها یک بیت جدید وارد حالت ثبات خطی دوم خواهد شد و لذا آنتروپی متقابل دو گروه متوالی حداکثر برابر یک بیت بر سمبل است.

از نکته بیان شده در رابطه با همبستگی بین انتخاب گروه‌های متوالی می‌توان برای تصمیم‌گیری در مورد صحت حدس گروه فعال بهره برد. مرتبه پیچیدگی حدس دنباله گروه‌های فعال (به طول n) با توجه به همبستگی انتخاب‌های متوالی برابر با K*2n-1

است. همانطور که گفته شد مهاجم دنباله فرکانس‌های انتخابی را شنود می‌کند، لذا با دیدن هر فرکانس (یا معادلا اندیسی از ماتریس گروه‌بندی) می‌تواند تشخیص دهد که فرکانس بعدی بایستی در کدام دو گروه قرار گیرد. اگر چنانچه فرکانس بعدی در هیچکدام از گروه‌ها نباشد، کاندیدای ماتریس گروه‌بندی (MGROUP) صحیح نیست و کاندیدای بعدی باید بررسی شود. بدین ترتیب کاندیدای محتمل (ماتریس گروه‌بندی محتمل) کاندیدایی است که فرکانس‌های متوالی شنود شده را با توجه به همبستگی آنها به درستی گروه‌بندی کرده باشد و مهاجم با این روش به ماتریس گروه‌بندی دست می‌یابد و سپس از روی ماتریس براحتی حالت اولیه ثبات خطی اول را هم کشف خواهد کرد.

۲-۵ حمله خطی مستقیم به ثبات دوم

با توجه به نکته همبستگی بین انتخاب‌های متوالی گروه‌های فعال توسط ثبات خطی دوم می‌توان مستقیما به ثبات دوم حمله خطی نمود. طول ثبات خطی دوم همانطور که گفته شد برابر با $Log_2L=l$ است. لذا با داشتن 2*l بیت از خروجی ثبات دوم شکسته می‌شود (یعنی حالت اولیه و چندجمله‌ای فیدبک آن بدست می‌آید) [۴]. با توجه به اینکه حالت ثبات دوم بیانگر گروه فعال است، با حدس زدن 2*l گروه فعال متوالی هم می‌توان ثبات دوم را شکاند. مرتبه پیچیدگی حدس 2*l گروه فعال متوالی با فاصله یک کلاک (بیشترین همبستگی) و K کلاک (کمترین همبستگی) در رابطه ۶ و ۷ محاسبه شده است.

$$O(2 * l\ Groups\ per\ 1\ Clock\ ) = K * 2^{2*l-log_2K} = L^2 \quad (۶)$$

$$O(2 * l\ Groups\ per\ K\ Clocks) = K * K^{2*l-1} = L^{2*log_2K} \quad (۷)$$

همانطور که در رابطه ۶ و ۷ آمده است، مرتبه پیچیدگی حدس نسبت به L چندجمله‌ای است. در طراحی سیستم فرض شده است که چندجمله‌ای فیدبک ثبات دوم در اختیار است، لذا میزان پیچیدگی ابهام به مقدار K*2l-logK=L یا در بدترین حالت LlogK خواهد بود. در نتیجه اگر مقدار L (دوره تناوب ثبات دوم) محدود باشد (L<240) و یا اگر تعداد جملات چندجمله‌ای فیدبک ثبات دوم کم باشد، تعداد حدس‌های موثر به شدت کاهش می‌یابد و با استفاده از چندجمله‌ای فیدبک می‌توان معادلات توازن‌آزمای زیادی تولید کرد و کاندیداهای محتمل را شناسایی نمود و در نهایت گروه‌بندی فرکانس‌ها را حدس زد.

۳-۵ راه کار بهبود امنیت سیستم

برای بهبود امنیت سیستم پیشنهادی در بخش ۴ پیشنهاد می‌شود که به جای ثبات خطی اول از یک Transformation Shift Register(TSR) با فیدبک غیرخطی استفاده شود. زیرا این سیستم غیرخطی تعداد حالات ماتریس گروه‌بندی معرفی شده در رابطه ۵ را به شدت افزایش می‌دهد، لذا مرتبه پیچیدگی حدس ماتریس به مقدار بیشینه !M نزدیک می‌شود. همچنین در این حالت دیگر لزومی ندارد که امنیت سیستم مبتنی بر مخفی‌ماندن فیدبک TSR باشد و تنها کلید سیستم حالت اولیه TSR است. در اینجا به دلیل آنکه دوره تناوب سیستم غیرخطی بسیار بزرگ است، امکان حدس حالت اولیه عملا غیرممکن است.

به جای ثبات خطی دوم هم می‌توان از یک TSR با خانه‌های حافظه حداقل K-بیتی استفاده کرد تا در هر کلاک (همزمان با هر پرش) یک کلمه حداقل K-بیتی برای انتخاب گروه فعال در اختیار داشته باشیم. در اینجا برای سهولت عمل رهگیری می‌توان چندجمله‌ای فیدبکی برای TSR درنظر گرفت تا TSRی خطی تنها توسط گیرنده قابل شکستن باشد و گیرنده در نهایت بتواند خود را با فرستنده همزمان کند. در نتیجه عمل رهگیری و آشکارسازی غیرهمزمان در گیرنده قابل پیاده‌سازی خواهد بود.

ایده گروه‌بندی عملیات رهگیری در گیرنده را آسان‌تر می‌کند ولی باعث تضعیف امنیت سیستم می‌شود. مصالحه بین امنیت و کارایی سیستم در بسیاری از موارد وجود دارد. در اینجا نیز اگر مولد کد شبه‌تصادفی شکل ۲، TSR با فیدبک غیرخطی باشد که خانه‌های حافظه حداقل log2M دارد، امنیت سیستم به مقدار زیادی بهبود می‌یابد. زیرا اگر کلید سیستم حالت اولیه TSR به طول L باشد، کلید سیستم حداقل log2(L*log2M) بیت بر سمبل آنتروپی خواهد داشت و لذا مقدار آنتروپی هر خانه حافظه TSR (برحسب کلمه) برابر log2log2M خواهد بود. ولی مرتبه پیچیدگی حدس هر خانه حافظه TSR برابر 2logM=M است که بیشترین مقدار ممکن است. در نتیجه دشمن در هر پرش با بیشترین ابهام برای حدس فرکانس حامل بعدی روبروست. مشکل اصلی این روش این است که دیگر نمی‌توان آشکارسازی را به صورت غیرهمزمان انجام داد، و بایستی گیرنده و فرستنده از ابتدا با روشی دیگر همزمان شوند.

در عمل برای ارتقاء بیشتر امنیت سیستم و برای جلوگیری از شنود فرکانس‌های حامل پرانرژی توسط دشمن پیشنهاد می‌شود که روش پرش فرکانس تفاضلی متغیر به صورت تلفیق با روش‌های دنباله مستقیم در سیستم طیف گسترده به‌کاررود. با تلفیق دو روش طیف گسترده فرکانسی سیگنال ارسالی یکنواخت‌تر خواهد شد و در فرکانس‌های حامل پرش انرژی بالا نخواهیم داشت درنتیجه دشمن در آشکارسازی فرکانس حامل پرش دچار مشکل خواهد شد. طبیعتا مشکلی که در این حالت پیش می‌آید افزایش پیچیدگی سیستم است و همچنین عمل رهگیری در گیرنده مشکل‌تر خواهد شد، اما امنیت سیستم به واسطه بهبود خاصیت LPD افزایش خواهد یافت.

۶- نتیجه‌گیری

در این مقاله روش پرش فرکانس تفاضلی به عنوان روشی کارا در عملیات رهگیری و آشکارسازی ناهمزمان مورد بررسی قرار گرفت، ولی ضعف‌های شدید امنیتی آن باعث شد که در محیط‌های جنگ الکترونیک چندان به آن توجهی نشود. در نتیجه روش پرش فرکانس تفاضلی متغیر که به دلیل استفاده از گراف انتقال فرکانس متغیر از نظر امنیتی در سیستم‌های مخابرات طیف گسترده قوی‌تر است، توسط زیبایی‌نژاد مطرح شد. در اینجا سیستم مبتنی روش فرکانس تفاضلی متغیر توضیح داده شد و مزایای این سیستم نسبت به سیستم‌های مطرح شده در این زمینه بررسی شد.

علی‌رغم مزایای روش پرش فرکانس تفاضلی متغیر، سیستم مبتنی بر آن دارای ضعف‌های جدی امنیتی بود، که این ضعف‌ها در قالب دو حمله خطی توصیف شد و نشان داده شد که با استفاده از ثبات‌های خطی امنیت سیستم دچار مشکل خواهد شد. لذا برای رفع این مشکلات راه‌کارهایی جهت غیرخطی کردن سیستم و بالابردن مرتبه پیچیدگی حمله موثر به سیستم پیشنهاد شد. اما همانطور که بیان شد با به‌کاربستن برخی ایده‌های افزایش امنیت، مزایای سیستم همچون رهگیری آسان و آشکارسازی ناهمزمان از دست می‌رود و این مصالحه بین امنیت و کارایی سیستم در اینجا نیز مشاهده می‌شود.

مراجع

[۱] زیبایی‌نژاد، علی، تحلیل روش پرش فرکانسی تفاضلی و طراحی یک سیستم امن مبتنی بر آن، پایان‌نامه کارشناسی ارشد، دانشگاه صنعتی شریف، پاییز ۱۳۸۵.

[2] R. L. Peterson, R. E. Ziemer, D. E. Borth, "Introduction to Spread-Spectrum Communications", Prentice-Hall, Englewood Cliffs, N.J., 1995.

[3] D. J. Torrieri, "Principles of Spread-Spectrum Communication Systems", Springer, 2005.

[4] H. Beker and F. Piper, "CIPHER SYSTEMS: The Protection of Communications", Northwood Publications, 1982.

[5] D. L. Nicholson, "Spread Spectrum Signal Design: LPE and AJ", C.S. Press, 1988.

[6] D. L. Herrick, P. K. Lee, "CHESS: A New Reliable High Speed HF Radio", IEEE Proc. Of Military Communications Conference (MILCOM'96), Vol.3, Washington DC, Oct 1996.

[7] D. G. Mills, D. E. Egnor, G. S. Edelson, "CHESS Study: Final Report", Report for DARPA and ARFL, Feb 2001.

[8] Z. Chen, S. Li, B. Dong, "A Frequency Transition Function Construction Method of Differential Frequency Hopping System", IEEE Vehicular Tech. Conf. 60th, Vol.7, Sep 2004.

[9] A. Zibaee-Nejad, F. Ashtiani, M. R. Aref, "Differential Frequency Hopping with Variable Frequency Transition Function", IEEE Sarnoff Symposium, Nassau Inn in Princeton, N.J. USA, April-May 2007.