تاریخ دریافت:۱۴۰۲/۰۳/۱۸ پژوهشنامه علوم دفاعی، شماره ۱۰ ، تابستان ۱۴۰۲
تاریخ پذیرش: ۱۴۰۲/۰۶/۱۷ ص ص ۶۹ تا ۸۰

ایمن نمودن پیام‌های نظامی با استفاده از کدهای زیرفضا

سلیمان عسگری[۱]

چکیده

هدف اصلی این مقاله استفاده از روش‌های جبری بکار رفته در فرایند کدگذاری شبکه به جهت مقابله با حملات تخریبی و آلودگی دشمن به شبکه انتقال اطلاعات می‌باشد. کدگذاری خطی تصادفی شبکه برای افزایش توان عملیاتی یک شبکه انتقال اطلاعات با اجازه دادن به ترکیب خطی تصادفی بسته‌ها در یک شبکه استفاده می‌شود. در این تحقیق جهت افزایش توان عملیاتی شبکه انتقال اطلاعات و نیز به‌منظور مقابله با تهدیدات شنود، تخریب و آلودگی شبکه، یک مدل ریاضی از کدگذاری تصادفی شبکه بنام کدهای زیرفضا را موردمطالعه قرار داده و با استفاده از روش‌های جبری به‌کاررفته در این فرایند، ساختارهای جدیدی از کدهای زیر فضا با پارامترهای بهینه‌شده را به دست آوردیم که علاوه بر بهبود نتایج پیشین، موجب افزایش توان عملیاتی شبکه، کاهش زمان انتقال اطلاعات، افزایش ضریب ایمنی شبکه و کاهش انرژی و هزینه‌های پهنای باند مصرفی شبکه می‌شوند. به‌طور خاص با استفاده از زیرگروه‌های خاص ماتریسی، رده‌های جدیدی از کدها را به دست می‌آوریم.

واژه‌های کلیدی : کدگذاری جبری، گروه‌های ماتریسی، امنیت تبادل اطلاعات.

[۱] . استادیار ریاضی گروه ریاضی دانشکده علوم پایه دانشگاه امام علی (ع)، تهران، ایران. ایمیل: s.asgary95@gmail.com

مقدمه

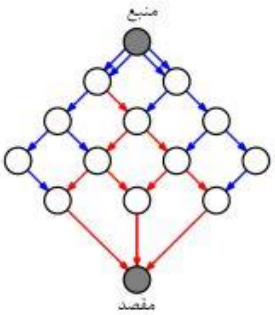
در اوایل دهه ۱۹۹۰، یعنی در سال‌های آغازین پس از جنگ سرد، پژوهشگرانی که برای موسسه رند کار می‌کردند، گزارشی درمورد آنچه مدل نبرد مبتنی بر فناوری برتر خوانده‌اند، ارائه دادند. هرچند بعضی نویسندگان ادعا کردند که این بحث‌های نظری نارسا هستند، اما نظریه‌ی جنگ اطلاعاتی که اقامه کردند مدت‌ها پیش از این، یعنی قبل از سال ۱۹۹۵ در درون تشکیلات ارتش ایالات‌متحده اعتبار یافته بود. رئیس سابق ستاد نیروی هوایی آمریکا اظهار داشت سیطره بر پهنه اطلاعات در حال حاضر به‌اندازه تصرف سرزمین یا کنترل فضای هوایی – که درگذشته اهمیت زیادی داشت – در منازعات اهمیت یافته است. این تغییر پارادایم، سطوح جدیدی را برای تفکرات و بودجه‌های نظامی ایالات‌متحده درزمینه فضای نبرد اطلاعاتی بوجود آورده است. جنگ اطلاعاتی، دیگر ماجراجویی غیرحرفه‌ای‌ای در عرصه سرقت‌های کامپیوتری محسوب نمی‌شود، بلکه یکی از اصلی‌ترین فعالیت‌های نظامی بسیار مشروع مقتدرترین ارتش‌های جهان است که در کنار تجهیزات لجستیکی و تسلیحات هدایت‌شونده جدید به کار می‌آید. درواقع، جنگ اطلاعاتی، آن دسته از فعالیت‌هایی است که با هدف ایجاد اختلال، تخریب، و جلوگیری از دستیابی دشمن به اطلاعات در عملیات پدافندی و آفندی انجام می‌گیرد . ارتش جمهوری اسلامی ایران نیز بسیاری از خدمات خود را از طریق فناوری اطلاعات انجام می‌دهد که از این جنبه، ضرورت تبادل داده‌ها در یک بستر امن امری انکارناپذیر است. از مهم‌ترین رویکردهای جلوگیری از دستیابی دشمن به اطلاعات در عملیات‌های پدافندی و آفندی، استفاده از کدگذاری می‌باشد. اگرچه برخی دستگاه‌های کدگذاری با استفاده از روش‌های ریاضی به‌صورت از پیش تعریف شده موجودند، اما با توجه به ماهیت سازمانی ارتش لزوماً قابل استفاده برای ارتش جمهوری اسلامی ایران نمی‌باشند. لذا نیاز است تا برخی از این دستگاه‌های کدگذاری بهینه‌سازی و بومی‌سازی گردند که این امر از اهداف اصلی این پژوهش می‌باشد.

آنچه در عصر حاضر شاهد آن هستیم، درهم‌آمیختگی عمیق جهان‌های نظامی و غیرنظامی می‌باشد. تشریح این امکان در بخش اعظم ادبیاتی که در مورد جنگ اطلاعاتی وجود دارد منعکس‌شده است. جنگ اطلاعاتی به ساختارهای نظامی سنتی محدود نمی‌شود. برای مثال، جنگ اطلاعاتی ممکن است موارد زیر را در برگیرد: دریچه نرم‌افزاری کنترل شبکه‌های همگانی، حمله به شماره‌گیری‌های انبوه، کنترل الکترونیکی بر رادیو یا تلویزیون، نظارت با دوربین‌ها، بمب منطقی، تغییر فرمول‌های پزشکی - درمانی یا اطلاعات، حمله‌ی هماهنگ به پست‌های الکترونیکی، تغییر مسیر بودجه یا داده‌های بانک‌های فاسد، دستبرد زدن به اطلاعات شخصی و مسدودسازی آن‌ها، ویروس‌ها یا کرم‌های رایانه‌ای، مسدودسازی اطلاعات، و ایجاد اختلال در زیرساخت فرماندهی و کنترل نظامی کشور. در یک شبکه اطلاعات، شبکه نسبت به انتشار خطا بسیار حساس خواهد بود. درواقع ورود حتی یک بسته‌ی خراب می‌تواند منجر به خراب شدن همه‌ی اطلاعات شود. این نکته خود گویای اهمیت و ضرورت استفاده از دستگاه‌های کدگذاری شبکه هست. این وضعیت، با توجه به موقعیت ویژه ایرانِ مستقل در جهان دوقطبی امروز و نیز جنگ نرم همه جانبه‌ای که از سوی قدرت‌های بزرگ علیه سازمان‌های علمی و نظامی کشورمان در جریان است، ضرورت و اهمیت استفاده از دستگاه‌های کدگذاری را برای ارتش جمهوری اسلامی ایران دوچندان می‌کند. همچنین، از دیدگاه نظامی و امنیتی، عدم به‌کارگیری دستگاه‌های کدگذاری علاوه بر اینکه موجب دریافت اطلاعات با اختلال بسیار بالا در مقصد خواهد شد، بلکه

ضریب امنیت اطلاعات را نیز بسیار کاهش داده و خطر مسدودسازی یا ایجاد اختلال در آن اطلاعات توسط دشمن را نیز افزایش می‌دهد. در این پروژه روش‌های مؤثر جبری در ایجاد دستگاه‌های کدگذاری اطلاعات را مورد مطالعه قرار داده و از طریق بهبود بخشیدن به برخی ساختارهای به‌کاررفته در این فرآیند، امکان ایجاد دستگاه‌های جدید کدگذاری اطلاعات را فراهم می‌نماییم. همچنین فرض بر این است که خواننده با تعاریف و اصطلاحات مقدماتی جبر آشنایی دارد.

پیشینه تحقیق و مبانی نظری

زندگی بشر همواره متأثر از فناوری بوده است. اما باگذشت زمان و پیشرفت فناوری، این تأثیرپذیری تشدید شده است. فناوری‌های پیچیده دوران مدرن که تمامی حوزه‌های حیات انسانی را درنوردیده، به حوزه جنگ و منازعات نیز رسوخ کرده و بر پویش امنیتی جوامع تأثیر نهاده است. همچنین، تحولات نوظهور از قبیل پایان جنگ سرد، ظهور تروریسم فراملی، و جهانی‌شدن در دو دهه اخیر ماهیت منازعات و امنیت را دگرگون ساخته است. به‌گونه‌ای که شیوه نقش‌آفرینی فناوری در حوزه جنگ و منازعات بیشتر به حوزه‌های پدافند غیرعامل معطوف شده است . پیرو این دگرگونی، مفاهیمی نظیر جنگ اطلاعات و جنگ سایبر مطرح گردیده‌اند. اکنون با قاطعیت می‌توان گفت ماشین به‌عنوان زیربنای تولید تسلیحات برای تأمین امنیت، جای خود را به فناوری‌های اطلاعات و ارتباطات داده است. درنتیجه، این فناوری‌ها در محور استراتژی پردازی‌های نظامی قرارگرفته‌اند. این وضعیت، آسیب‌پذیری جوامع را به‌شدت افزایش داده و تهدیدهای امنیتی را بیش از پیش پیچیده‌تر ساخته است. درواقع، به دنبال ارتقای جایگاه و اهمیت دستگاه‌های اطلاعاتی و شبکه‌های مخابراتی در سیاست‌های دفاعی بسیاری از کشورها، موضوع وابستگی به فناوری ارتباطات و اطلاعات بیش از پیش موردتوجه قرارگرفته است. در چنین شرایطی، حفظ امنیت پیام‌ها و اطلاعات نظامی کشور از اهمیتی غیرقابل انکار برخوردار است و استفاده از روش‌های کدگذاری پیام‌ها و اطلاعات یکی از راه‌های مؤثر و کارا در این راستا می‌باشد. افزایش توان عملیاتی یکی از چالش‌های مهم تحقیقاتی در دستگاه‌های ارتباطی بی‌سیم است. پیش‌بینی می‌شود که نیازهای توان عملیاتی شبکه برای شبکه‌های بی‌سیم در آینده بسیار بیشتر از امروز باشد. باند فرکانس یک منبع محدود است، بنابراین راه‌حل‌های جدیدتر و پیچیده‌تری برای به حداکثر رساندن داده‌های تحویل‌شده در این طیف محدود مورد نیاز است. کدگذاری شبکه خطی تصادفی برای افزایش توان عملیاتی اطلاعات با اجازه دادن به ترکیب خطی تصادفی بسته‌ها در یک شبکه استفاده می‌شود. یعنی هر گره داخلی شبکه ترکیبات خطی تصادفی بسته‌های دریافتی را به گره‌های مجاور منتقل می‌کند. با توجه به روش کدگشایی، گیرنده‌ها قادر به بازسازی بسته‌های اصلی هستند که در منابع آن به شبکه تزریق‌شده است. اگرچه این روش بسیار مؤثر است، اما نسبت به انتشار خطا بسیار حساس است. در شکل زیر نمونه‌ای از پدیده انتشار خطا نشان داده‌شده است.



شکل (۱) : پدیده انتشار خطا

برای حل این مشکل (کوتر[۱]، ۲۰۰۸، ۵) یک مدل ریاضی از کدگذاری تصادفی شبکه بنام کدهای زیرفضا ارائه نمودند؛ که در آن پیام‌ها به‌صورت زیرفضاهایی از یک فضای برداری ثابت روی یک میدان متناهی در نظر گرفته می‌شوند. کدهای زیرفضا اخیر موردتوجه تحقیقات بسیاری قرارگرفته‌اند. یک رده مهم از کدهای زیرفضا، کدهای موسوم به کدهای مدار می‌باشند که به‌صورت مدار یک زیرفضا تحت عمل زیرگروهی از گروه ماتریسی خطی عام در نظر گرفته می‌شوند. کدهای مداری که در آن‌ها اشتراک هر دو کد کلمه برابر صفر باشد اسپرید جزئی نامیده می‌شوند. کدهای مدار در مبحث کدگذاری شبکه اولین بار در (تروتمن[۲]، ۲۰۱۰، ۶) معرفی گردیدند که در آن نویسندگان نشان دادند چگونه کدهای اسپرید ساخته‌شده را می‌توان به‌عنوان حالات خاصی از کدهای مدار به دست آورد. کدهای مدار معمولاً بوسیله گروهی که مدار را تولید می‌نماید شناسایی و دسته‌بندی می‌شوند. به‌عنوان مثال اگر گروه مولد مدار گروهی دوری باشد، کد مدار حاصل را دوری می‌نامند. هدف اصلی ما در این پژوهش بررسی این مسئله باز و ارائه ساختارهای جدیدی از کدهای مدار جابجایی و غیرجابجایی می‌باشد که دارای اندازه‌ای بزرگتر از ساختار ارائه‌شده در (کلیمنت[۳]، ۲۰۱۹، ۴) بوده و نیز دارای بیشترین فاصله کمینه کد کلمات هستند. برای این منظور از قضیه مشهور اشباخر-دنکین[۴] درخصوص رده‌بندی زیرگروه‌های ماکسیمال گروه خطی عام یعنی $GL(n,q)$ برای انتخاب فرم زیرگروه تولیدکننده مدار استفاده می نمائیم که ضمن پاسخ‌گویی به مسئله ارائه‌شده فوق، ساختار کدهای ارائه‌شده در این تحقیق و پارامترهای کدهای ساخته‌شده در (چن[۵]، ۲۰۲۰، ۳) و (کلیمنت[۶]، ۲۰۱۹، ۴) را به‌طور محسوسی بهبود می‌بخشیم.

روش‌شناسی پژوهش

---

۱. Kotter
۲. Trautmann
۳. Climent
٤. Aschbacher-Donkin
٥. Chen
٦. Climent

یک شبکه را به‌وسیله‌ی یک گراف جهت‌دار بدون دور نشان می‌دهیم، که در آن یال‌ها مسیر انتقال اطلاعات هستند. سه نوع متفاوت از رئوس در یک شبکه موجودند، رئوس بدون یال ورودی که گره‌های منبع نامیده می‌شوند، رئوس بدون یال خروجی که گره‌های مقصد نامیده می‌شوند و رئوس با یال‌های ورودی و خروجی که گره‌های داخلی نامیده می‌شوند. فرض بر این است که حداقل یک منبع و یک مقصد در هر شبکه موجود است. کدگذاری شبکه از یک ایده‌ی ساده نشأت می‌گیرد که به گره‌های داخلی اجازه داده شد تا به‌جای هدایت بسته‌های دریافتی روی پیوندهای خروجی، نوعی از کدگذاری و تغییر را روی بسته‌های اطلاعات انجام داده و حاصل این کدگذاری را روی پیوندهای خروجی هدایت کنند. منظور از کدگذاری خطی شبکه حالتی است که گره‌های داخلی ترکیبات خطی از بردارهای اطلاعات ورودی را روی پیوندهای خروجی هدایت می‌کنند. اغلب استفاده از کدگذاری خطی شبکه در مقایسه با هدایت بدون کدگذاری بسته‌های ورودی اطلاعات توسط گره‌های میانی، توان عملیاتی شبکه را بهبود می‌بخشد. در مبحث کدگذاری خطی شبکه وقتی توپولوژی شبکه شناخته‌شده نباشد و یا در زمان‌های مختلف توپولوژی شبکه تغییر کند، از کدگذاری خطی تصادفی یا غیرمنسجم صحبت می‌کنیم.

علیرغم مزیت‌های کدگذاری خطی شبکه، تحت کدگذاری، شبکه نسبت به انتشار خطا بسیار حساس خواهد بود. درواقع حتی ورود یک بسته خراب می‌تواند منجر به خراب شدن همه اطلاعات شود. نویسندگان (کوتر[۱]، ۲۰۰۸، ۵) و (چیسچانگ[۲]، ۲۰۰۸، ۵) با ارائه یک مدل ریاضی نشان دادند که در عمل بهتر است از فضای برداری بجای یک بردار برای کدگذاری در شبکه استفاده شود. در این مدل منبع یک پایه از کد کلمه مورد نظر را به شبکه تزریق می‌کند و هر یک از گره‌های میانی یک ترکیب خطی از بردارهای ورودی خود را روی پیوند خروجی هدایت می‌کنند. بنابراین هر مقصد ترکیب‌های خطی از بردارهای اصلی را دریافت می‌کند که اگر خطایی در حین انتقال رخ نداده باشد فضای برداری یکسانی را مانند بردارهای پایه فرستاده شده تولید می‌کند. با ارائه این مدل ریاضی فصل جدیدی در مطالعه کدها موسوم به کدهای زیرفضا آغاز شد که در ادامه به آن می‌پردازیم. کدهای زیرفضا درواقع زیرمجموعه‌هایی از زیرفضاهای مشمول در یک فضای برداری می‌باشند که در آن این زیرفضاها نقش کدکلمات را بازی می‌کنند.

یافته‌ها

تعریف ۱. فرض کنید q توانی از عدد اول p باشد. میدان متناهی با q عضو را با $\mathbb{F}_q$ نشان می‌دهیم. در این صورت p مشخصه میدان است و

$$\mathbb{F}^*_q = \mathbb{F}_q - \{0\}$$

گروه ضربی میدان است که شامل تمام عناصر وارون‌پذیر میدان می‌باشد.

۱. Kotter

۲. Kschischang

تعریف ۲. فضای برداری $\mathbb{F}_q^n$ را در نظر بگیرید. یک هندسه تصویری از $\mathbb{F}_q^n$ مجموعه همه زیرفضاهای فضای برداری $\mathbb{F}_q^n$ است که با $PG(n-1,q)$ نشان داده می‌شود. مجموعه همه زیرفضاهای با بعد k از $\mathbb{F}_q^n$ را گراسمانیان می‌گوییم و با نماد $\varsigma_q(k,n)$ نشان می‌دهیم. همچنین تعداد اعضای یک گراسمانیان از رابطه

$$|\varsigma_q(k,n)| = \frac{\prod_{i=n-k+1}^{i=n}(q^i-1)}{\prod_{i=1}^{i=k}(q^i-1)}$$

محاسبه می‌گردد.

تعریف ۳. یک کد زیرفضایی C زیر مجموعه‌ای از $PG(n-1,q)$ است. اگر همه کد کلمات C دارای بعد یکسان k باشند، آنگاه C را یک کد با بعد ثابت می‌نامیم و داریم

$$C \subseteq \varsigma_q(k,n)$$

تصحیح خطا و کد گشایی

در هنگام انتقال اطلاعات و با استفاده از کدهای زیرفضایی امکان دارد دو نوع خطا رخ دهد: کاهش بعد فضای ارسالی که پاک‌شدگی نامیده می‌شود و یا افزایش بعد فضای ارسالی که الحاق نامیده می‌شود. فرض کنید $U \in PG(n-1,q)$ فرستاده شده است و طی فرایند انتقال، پاک شدگی و الحاق‌هایی صورت گرفته است. به این ترتیب کلمه دریافتی به‌صورت

$$R = \overline{U} \oplus \varepsilon$$

است که در آن $\overline{U}$ زیرفضایی از U و ε فضای خطا است. برای داشتن مفهومی جهت قابلیت کدگشایی برای کدهای زیرفضا لازم است روی مجموعه $PG(n-1,q)$ یک متر و فاصله مناسب تعریف کنیم.

تعریف ۴. فاصله زیر فضایی d که روی هندسه تصویری $PG(n-1,q)$ به‌صورت

$$d(U,V) = \dim(U) + \dim(V) - 2\dim(U \cap V)$$

تعریف می‌شود، یک متر نامیده می‌شود.

تعریف ۵. کمترین فاصله زیرفضا از یک کد زیرفضایی $C \subseteq PG(n-1,q)$ به‌صورت

$$d(C) = \min\{d(U,V) : U,V \in C, U \neq V\}$$

تعریف می‌شود.

در ادامه مقاله، منظور ما از فاصله، فاصله زیرفضایی می‌باشد. بنابراین یک کد زیرفضا

$$C \subseteq \varsigma_q(k,n)$$

با کمترین فاصله زیرفضای d و تعداد کد کلمات N را یک $[n,N,d;k]$ - کد می‌گوییم. یادآوری می‌کنیم که فضای دوگان $U^{\perp}$ از یک زیر فضای $U \subseteq \varsigma_q(k,n)$ به‌صورت زیر تعریف می‌شود.

$$U^{\perp} = \{v \in \mathbb{F}_q^n : vu^T = 0, \forall u \in U\}$$

قضیه ۱. اگر C یک کد با پارامترهای $[n,N,d;k]$ باشد، آنگاه $C^{\perp}$ یک کد با پارامترهای $[n,N,d;n-k]$ است.

برهان . اثبات با استفاده از فرمول‌های

$$(U+V)^{\perp} = U^{\perp} \bigcap V^{\perp}$$

و

$$U^{\perp} + V^{\perp} = (U \bigcap V)^{\perp}$$

به‌راحتی نتیجه می‌شود.

این قضیه تضمین می‌کند که در مطالعه روی کدهای با بعد ثابت می‌توانیم خود را به مواردی که $k \le \frac{n}{2}$ می‌باشد؛ محدود نمائیم. کدهای دوگان از کدهای حاصل که دارای کمترین فاصله و مرتبه‌ای برابر با کد اولیه می‌باشند، بقیه کدها را تشکیل می‌دهند.

اکنون فرض کنیم $C \subseteq PG(n-1,q)$ یک کد زیرفضایی و $R \subseteq PG(n-1,q)$ یک کلمه دریافتی باشد. در این صورت، یک کدگشای کمترین فاصله، نزدیک‌ترین کدکلمه به کلمه دریافتی را نسبت به متر زیرفضا انتخاب می‌کند. اگر بیش از یک نزدیک‌ترین کدکلمه موجود باشد، آنگاه کدگشا پیام شکست را اعلام می‌کند.

قضیه ۲. فرض کنیم $C \subseteq PG(n-1,q)$ یک کد زیرفضایی با کمترین فاصله زیر فضای d و $R \subseteq PG(n-1,q)$ یک کلمه دریافتی باشد. اگر $U \in C$ موجود باشد که

$$d(R,U) \le \frac{d-1}{2}$$

آنگاه U نزدیک‌ترین کد کلمه یکتا به R است و تحت کد گشای کمترین فاصله، همواره U به R بازگردانده می‌شود.

برهان. با توجه به $d(R,U)$، درصورتی‌که R به کد کلمه دیگری چون V بازگردانده شود، آنگاه از خواص متریک نتیجه می‌شود که $d(U,V) < d$ که متناقض با فرض می‌باشد.

نتیجه ۱. با توجه به قضایای بالا در خصوص کدهای زیرفضایی به ازای هر $k \le \frac{n}{2}$ روش ساخت رده‌ای از کدها که دارای حداقل فاصله کد کلمات بود ارائه شد.

امنیت انتقال پیام در شبکه

با توجه به اینکه شبکه نسبت به انتشار خطا بسیار حساس می‌باشد؛ لزوم استفاده از کدگذاری شبکه بسیار احساس می‌شود. با این حال در شبکه‌های حساس اطلاعاتی ازجمله شبکه‌های انتقال پیام و داده‌های نظامی دارای طبقه‌بندی، یک حمله و تهدید مهم، حمله شنود داده‌های در حال انتقال توسط دشمن می‌باشد؛ که در زیر به آن اشاره می‌شود.

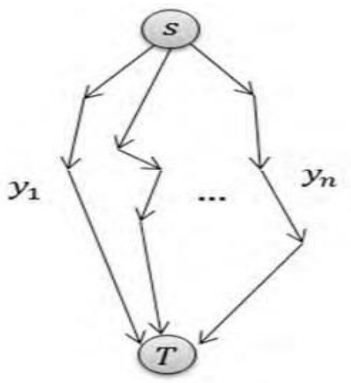
حمله شنود

حمله شنود درواقع به این معنی است که دشمن به‌عنوان یک ناظر بیرونی یا به‌عنوان یکی از گره‌های میانی شبکه، جریان انتقال اطلاعات را رصد کرده و با دسترسی به برخی از یال‌های شبکه، سعی می‌کند بیشترین اطلاعات ممکن را از طریق بسته‌های اطلاعاتی روی یال‌هایی که به آن‌ها اشراف دارد؛ به دست آورد. از دیدگاه امنیتی تاکنون طرح‌های مختلفی برای محافظت از اطلاعات منبع در برابر شنودگری که به تعداد محدودی از یال‌های شبکه دسترسی دارد؛ ارائه شده است که یکی از مهم‌ترین آن‌ها طرح امنیت شانون است که در زیر موردبررسی قرار می‌گیرد.

طرح امنیت شانون

کانال‌های شنود کانال‌هایی هستند که در آن‌ها گیرنده‌های غیر مجاز نیز قادرند اطلاعات فرستنده را دریافت و بهره‌برداری کنند. به‌طورکلی میزان نرخ اطلاعات قابل ارسال توسط فرستنده‌ها که توسط هیچ گیرنده‌ای غیر از گیرنده مجاز قابل پردازش نباشند؛ تحت عنوان ظرفیت امن شناخته می‌شوند. به‌طور خاص فرض کنید ظرفیت بیشینه کانال برابر n باشد و دشمن شنودگر بتواند حداکثر k یال از شبکه را شنود نماید. در این صورت فرستنده باید $n-k$ واحد اطلاعات را به همراه k سمبل تصادفی ارسال نماید تا هیچ اطلاعاتی برای دشمن شنودگر قابل بازیابی نباشد.

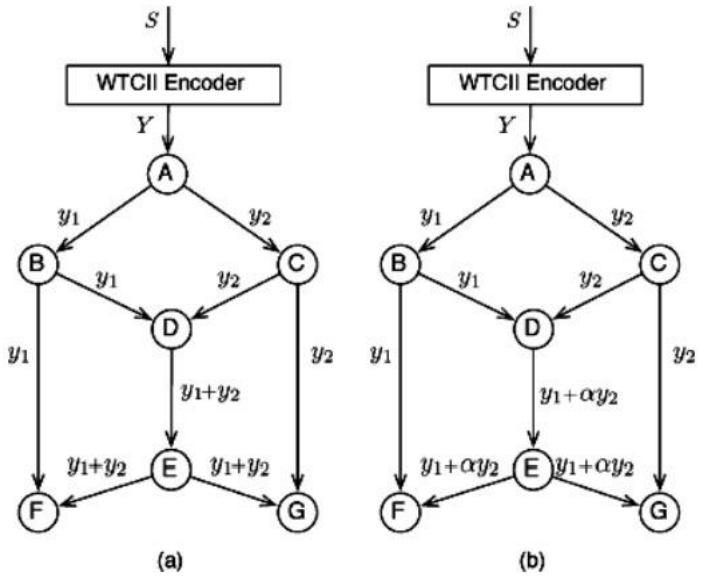
مثال . در شکل زیر فرض کنید $n=2$ و فرستنده می‌خواهد پیام‌های y_1 و y_2 را در حضور دشمن شنودگری که به یک یال اشراف اطلاعاتی دارد؛ ارسال نماید. با استفاده از طرح امنیت شانون، منبع می‌تواند $n-k=1$ واحد اطلاعات را به صورت امن ارسال کند.



شکل (۲): طرح امنیت شانون

یک روش کدگذاری که ما را به این هدف می‌رساند؛ به این صورت است که هرگاه منبع قصد ارسال بیت ۰ را داشته باشد، آنگاه بیت $(0,0)$ یا $(1,1)$ را ارسال نماید و هر گاه بخواهد بیت ۱ را ارسال نماید؛ آنگاه به جای آن بیت $(1,0)$ یا $(0,1)$ را با احتمال مساوی ارسال نماید. می‌توان مشاهده کرد که شنودگر با شنود y_1 یا y_2 قادر نخواهد بود هیچ اطلاعاتی از بیت‌های منبع به دست آورد. حال با تغییر توپولوژی شبکه مثال دیگری را در نظر می‌گیریم.

مثال . شبکه پروانه‌ای شکل زیر را در نظر بگیرید. برای $n=2$ و $k=1$ همانند مثال کانال شنود قبل، فرض می‌کنیم هرگاه فرستنده در میدان $\mathbb{F}_2$ قصد ارسال بیت ۰ را داشته باشد بجای آن بیت $(0,0)$ یا $(1,1)$ را ارسال نماید و هرگاه بخواهد بیت ۱ را ارسال نماید؛ آنگاه به‌جای آن بیت $(1,0)$ یا $(0,1)$ را ارسال نماید. این کدگذاری تصادفی هر دو خاصیت کدهای قابل‌قبول را دارد. اما مشاهده می‌کنیم که هرگاه شنودگر هرکدام از یال‌های DE یا EF و یا EG را شنود کند، می‌توان به سمبول ارسالی منبع پی برد.



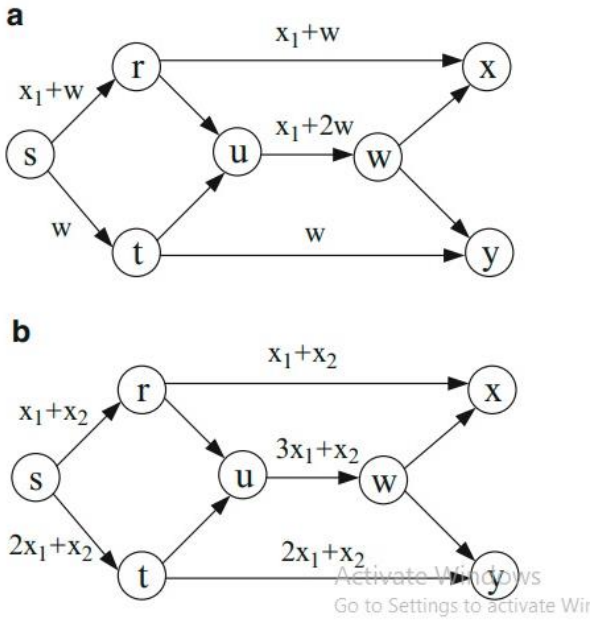
شکل (۳) : شبکه پروانه‌ای

ولی اگر کدگذاری شبکه روی میدان $\mathbb{F}_3$ ارسال شود به‌طوری‌که α یک عضو اولیه میدان $\mathbb{F}_3$ است، آنگاه دشمن شنودگر قادر به بازیابی اطلاعات منتقل‌شده نخواهد بود. تعمیم این مفهوم قضیه زیر را بر اساس طرح شانون برای ایجاد یک کدگذاری امن شبکه در مقابل حمله شنود به دست می‌دهد.

قضیه. برای یک شبکه پخش که در آن برش کمینه (یا ظرفیت بیشینه) بین فرستنده و هر گیرنده حداقل برابر n است، یک کدگذاری شبکه وجود دارد که به ازای آن شنودگری که به حداکثر k یال شبکه دسترسی دارد، هیچ اطلاعاتی از سمبل‌های ارسالی فرستنده به دست نمی‌آورد و فرستنده قادر است اطلاعات را با نرخ $n-k$ به تمام گیرنده‌ها برساند. چنین کدی را کد (n,k) − امن گوییم.

طرح امنیت ضعیف

یک سیستم یا شبکه اطلاعاتی امن گفته می‌شود، هرگاه دشمن شنودگر نتواند هیچ اطلاعات معناداری را طریق شنود برخی از یال‌های شبکه بازیابی نماید. برای تشریح این مفهوم و تمایز آن با طرح امنیت شانون شکل زیر را در نظر بگیرید.

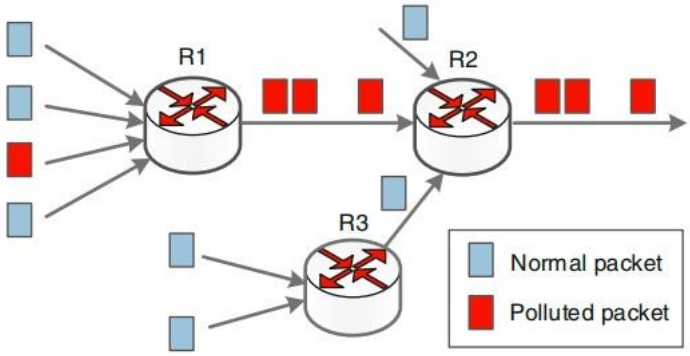


شکل (۴) : طرح امنیت ضعیف

در شکل a حرف x_1 یک پیام اطلاعاتی است که می‌بایست منتقل شود و W یک کلید تصادفی تولید شده توسط منبع است. برای بازیابی پیام x_1، دشمن شنودگر می‌بایست لااقل دو یال گراف شبکه را شنود کند. بنابراین با فرض اینکه دشمن تنها امکان شنود یک یال از شبکه را دارد، این شبکه یک شبکه اطلاعاتی امن با طرح امنیت شانون می‌باشد. در شکل b، x_1 و x_2 دو پیام منبع می‌باشند که می‌بایست منتقل شوند. در این حالت یک شنودگر هم می‌تواند یکی از یال‌های شبکه را شنود نماید، هرچند می‌تواند به شبه‌اطلاعاتی از شبکه دسترسی داشته باشد (که همان ترکیب خطی x_1 و x_2 است)، بنابراین شبکه با طرح امنیت شانون امن نیست. اما در هر صورت با شنود یک یال، شنودگر قادر به کدگشایی و دستیابی به پیام‌های منبع x_1 و x_2 (اطلاعات معنادار) نخواهد بود. در این حالت می‌گوییم شبکه دارای طرح امنیت ضعیف است.

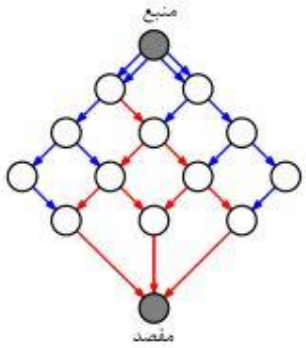
حمله‌های آلودگی

در این حالت دشمن به‌عنوان یکی از گره‌های میانی شبکه محسوب می‌شود، با این تفاوت که در این حالت این گره اخلالگر با واردکردن اطلاعات مخرب سعی در تخریب اطلاعات ارسالی منبع به گیرنده را دارد. شکل زیر نشان می‌دهد که چگونه ورود یک بسته آلوده و مخرب می‌تواند در شبکه تأثیر بگذارد.



شکل (۵) : حمله آلودگی

چنانچه پیشتر اشاره شد، باوجود استفاده از کدگذاری شبکه، شبکه نسبت به انتشار خطا بسیار حساس می‌باشد و حتی ورود یک بسته آلوده می‌تواند با نرخ تأثیر بالایی تمام شبکه را آلوده کند. همان‌طور که شکل زیر نرخ رشد بالای تکثیر آلودگی در یک شبکه با ورود یک بسته مخرب نشان می‌دهد.



شکل (۶) : تکثیر آلودگی

نتیجه‌گیری

هدف اصلی این تحقیق بهینه‌سازی روش‌های جبری به‌کاررفته در فرایند کدگذاری شبکه به جهت مقابله با حمله شنود دشمن به شبکه اطلاعات می‌باشد. در این تحقیق جهت افزایش توان عملیاتی شبکه انتقال اطلاعات و نیز به‌منظور مقابله با تهدیدات شنود، یک مدل ریاضی از کدگذاری تصادفی شبکه به نام کدهای زیر فضایی را موردمطالعه قرار داده و با استفاده از روش‌های جبری به‌کاررفته در این فرایند، ساختارهای جدیدی از کدهای زیر فضا را به دست آوردیم.

مراجع

Askary, S. Biranvand, N. and Shirjian, F. (2023). "New constructions of orbit codes based on imprimitive wreath products and wreathed tensor products", The Rendiconti del Circolo Matematico di Palermo 2, Vol. 72, No. 4, PP. 1-14.

Bardestani, F. and Iranmanesh. (2015). " Cyclic orbit codes with the nor-malizer of a Singer subgroup" J. Sci. Islamic Republic Iran. Vol. 26, No.1, PP. 49–55.

Chen, S. and Liang, J. (2020). "New Constructions of Orbit Codes Based on the Operations of Orbit Codes". Acta Math. Appl. Sin. Engl. Ser. Vol. 36, PP. 803–815.

Climent, J. Requena, V. and Soler X. (2019). " A construction of Abelian non-cyclic orbit codes" Cryptogr. Commun. Vol. 11, PP. 839–852.

Kotter, R. and Kschischang, F. (2008). "Coding for errors and erasures in random network coding". IEEE Trans. Inf. Theory, Vol. 54, No.8, PP. 3579–3591.

Trautmann, A Manganiello, F. and Rosenthal. (2010). " Orbit codes a new concept in the area of network coding" . In: Proceedings of the 2010 IEEE information theory workshop (ITW 2010), Dublin, Ireland. IEEE.