امنیت ارسال چندمقصدی داده‌ها با کدگذاری شبکه در حضور دشمن غیرفعال

حسام محمدحسینی

بخش مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران

کاوه سلامتیان

Associate Professor, Université Pierre et Marie Curie, Paris, France

احمدرضا شرافت*

استاد بخش مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران

چکیده

در این مقاله روش جدیدی برای امنیت بخشیدن به ارسال چندمقصدی (مالتی‌کست) اطلاعات با کدگذاری شبکه در حضور دشمن غیرفعال ارائه می‌کنیم. در کدگذاری شبکه، گره‌های (میانی) شبکه به جای تکرار اطلاعات دریافتی، ترکیب مناسبی از آنها را روی پورت‌های خروجی خود ارسال می‌کنند. روش‌های موجود امنیت‌دهنده به کدگذاری شبکه تنها دشمنی را در نظر گرفته‌اند که امکان شنود تعدادی از کانال‌های شبکه را دارد. در این مقاله حالتی را که گره‌های میانی شبکه غیرخودی هستند، نیز در نظر گرفته‌ایم. نوع امنیت، نرخ ارسال چندمقصدی امن اطلاعات، تعداد کانال‌ها/ گره‌های در اختیار دشمن و تعداد کلیدها در سیستم پیشنهادی را مطالعه و احتمال شنود اطلاعات در گره‌های میانی شبکه را محاسبه نموده‌ایم. در مورد مصالحه بین نوع امنیت و نیاز به ارسال کلید نیز بحث نموده‌ایم. با توجه به نیاز به ارسال کلید از طریق کانال خصوصی امن به منظور داشتن امنیت نظریه اطلاعاتی، روش پیشنهادی به گونه‌ای اصلاح شده تا این نیاز برطرف شود.

واژه های کلیدی: ارسال چندمقصدی، امنیت[۱]، امنیت ضعیف[۲]، شنود[۳]، کدگذاری امن شبکه[۴]، کدگذاری شبکه[۵].

۱- معرفی کدگذاری شبکه

کدگذاری شبکه [۱] بر این اساس بنا شده است که گره‌های میانی می‌توانند به جای تکرار ساده اطلاعات دریافتی، ترکیبی از آن‌ها را بر روی پورت‌های خروجی ارسال کنند. پژوهش‌های اخیر در تئوری اطلاعات شبکه نشان می‌دهند که با انجام یک پردازش نسبتا ساده، یعنی انتخاب ترکیب خطی مناسب از اطلاعات دریافتی بر روی پورت‌های ورودی و ارسال حاصل ترکیب بر روی پورت (های) خروجی، می‌توان به حد بالایی برای ارسال چندمقصدی در شبکه، که از قضیه Max-flow Min-cut به دست می‌آید، دست یافت [۲].

این حد، برای بیشتر شبکه‌ها با ارسال ساده و مسیریابی، قابل دستیابی نیست.

در حقیقت، مسیریابی در شبکه، حالت خاصی از کدگذاری شبکه است [۳]. در کدگذاری تصادفی شبکه، گره‌های شبکه، با ضرایب تصادفی، بسته‌های اطلاعاتی را با یکدیگر ترکیب و ارسال می‌کنند. در این حالت نشان داده‌اند که احتمال اینکه بتوانیم در مقصدها با استفاده از بردارهای دریافتی اقدام به کدبرداری شبکه نماییم با بزرگتر کردن اندازه میدان[۶] مورد استفاده به سمت یک میل می‌کند [۴].

پیش از ارائه کدگذاری تصادفی شبکه، فرض بر استفاده از بردارهای ثابت کدکننده در گره‌های میانی شبکه بود که به آن کدگذاری غیرتصادفی شبکه[۷] می‌گویند. در کدگذاری

* Corresponding author's email: sharafat@isc.iranet.net

غیرتصادفی شبکه، با فرض آگاهی از توپولوژی شبکه و ظرفیت کانال‌ها، باید یک‌بار، پیش از شروع به ارسال، بردارهای کدکننده مناسب برای رسیدن به ظرفیت ارسال چندمقصدی را محاسبه کنیم و پس از آن در همه ارسال‌ها این بردارها ثابت هستند. در [۱] نشان داده شده است که برای هر توپولوژی شبکه، ظرفیت ارسال چندمقصدی شبکه، با انتخاب مناسب توابع کدگذار در گره‌های میانی شبکه، قابل حصول است. این ظرفیت ممکن است در مورد ساده‌ترین توپولوژی شبکه با مسیریابی قابل حصول نباشد. همچنین در [۵] نشان داده شده است که محاسبه بردارهای مناسب کد شبکه برای هر شبکه‌ای، با پیچیدگی محاسباتی از مرتبه چندجمله‌ای[^] انجام پذیر است؛ در حالی‌که می‌دانیم حل مساله مسیریابی در شبکه دارای پیچیدگی از مرتبه نمایی است. بیشتر مقالات در زمینه امنیت از دسته کدگذاری غیر تصادفی هستند؛ به عبارت دیگر از توپولوژی شبکه آگاهی کامل دارند.

در این مقاله روش جدیدی برای امنیت بخشیدن به ارسال چندمقصدی اطلاعات در شبکه‌های مبتنی بر کدگذاری غیرتصادفی شبکه ارائه می‌کنیم. بر خلاف روش‌های موجود که عموما با کاهش نرخ ارسال چندمقصدی اطلاعات و یا نیاز به استفاده از میدانی با تعداد عناصر بیشتر (در مقایسه با ارسال غیر امن) همراه‌اند، این روش، سیستمی با امنیت ضعیف برای ارسال چندمقصدی اطلاعات در یک شبکه را فراهم می‌آورد. به علاوه، بر خلاف روش‌های موجود که باید تعداد کانال‌های در حال شنود، از ظرفیت ارسال چندمقصدی شبکه کوچکتر باشد؛ در روش پیشنهادی، تعداد کانال‌های مورد شنود می‌تواند بیشتر از ظرفیت ارسال چندمقصدی باشد. همچنین برای تامین امنیت، نیازی به افزایش اندازه میدان نیست. به علاوه در مقالات موجود، فرض بر خودی بودن گره‌های میانی شبکه است؛ به عبارت دیگر فهم (همه یا بخشی از) اطلاعات ارسالی چندمقصدی توسط این گره‌ها بلامانع است. در روش پیشنهادی ما، گره‌های میانی شبکه در صورتیکه از کلید خصوصی آگاه نباشند، قادر به تشخیص اطلاعات ارسالی چندمقصدی نیستند.

ادامه مقاله به صورت زیر است. در بخش ۲ شرح مختصری از مساله امنیت در کدگذاری شبکه به همراه مرور مقالات آن ارائه می‌شود. در بخش ۳ روش جدید ارائه شده است و مزیت‌ها و معایب آن در مقایسه با روش‌های موجود به تفصیل بیان می‌شود. در بخش ۴ امنیت روش پیشنهادی را بررسی می‌کنیم. با توجه به معایب بیان شده در بخش سوم، در بخش ۵ روش پیشنهادی را به گونه‌ای اصلاح می‌کنیم که این ضعف‌ها نیز برطرف شوند. نتیجه‌گیری و پیشنهاد برای ادامه کار در بخش ۶ مطرح شده است.

۲- معرفی کدگذاری امن و کدگذاری امن ضعیف شبکه

شبکه مخابراتی بدون دور با گراف جهت‌دار شبکه $G=(V,E)$ را در نظر می‌گیریم که V مجموعه گره‌های شبکه و E مجموعه کانال‌های شبکه، $E \subseteq V \times V$، است. در ارسال چندمقصدی، گره منبع S می‌خواهد اطلاعات $\mathbf{x}=(x_1,x_2,\cdots,x_h)^{\mathrm{T}}$ را به گره‌های مقصد $D=(d_1,d_2,\cdots,d_{|D|})$ ارسال کند. تمامی کانال‌های شبکه بدون خطا هستند و ظرفیت آنها برابر 1 (و یا مضرب صحیحی از آن) است. در [۶] فرض شده است که دشمن امکان دسترسی و شنود به تعداد محدودی از کانال‌ها در شبکه، یعنی $A \subset E$، را دارد. مجموعه کانال‌های واردشونده به گره v را با $\mathrm{In}(v)$ و گره‌های خارج‌شونده از آن را با $\mathrm{Out}(v)$ و تعداد اعضای مجموعه را نیز با نماد $|\ |$ نمایش می‌دهیم. برای این شبکه می‌خواهیم حداکثر نرخ ارسال چندمقصدی که دارای امنیت ضعیف باشد(یعنی دشمن با شنود کانال‌های A، متوجه پیام ارسالی نگردد) را بدست آوریم. با فرض $A=\varnothing$، مساله به کدگذاری شبکه [۱] کاهش می‌یابد. در این صورت ظرفیت ارسال چندمقصدی شبکه، یعنی h، با به کارگیری کدگذاری شبکه قابل حصول است.

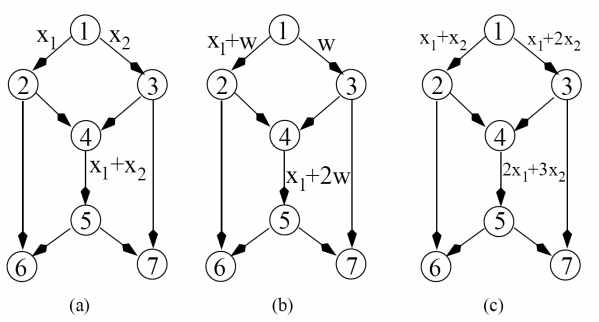
شکل ۱-(a) استفاده از کدگذاری شبکه برای رسیدن به ظرفیت ارسال چندمقصدی شبکه را ، که در این شکل برابر 2 است، نشان می‌دهد. به بیان دیگر برای رسیدن به ظرفیت، باید در گره شماره 4 کدگذاری خطی شبکه انجام شود. در [۶] برای یک کدگذاری شبکه ارسال چندمقصدی بدون سیکل با نرخ h نشان داده شده است که اگر n پیام مستقل، $n<h$، شنود شود، در این‌صورت می‌توان کد خطی شبکه را اصلاح کرده و با نرخ $h-n$ به ارسال چندمقصدی امن اطلاعات پرداخت. شکل ۱-(b) استفاده از کدگذاری شبکه را برای ارسال امن اطلاعات [۶] نشان می‌دهد. در این

مثال با استفاده از یک متغیر تصادفی کمکی w، که مستقل از اطلاعات ارسالی است، پیام‌های ارسالی را به صورت تصادفی درآورده و آن‌ها را از دشمنی که توانایی شنود فقط یک کانال را دارد، پنهان می‌کنیم. امنیت مورد نظر [۶] امنیت تئوری اطلاعاتی (امنیت مطرح شده توسط شانون) است یعنی اطلاعات متقابل بین پیام‌های ارسالی منبع و اطلاعات شنیده شده توسط دشمن، $I(X;A)$، صفر است. البته همان طور که در ۱-(b) در می‌یابیم ظرفیت ارسال چندمقصدی امن در این شبکه به 1 کاهش می‌یابد.

کد خطی شبکه بر روی گراف G با $(G,\Phi,h,\mathrm{F_q})$ تعریف می‌گردد که در آن Φ نگاشت ورودی- خروجی برای هر گره شبکه، h نرخ ارسال منبع، $\mathrm{F_q}$ میدانی با اندازه q (که توابع کدگذاری بر روی آن تعریف می‌شوند)، و q عددی اول یا توانی از یک عدد اول $q = p \ \ or \ \ p^m$ است. در کدگذاری خطی شبکه[۹]، پیام ارسالی بر روی کانال $e_j \in E$ شبکه را به صورت $\boldsymbol{\gamma}_{e_i}\mathbf{x}$ نمایش می‌دهیم که $\boldsymbol{\gamma}_{e_i}$ برداری سطری به طول h با عناصری از $\mathrm{F_q}$ است.

در کدگذاری خطی شبکه، اگر گره منبع ترکیبی خطی از سمبل‌ها را، به جای خود آن سمبل‌ها، ارسال کند، اطلاعات عبوری (ارسالی) روی کانال‌های شبکه باز هم ترکیبی خطی از همان سمبل‌ها هستند. در این حالت پیام ارسالی منبع برابر $\mathbf{Cx}$ و پیام ارسالی روی کانال e_j برابر $\boldsymbol{\gamma}_{e_i}\mathbf{Cx}$ است. در این روش، اطلاعات ارسالی از کانال‌های خروجی گره منبع برای دشمن قابل فهم نیستند؛ بدون اینکه نیازی به استفاده از متغیر تصادفی اضافی، و در نتیجه کاهش نرخ ارسال چندمقصدی، برای امنیت بخشیدن به سیستم (روش مطرح شده [۶]) باشد. زیرا در بقیه کانال‌های شبکه، با فرض استفاده از کدگذاری خطی شبکه، اطلاعات ارسالی در هر کانال، ترکیبی از سمبل‌های اطلاعاتی منبع است که برای دشمن قابل فهم نیست.

در [۸]، با توجه به این نکته که دسترسی به یک سمبل از اطلاعات ارسالی الزاما به معنی دسترسی مستقیم به همه یا حتی بخشی اطلاعات ارسالی نیست، مفهوم امنیت ضعیف، (weak security)، تعریف شده است. برای مثال، دشمن با دست یافتن به بیت $x_1 \oplus x_2$ از اطلاعات ارسالی روی کانال‌های شبکه در شکل ۱-(a)، قادر به یافتن



شکل ۱- مثال‌هایی از کدگذاری امن شبکه و امن ضعیف بر روی یک شبکه نمونه.

اطلاعات مشخصی در مورد هر یک از بیت‌های x_1 و x_2 نیست. هر چند این امنیت، امنیت تئوری اطلاعات نیست، ولی برای بسیاری از کاربردها کافی به نظر می‌رسد. در بسیاری از کاربردها، امنیتی کمتر از امنیت شانون، یعنی ایجاد ابهام در مورد اطلاعات ارسالی، با هدف جلوگیری از دستیابی دشمن به اطلاعات چندمقصدی ارسالی، کافی است. این ایده، یعنی secret sharing، اولین بار توسط Shamir در [۷] مطرح گردید. بنابراین انجام کدگذاری شبکه تا حدودی باعث امنیت بخشیدن به سیستم، حداقل در برابر شنود اطلاعات می‌شود.

در [۸] نشان داده شده است که می‌توان بدون نشت (درز) اطلاعات معنی‌دار و نیز بدون کاستن از نرخ ارسال چندمقصدی، به ارسال اطلاعات با امنیت ضعیف به کمک کدگذاری شبکه پرداخت به شرطی که تعداد سمبل‌های مستقل در اختیار دشمن، یعنی $|A| = n$، از ظرفیت ارسال چندمقصدی شبکه، یعنی h، کمتر باشد. شکل ۱-(c)، روشی برای ارسال امن ضعیف با کدگذاری شبکه با نرخ 2 را برای این شبکه نشان می‌دهد. با سمبل‌های ارسال شده در کانال‌ها، و به شرط شنود تنها یک کانال از کانال‌های شبکه، یعنی $|A| = n = 1$، دشمن نمی‌تواند اطلاعات معنی‌داری در مورد سمبل‌های ارسالی منبع بدست آورد. در شکل ۱- (c) کدگذاری شبکه با بزرگتر کردن میدان مورد استفاده دارای امنیت ضعیف گردیده است. در روش پیشنهادی، برای نیل به امنیت شکل ۱-(c)، فقط لازم است که سمبل‌های خروجی منبع را تغییر داد و نیازی به تغییر دادن توابع کدگذاری شبکه در گره‌های میانی شبکه نیست. به عبارت دیگر پس از ترکیب اطلاعات در گره مبدا، که روش پیشنهادی [۸] است، همان توابع کدگذاری شبکه

شکل ۱-(a) در شکل ۱-(c) استفاده شده‌اند و بر خلاف [٦]، نیازی به محاسبه مجدد توابع کدگذاری شبکه برای گره‌های میانی نیست. به علاوه، عموما برای برقراری امنیت ضعیف، لازم است که اندازه میدان مورد استفاده (شکل‌های ۱-(b) و ۱-(c)) افزایش یابد.

از نظر نیت دشمن، امنیت شبکه‌ای را که در آن از کدگذاری شبکه استفاده شده است می‌توان به سه دسته زیر تقسیم کرد [۹]:

۱- امنیت در برابر شنود (استراق سمع) اطلاعات. در این حمله هدف دشمن بدست آوردن بخشی از اطلاعات ارسالی در شبکه است.

۲- امنیت در برابر گره‌های مزاحم[۱۰] (مانند گره‌هایی که به قصد مزاحمت و اختلال در شبکه‌های بی‌سیم به شبکه اضافه می‌شوند، یا گره‌هایی از شبکه که دشمن به آنها نفوذ کرده است). دشمن در تلاش است تا با دستکاری[۱۱] در همه یا بخشی از اطلاعات، موجب دریافت اطلاعات غلط در گیرنده‌ها شود. در صورت استفاده از کدگذاری شبکه، حتی ورود یک بسته غلط به شبکه می‌تواند باعث پخش سریع اطلاعات غلط در شبکه شود. نتیجه فوری چنین عملی، عدم رسیدن به ظرفیت ارسال چندمقصدی در شبکه است.

۳- امنیت در مقابل حملات اختلال[۱۲] در شبکه. این حملات برای از بین بردن یک یا چند کانال ارتباطی در شبکه یا عدم امکان دریافت (ارسال) اطلاعات در یک یا چند گره شبکه اجرا می‌شوند.

در رمزنگاری، سه دسته مطرح شده از حملات ممکن در شبکه را بر این اساس که آیا دشمن به صورت فعال قصد شرکت در حمله دارد یا نه، طبقه‌بندی می‌کنند. بر پایه این طبقه‌بندی، دسته اول یک حمله غیر فعال[۱۳] است. در حالی که حملات دسته دوم و سوم حملات فعال[۱٤]اند، یعنی در این حملات، هدف دشمن دستکاری در محتوای اطلاعات ارسالی، ارسال یک پیام معتبر قدیمی و یا مشاهده و استفاده از رفتار شبکه در برابر دریافت اطلاعات دستکاری شده است. در این مقاله، چالش‌های امنیتی ارسال با کدگذاری خطی شبکه در حضور دشمن غیرفعال را مورد توجه قرار می‌دهیم.

در [۱۰] نشان داده شده است که مساله ارسال امن اطلاعات با کدگذاری خطی شبکه، معادل با یافتن کد خطی با خواص تعمیم یافته‌ای در مورد فاصله کلمات کد است. در [۱۱]، [۱۳]، و [۱۵]، کدگذاری شبکه در حالتی‌که دشمن دست به تزریق اطلاعات می‌زند را در نظر گرفته و نشان داده‌اند که با اضافه کردن افزونگی[۱۵] مناسب به ارسال چندمقصدی، می‌توان با حمله دشمن مقابله کرده و خطاهای تحمیلی به ارسال را، به شرط آنکه از کران تعیین‌شده توسط توپولوژی شبکه کمتر باشد، تصحیح نمود. در [۱۲] با همکاری گره‌های غیر دشمن، روشی برای جلوگیری از انتشار اطلاعات گره‌هایی که بسته‌های مخرب ارسال می‌کنند معرفی شده است. همچنین در [۱۶] روش امضای دیجیتالی مطرح شده که می‌تواند به همراه کدگذاری شبکه استفاده گردد.

در بخش ۳ روشی را ارائه می‌کنیم که امنیت نظریه اطلاعاتی در ارسال با کدگذاری شبکه را فراهم می‌کند و در عین حال در آن نیازی به افزایش اندازه میدان، مانند روش کدینگ شبکه با امنیت ضعیف در [۸]، نیست. به علاوه، در مقایسه با [۶] و [۸]، دارای مزایا و برتری‌های متعددی است. البته این روش نیاز به توافق قبلی بر روی کلید خصوصی و یا ارسال کلید از طریق کانال خصوصی امن به تمامی گره‌های مقصد دارد. پس از توضیح موارد برتری و اختلاف این روش با روش‌های موجود، و بررسی مباحث امنیتی آن، در بخش ۵ روش پیشنهادی را به گونه‌ای اصلاح می‌کنیم که محدودیت‌های یاد شده برطرف گردد اما سیستم دارای امنیت ضعیف می‌شود.

۳- استفاده از رمزنگاری کلید خصوصی در ارسال با کدگذاری شبکه

در [۸] برای حصول امنیت از نوع ضعیف، در ارسال با کدگذاری شبکه پیشنهاد شده است که به جای ارسال $\mathbf{x}$ بر روی شبکه، بردار $\mathbf{Cx}$، که با ترکیب سمبل‌های بردار $\mathbf{x}$ با ماتریس $\mathbf{C}$ بدست می‌آید، ارسال شود. روش پیشنهادی ما برای امن‌تر نمودن سیستم، استفاده از یک بردار تصادفی دیگر (یعنی کلید خصوصی ارسال چندمقصدی) است. به این ترتیب که به جای ارسال $\mathbf{Cx}$ آنرا با بردار $\mathbf{k}$ نیز جمع نموده و نتیجه حاصل، یعنی $\mathbf{x'=Cx+k}$ را برای ارسال به عنوان بردار اطلاعات ورودی به شبکه در نظر بگیریم.

مولفه‌های بردار $\mathbf{k}=(k_1,k_2,...,k_h)^T$ عناصری از میدان $\mathrm{F_q}$ هستند که به صورت تصادفی و با توزیع یکنواخت انتخاب می‌شوند.

شبکه مفروض G، پیش از استفاده از روش‌های امنیتی پیشنهادی را در نظر بگیرید. با توجه به استفاده از کدگذاری خطی شبکه، می‌توان ارسال اطلاعات $\mathbf{x}$ از گره منبع به هر گره مقصد d_i را به وسیله ماتریس انتقال $\mathbf{M}_{S\to d_i}$ نمایش داد[۳]. به این ترتیب در گره مقصد d_i اطلاعات $\mathbf{y}_{d_i}=\mathbf{M}_{S\to d_i}\mathbf{x}_S$ دریافت می‌شود. منظور از $\mathbf{M}_{S\to d_i}$ تابع انتقال شبکه از گره مبدا S به گره مقصد d_i است. برای اینکه اطلاعات خارج‌شونده از تمامی کانال‌های خروجی از گره منبع، ترکیبی از سمبل‌های اطلاعاتی منبع باشد، در [۸] پیشنهاد ترکیب بوسیله ماتریس $\mathbf{C}$ به صورت

$$\begin{cases}\mathbf{x}'=\mathbf{C}\mathbf{x}\\ \mathbf{y}_{d_i}=\mathbf{M}_{S\to d_i}\mathbf{x}'=\mathbf{M}_{S\to d_i}\mathbf{C}\mathbf{x}\end{cases} \qquad (۱)$$

ارائه شده است. روش پیشنهادی این مقاله به صورت زیر است

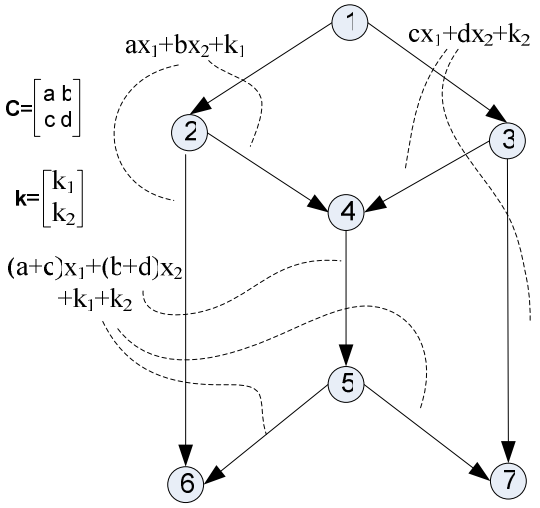
$$\begin{cases}\mathbf{x}'=\mathbf{C}\mathbf{x}+\mathbf{k}\\ \mathbf{y}_{d_i}=\mathbf{M}_{S\to d_i}\mathbf{x}'=\mathbf{M}_{S\to d_i}(\mathbf{C}\mathbf{x}+\mathbf{k})\end{cases} \qquad (۲)$$

برای بازیابی اطلاعات ارسال چندمقصدی در مقصدها، با توجه به آگاهی آنها از کلید خصوصی $\mathbf{k}$ و ماتریس $\mathbf{C}$، داریم

$$\mathbf{x}=\mathbf{C}^{-1}(\mathbf{M}^{-1}_{S\to d_i}\mathbf{y}_{d_i}-\mathbf{k}) \qquad (۳)$$

با توجه به استفاده از کدگذاری خطی و اینکه هدف، ارسال چندمقصدی به گره‌های D است، گره‌های میانی نیازی به دانستن ماتریس $\mathbf{C}$ و بردار $\mathbf{k}$ ندارند. گره‌های میانی بر اساس کد شبکه موجود با مولفه‌های بردار $\mathbf{x}'$ سروکار دارند. برای بازیابی اطلاعات $\mathbf{x}$، تنها مقصدهای D نیاز به آگاهی از ماتریس $\mathbf{C}$ و بردار $\mathbf{k}$ دارند. به این ترتیب $\{\mathbf{C},\mathbf{k}\}$ را می‌توان کلید خصوصی برای این سیستم دانست و این روش در واقع استفاده از رمزنگاری کلید خصوصی هنگام ارسال با کدگذاری شبکه است. گره منبع S و گره‌های مقصد قبلا بر روی $\{\mathbf{C},\mathbf{k}\}$ توافق نموده‌اند. در شکل ۲، این روش برای شبکه شکل ۱ به کار برده شده است.

استفاده از رمزنگاری کلید خصوصی به صورت مستقل و مجزای از ارسال با کدگذاری شبکه، یعنی رمز نمودن



شکل۲- استفاده از روش پیشنهادی برای انجام کدگذاری امن ضعیف شبکه.

اطلاعات با کلید خصوصی مستقل از کد شبکه مورد استفاده، را می‌توان به صورت

$$\mathbf{x}'=\mathbf{x}+\mathbf{k} \qquad (۴)$$

نمایش داد. بنابراین و با مقایسه (۲) و (۴)، تفاوت روش پیشنهادی این مقاله با استفاده صرف از رمزنگاری کلید خصوصی آشکار می‌شود. این روش در مقایسه با مقالات موجود، به خصوص [۶] و [۸]، برتری‌های زیر را دارد:

۱- با فرض خصوصی بودن بردار کلید $\mathbf{k}$، یعنی ارسال آن از طریق کانال خصوصی امن برای تمامی گره‌های مقصد، امنیت سیستم، امنیت نظریه اطلاعاتی است. به بیان دیگر بردار کلید مستقل از بردار اطلاعات و ماتریس ترکیب کننده $\mathbf{C}$ بوده و عناصر آن با توزیع یکنواخت از میدان $\mathrm{F_q}$ انتخاب می‌گردند.

۲- عدم نیاز به افزایش اندازه میدان مورد استفاده، یعنی q، برای حصول خواسته‌های امنیتی. در [۶] با فرض شنود n کانال توسط دشمن، حداقل اندازه میدان لازم برابر $q\geq\binom{|E|}{n}$ است. حال ماتریس $\mathbf{A}$ را که سطرهای آن حاوی ضرایب کدگذاری کانال‌های شنود شده است در نظر می‌گیریم. در [۸] با فرض $n=\mathrm{rank}(\mathbf{A})<h$ ثابت شده است که یک ماتریس تبدیل[۱۶] (ترکیب، نگاشت) $\mathbf{C}_{h\times h}$ با عناصری از میدان $\mathrm{F_q}$، با شرط

$q^h > |A| q^n + q^{h-1}$، وجود دارد که با به کارگیری آن در منبع می‌توان کد شبکه بیان شده را امن ضعیف نمود. این در حالیست که در مورد کدگذاری شبکه بدون در نظر گرفتن امنیت، میدان مورد نیاز برابر $q \geq |D|$ است[۲]. روش پیشنهادی ما نیازی به استفاده از میدانی بزرگتر از $q \geq |D|$ ندارد. البته بر حسب امنیت مورد انتظار و احتمال شنود قابل قبول در گره‌ها می‌توان q مناسب را انتخاب کرد (به بخش ۴ نگاه کنید).

۳- روش‌های [۶] و [۸] تنها در صورتی قابل استفاده هستند که تعداد کانال‌های تحت شنود توسط دشمن، یعنی h، از ظرفیت ارسال چندمقصدی شبکه، یعنی h، کمتر باشد. در روش پیشنهادی این مقاله، این مقدار حداقل برابر $\frac{1}{4}h^2 + 2h$ است. دشمن برای فهم اطلاعات ارسالی در یک بار ارسال نیازمند به دستیابی به اطلاعات کافی برای بدست آوردن پارامترهای ماتریس $\mathbf{C}$ و بردارهای $\mathbf{k}$ و $\mathbf{x}$ است. مجموع تعداد پارامترهای این سه، برابر $h^2 + 2h$ پارامتر است. دشمن شنود کننده باید به اندازه کافی کانال از میان کانال‌های شبکه شنود کند تا بتواند به کمک اطلاعات آنها مقادیر این پارامترها را استخراج نماید. شرط مورد نیاز در مورد ماتریس $\mathbf{C}$ در روش پیشنهادی با توجه به رابطه (۳) معکوس‌پذیری این ماتریس در میدان $\mathrm{F_q}$ است. در [۱۴] نشان داده شده که حداقل $\frac{1}{4}$ این ماتریس‌ها معکوس‌پذیرند. اگر دشمن به این نکته توجه کند، می‌تواند فضای جستجوی خود برای یافتن ماتریس $\mathbf{C}$ را کوچک‌تر نماید. لذا حداقل تعداد کانال‌های مورد نیاز برای دشمن به منظور دستیابی به مولفه‌های مجهول سیستم برابر $\frac{1}{4}h^2 + 2h$ است. (به بخش ۴ نگاه کنید.)

۴- در روش‌های [۶] و [۸] نیاز است که پیش از طراحی کد امن/امن ضعیف شبکه، از مجموعه کانال‌های شنود شونده توسط دشمن، یعنی مجموعه A، آگاهی داشته باشیم. در روش پیشنهادی ما نیازی به دانستن این مجموعه نیست و تنها بر روی تعداد اعضای آن محدودیت داریم. روش مقاله [۸] تنها برای یک بار ارسال در شبکه قابل استفاده است. در حالی که روش [۶] قابلیت استفاده برای تعداد نامحدودی ارسال را دارد. در بخش ۵ مقاله، روش پیشنهادی را به گونه‌ای تعمیم می‌دهیم که برای چندین ارسال قابل استفاده شود. روش پیشنهادی محدودیت موجود در [۶] یعنی ثابت با زمان بودن مجموعه A را ندارد. در روش پیشنهادی نیازی به تغییر عملکرد گره‌های میانی شبکه نیست و تنها باید تغییر جزئی در عملیات کدگذاری شبکه در گره منبع و کدگشایی در گره‌های مقصد اعمال کنیم.

۵- در تمامی مقالات موجود در مورد امنیت ارسال با کدگذاری شبکه، فرض شده گره‌های میانی شبکه، گره‌های خودی هستند. در این مقالات تنها توانایی دشمن غیرفعال، شنود کانال‌های مجموعه A، از کانال‌های شبکه است. در حالی‌که در کلی‌ترین حالت، دشمن غیرفعال می‌تواند در تعدادی از گره‌های شبکه نیز حضور داشته باشد. در واقع هر گره میانی شبکه تنها موظف است بر اساس کد خطی شبکه مورد توافق، اطلاعات دریافتی خود را به نحو مناسب برای ارسال پردازش کند. اما همین گره ممکن است علاقه‌مند به فهم اطلاعات چندمقصدی ارسالی در شبکه باشد. روش پیشنهادی این مقاله برای اولین بار این تهدید امنیتی را نیز مورد توجه قرار داده است. در این مورد در بخش بعدی پارامتری به نام احتمال شنود (موفقیت آمیز) اطلاعات توسط دشمن در تعدادی از گره‌های میانی شبکه معرفی و محاسبه شده است.

۶- روش پیشنهادی به پیچیدگی کدبرداری از کد شبکه و بازیابی اطلاعات اصلی منبع نمی‌افزاید. با توجه به رابطه (۳)، عملیات اضافی مورد نیاز، کم کردن $\mathbf{C}^{-1}\mathbf{k}$ از $\mathbf{C}^{-1}\mathbf{M}^{-1}{}_{d_i}\mathbf{y}_{d_i}$ است. با توجه به ثابت بودن $\mathbf{C}^{-1}\mathbf{k}$، تنها یک بار به محاسبه آن نیاز است.

روش پیشنهادی ما حالت کلی‌تری از روش [۸] است؛ با در نظر نگرفتن بردار کلید، یعنی $\mathbf{k} = \mathbf{0}$، در رابطه (۲) روش پیشنهادی به روش [۸] کاهش می‌یابد. روش [۸] نیز خود

حالت عام‌تری از روش [۶] است. روش [۶] نیز تعمیمی از روش secret sharing [۷] برای استفاده در شبکه است.

برتری‌های روش مطرح شده را در مقایسه با روش مقالات [۶] و [۸] بررسی نموده‌ایم. در ادامه این بخش، دو عیب روش فعلی را بیان می‌کنیم. آنگاه در بخش ۵، روش پیشنهادی برای ارسال امن اطلاعات با کدینگ شبکه را به نحوی اصلاح می‌کنیم که این نقص‌های روش نیز بر طرف شوند.

۱. در روش پیشنهادی **برای هر بار ارسال** امن اطلاعات، با امنیت نظریه اطلاعاتی، نیازمند ارسال یا توافق قبلی بر روی بردار کلید خصوصی $\mathbf{k}$ هستیم. به بیان دیگر اگر بردار کلید خصوصی ارسال بردار اطلاعات در لحظه t، یعنی $\mathbf{x}(t)$، را با $\mathbf{k}(t)$ نمایش دهیم، باید $\mathbf{k}(t)$ یا از طریق کانال خصوصی امن به گره‌های مقصد منتقل شود و یا پیش از شروع ارسال اطلاعات گره منبع و گره‌های مقصد بر روی حجم بزرگی از کلید خصوصی برای استفاده در ارسال‌ها توافق نمایند. هر چند فرض دوم قابل قبول است، به دنبال راه حلی هستیم تا بتوانیم نیاز به آن را بر طرف کنیم.

۲. استفاده از بردار $\mathbf{k}$ یکسان برای ارسال بردار اطلاعات چندمقصدی در لحظات مختلف، برای مثال $\mathbf{x}(t=i)$ و $\mathbf{x}(t=j)$، از نظر امنیتی قابل قبول نیست. زیرا دشمن می‌تواند با حمله تفاضلی، یعنی محاسبه تفاضل سمبل‌های ارسالی روی کانال‌های یکسان شنود شده در لحظات متفاوت، به ترکیب خطی از اطلاعات گره منبع دسترسی یابد. به منظور مقابله با چنین حمله‌ای باید کلید مورد استفاده در لحظات ارسال مختلف $t=i$ و $t=j$ متمایز باشند.

بر آورده کردن هر دو خواسته فوق و در عین حال انتظار داشتن امنیت نظریه اطلاعاتی در ارسال، در تضاد با یکدیگر هستند. به بیان دیگر، بده بستانی (مصالحه‌ای)[۱۷] بین امنیت سیستم، قابلیت استفاده از آن برای چندین ارسال و عدم نیاز به ارسال کلید از طریق کانال خصوصی امن وجود دارد. در بخش ۵، روش پیشنهادی را به نحوی اصلاح می‌کنیم که دو عیب فوق نیز برطرف شود. البته در این حالت، دیگر امنیت سیستم امنیت نظریه اطلاعاتی نیست، بلکه مشابه [۸] به امنیت ضعیف کاهش می‌یابد. در بخش بعدی ملاحظات امنیتی روش مطرح شده را بررسی می‌کنیم.

۴- امنیت سیستم

اکنون به بحثی در مورد امنیت سیستم با توجه به معیارهای شانون برای ارزیابی امنیت می‌پردازیم. با توجه به اینکه دیگر نیازی به استفاده از میدانی بزرگتر از $q \geq |D|$ برای تامین امنیت نیست، مطالعه فضای کلیدها و بررسی تعداد اعضای آن حیاتی است. همچنین می‌دانیم فاصله قابل شکست[۱۸]، یعنی N_0، در سیستم مضربی از آنتروپی کلید است. فضای کلیدها، شامل فضای بردار $\mathbf{k}$ و فضای ماتریس $\mathbf{C}$ است، که ذیلا به آنها اشاره می‌کنیم.

۴-۱- فضای بردار $\mathbf{k}$ و تعداد اعضای ممکن آن

بردار $\mathbf{k}$ دارای h مولفه از میدان $\mathrm{F_q}$ است. با فرض اینکه مولفه‌های آن مستقل از یکدیگر و با توزیع یکنواخت از میدان $\mathrm{F_q}$ انتخاب گردند، تعداد عناصر آن برابر با

$$|K_{\mathbf{k}}| = q^h - 1 \approx q^h \qquad (۵)$$

و آنتروپی آن $H(K_{\mathbf{k}}) = \log(q^h) = h\log(q)$ است.

۴-۲- فضای ماتریس $\mathbf{C}$ و تعداد اعضای ممکن آن

در مورد تعداد ممکن ماتریس‌های $\mathbf{C}$ با خواص مورد نظر، در [۸]، تنها برای حالت $n<h$ و $q^h > |A|q^n + q^{h-1}$ وجود یک ماتریس ثابت گردیده است. در روش پیشنهادی ما با توجه به رابطه (۳)، تنها شرط لازم برای $\mathbf{C}$ معکوس‌پذیر بودن است. تعداد ماتریس‌های معکوس‌پذیر $\mathbf{C}_{h\times h}$ در $\mathrm{F_q}$، یعنی $|K_{\mathbf{C}}|$، برابر است با

$$\begin{aligned} |K_{\mathbf{C}}| &= (q^h-1)(q^h-2)\ldots(q^h-q^{h-1}) \\ &= q^{h^2}\prod_{i=0}^{h-1}(1-q^{-i}) \end{aligned} \qquad (۶)$$

در [۱۴] نشان داده شده که احتمال اینکه یک ماتریس $h\times h$ با درآیه‌هایی از میدان $\mathrm{F_q}$ معکوس‌پذیر باشد از $\frac{1}{4}$ بیشتر است. بنابراین برای تعداد ماتریس $\mathbf{C}$ می‌توان کران پایین زیر را بیان کرد

$$|K_{\mathbf{C}}| \geq \tfrac{1}{4}q^{h^2} \qquad (۷)$$

با فرض هم احتمال بودن انتخاب، آنتروپی آن برابر $H(K_{\mathbf{C}}) \geq \log(\frac{1}{4}q^{h^2}) = h^2 \log(q) - 2$ است.
بنابراین فاصله قابل شکست سیستم برابر

$$H(K) = |K_{\mathbf{C}}| + |K_{\mathbf{k}}| \geq \log(\tfrac{1}{4}q^{h^2}) = (h^2 + h)\log(q) - 2. \quad (۸)$$

است.

۴-۳- احتمال شنود اطلاعات توسط دشمن در گره‌های میانی

با توجه به استفاده از کدگذاری خطی شبکه در مورد اطلاعات دریافتی در گره میانی v می‌توان نوشت

$$\mathbf{y}_v = \mathbf{M}_{S\to v}\mathbf{x}' = \mathbf{M}_{S\to v}(\mathbf{C}\mathbf{x} + \mathbf{k}) \quad (۹)$$

برای آگاهی یافتن از پیام ارسالی منبع، یعنی $\mathbf{x}$، دشمن نیازمند به آگاهی از $\{\mathbf{C},\mathbf{k}\}$ است. بنابراین احتمال شنود برابر با احتمال انتخاب صحیح $\{\mathbf{C},\mathbf{k}\}$ در رابطه (۹) است. با توجه به عدم آگاهی این گره از کلیدهای خصوصی فوق، این گره تنها می‌تواند کلیدهای فوق را حدس بزند. اگر فرض کنیم این گره قادر است اثر ارسال اطلاعات بر روی شبکه، یعنی اثر ماتریس $\mathbf{M}_{S\to v}$، را حذف نماید، حداکثر می‌تواند بخشی از اطلاعات تزریقی به شبکه، یعنی $\mathbf{x}'_{\mathrm{In}(v)\times 1}$ را بدست آورد. در این صورت احتمال شنود موفقیت آمیز، برابر احتمال حدس زدن زیر بخش‌های صحیحی از کلیدها، یعنی $(\mathbf{C}'_{\mathrm{In}(v)\times \mathrm{In}(v)}, \mathbf{k}'_{\mathrm{In}(v)\times 1})$، است. با توجه به بندهای ۴-۱ و ۴-۲ حداکثر این احتمال برابر است با

$$p_{\text{interception}} = \frac{4}{q^{(\mathrm{In}(v))^2}} \frac{1}{q^{\mathrm{In}(v)}} \quad (۱۰)$$

به این ترتیب باید بر اساس میزان امنیت قابل قبول در شبکه، اندازه میدان مورد نیاز، یعنی q، را انتخاب کرد.

۵- تلفیق رمزنگاری کلید خصوصی و کدینگ شبکه

می‌خواهیم روش پیشنهادی بخش ۳ را به نحوی اصلاح کنیم که

۱. نیاز به ارسال کلید خصوصی از طریق کانال خصوصی را بر طرف کنیم.
۲. برای ارسال در زمان‌های مختلف از کلیدهای خصوصی مختلفی استفاده نماییم.

راه حل پیشنهادی در این مورد، تولید کلید خصوصی به وسیله پارامترهای موجود در سیستم ارسال است به نحوی که دیگر نیاز به تبادل کلید به گره‌های مقصد d_i نباشد و این گره‌ها قادر باشند با اطلاعات در اختیارشان کلید خصوصی متناظر ارسال در لحظات مختلف را استخراج نمایند.

در این روش، کلید خصوصی ارسال در لحظه t، یعنی $\mathbf{k}(t)$ به کمک ماتریس $\mathbf{C}$ و تعداد h بردار چندمقصدی ارسال شده در لحظات قبلی، یعنی بردار $\mathbf{x}$ در زمان‌های $t-i$ تا $t-(i+h-1)$، تولید می‌شود. بنابراین تمامی گره‌های مقصد قادرند این کلید خصوصی را استخراج نمایند. معادلات روش ارسال جدید و نحوه تولید کلید در آن عبارتند از

$$\begin{cases} \mathbf{x}'(t) = \mathbf{C}\mathbf{x}(t) + \mathbf{k}(t) \\ \mathbf{y}_{d_i}(t) = \mathbf{M}_{S\to d_i}(\mathbf{C}\mathbf{x}(t) + \mathbf{k}(t)) \\ \mathbf{k}(t)\ is\ derived\ \ from\ charcteristic \\ equation\ of\ matrix\ \mathbf{C}\mathbf{X}(t-i)\mathbf{C} \end{cases} \quad (۱۱)$$

سطر آخر رابطه (۱۱) بیان می‌کند که اگر معادله مشخصه[19] به صورت $\varphi(\lambda) = \lambda^h + k_{h-1}\lambda^{h-1} + ... + k_1\lambda + k_0$ باشد، بردار کلید را به صورت $\mathbf{k}(t) = (k_{h-1}, k_{h-2}, ..., k_0)^T$ از آن استخراج می‌کنیم. ماتریس $\mathbf{X}(t-i)$ به صورت زیر با کنار هم قرار دادن بردارهای اطلاعات ارسال چندمقصدی زمان‌های قبلی به صورت ستونی تشکیل می‌شود. با فرض $i=1$، برای h ارسال اولیه نیازمند یک ماتریس $\mathbf{B}_{h\times h}$ هستیم. به عبارت دیگر برای زمان $t=1$، به جای ماتریس $\mathbf{X}(0)$، که موجود نیست، از ماتریس $\mathbf{B}$ استفاده می‌کنیم. برای زمان‌های بعدی تا $t=h$، به ترتیب ستون‌های $\mathbf{B}$ را از سمت چپ با بردارهای چندمقصدی ارسال شده در زمان‌های قبلی، جایگزین می‌کنیم. بنابراین در لحظه $t=j<h$ ماتریس مورد استفاده به جای ماتریس $\mathbf{X}$ عبارت است از

$$\mathbf{X} = [\ \underbrace{\mathbf{B}((h-(j-1)):h)}_{end\ h-(j-1)\ columns\ of\ \mathbf{B}}\ ,\ \underbrace{\mathbf{x}(1),...,\mathbf{x}(j-1)}_{j-1\ column\ vector}\ ] \quad (۱۲)$$

که منظور از $\mathbf{B}((h-(j-1)):h)$، ستون‌های $h-(j-1)$ تا h ماتریس $\mathbf{B}$ هستند. در این حالت ماتریس‌های $\{\mathbf{B},\mathbf{C}\}$ خصوصی هستند و تنها گره منبع و گره‌های مقصد از آنها آگاهی دارند.

هدف اصلی طراحی روش فوق، قابلیت استفاده از روش پیشنهادی برای چندین ارسال بر روی شبکه است. به علاوه

برای هر ارسال، کلید خصوصی متمایزی تولید و استفاده می‌کنیم. مهم‌ترین مزیت روش فوق این است که بر خلاف تمامی مقالات موجود دیگر نیازی به فرض ثابت با زمان بودن مجموعه کانال‌های تحت شنود دشمن، یعنی $\forall t : A(t) = fix$، نیست. هر چند امنیت بدست آمده با این روش امنیت نظریه اطلاعاتی نیست. همچنین با توجه به استفاده از بردارهای متمایز کلید در لحظات مختلف ارسال، حمله تفاضلی دشمن نیز بی اثر شده است. به بیان دیگر دشمن با حمله تفاضلی نمی‌تواند صرفا با استفاده از اطلاعات شنود شده، سمبل‌های ارسالی یا حتی ترکیبی از آن‌ها را تشخیص دهد. تمامی مزیت‌های بیان شده در بخش سوم، به جز مورد اول یعنی امنیت نظریه اطلاعاتی، همچنان برقرار هستند. البته در مورد حداقل تعداد کانال‌های شنود که برای بدست آوردن اطلاعات ارسالی لازم است، با توجه به آنچه که در زیر می‌آید وضعیت بهتر می‌شود.

تعداد پارامترهای وارد شده (تزریقی) به شبکه پس از تعداد T ارسال برابر است با

$$\underbrace{h^2}_{\mathbf{B}}+\underbrace{h^2}_{\mathbf{C}}+\underbrace{T.h}_{\mathbf{x}'s:multicast\ vectors}+\underbrace{T.h}_{\mathbf{k}'s:key\ vectors}=2h^2+2T.h$$

اگر n_i تعداد کانال‌های شنود شده در لحظه ارسال $t=i$ باشد، برای اینکه دشمن نتواند به هیچ بخش از اطلاعات چندمقصدی ارسالی دسترسی پیدا کند باید داشته باشیم:

$$\sum_{i=1}^{T} n_i < 2h^2 + 2T.h \qquad (۱۲)$$

اگر $\overline{n}$ را متوسط تعداد کانال‌های شنود شده در ارسال‌ها در نظر بگیریم، برای اینکه دشمن نتواند به اطلاعات چندمقصدی ارسالی بر روی شبکه دسترسی پیدا کند باید داشته باشیم

$$T \cdot \overline{n} < 2h^2 + 2T.h \rightarrow \overline{n} < 2h(1+\tfrac{h}{T}) \qquad (۱۳)$$

بنابراین، و درحالت حدی، در این روش دشمن باید به طور متوسط حداقل در هر ارسال $2h$ کانال از کانال‌های شبکه را شنود کند تا قادر باشد به اطلاعات ارسالی دسترسی پیدا کند.

به این ترتیب قید پایه‌ای موجود در [۶] و [۸]، یعنی عدم تغییر مجموعه کانال‌های شنود شده توسط دشمن، بر طرف می‌شود. به علاوه، در صورت استفاده از روش مقالات [۶] و [۸] باید پیش از طراحی کد امن شبکه از مجموعه کانال‌های شنود شده توسط دشمن، یعنی مجموعه A، آگاهی داشته باشیم که فرض معقولی نیست. در واقع در صورت تغییر این مجموعه باید کد امن/امن ضعیف شبکه مجددا طراحی شود. در روش پیشنهادی تنها قید موجود در مورد تعداد این کانال‌ها است. همچنین تعداد مجاز کانال‌های شنود شده برای حصول امنیت ضعیف از h در [۸] به $2h$ افزایش یافته است.

۶- نتیجه‌گیری و پیشنهاد

در این مقاله روشی جدید برای امن نمودن ارسال چندمقصدی در شبکه با استفاده از کدگذاری شبکه در حضور دشمن غیر فعال ارائه گردیده است. در مورد نوع امنیت روش پیشنهادی (امنیت نظریه اطلاعاتی یا امنیت ضعیف) بر حسب نحوه مبادله کلید خصوصی بحث نمودیم. در روش پیشنهادی، بر خلاف روش مقالات [۶] و [۸] نیازی به آگاهی از مجموعه کانال‌های شنود شده، یعنی A، پیش از طراحی کد امن/ امن ضعیف نیست. به علاوه در این روش تعداد کانال‌هایی که شنود آنها منجر به بدست آوردن کلید توسط دشمن می‌شود از مرتبه h^2 است؛ در حالی‌که در [۶] و [۸] این مقدار از مرتبه h است.

تنها توانایی در نظر گرفته شده در مقالات برای دشمن غیرفعال، امکان شنود مجموعه‌ای از کانال‌های شبکه است. برای اولین بار، در این مقاله ما این توانایی را به حضور دشمن غیرفعال در تعدادی از گره‌های شبکه گسترش دادیم. به بیان دیگر دلیلی ندارد گره‌های میانی شبکه را خودی فرض کنیم. آنها تنها موظف هستند بر اساس کدگذاری شبکه مشخص شده، داده‌های دریافتی را پردازش و ارسال نماید. این گره‌ها می‌توانند کنجکاو باشند تا از محتوی اطلاعات ارسالی آگاهی یابند.

روش پیشنهادی اول، در بخش سوم، قابلیت استفاده برای چندین ارسال را ندارد. در بخش پنجم، با اصلاح روش پیشنهادی، روش به گونه‌ای تغییر یافت که امکان استفاده از آن برای چندین ارسال فراهم گردید. البته این روش اصلاح شده دارای امنیت نظریه اطلاعاتی نیست و امنیت ضعیف دارد.

روش پیشنهادی اصلاح شده را می‌توان تلفیق یک سیستم رمزنگاری کلید خصوصی و کدگذاری شبکه دانست. با توجه به اینکه در ارسال چندمقصدی، هدف ارسال اطلاعات به مجموعه‌ای از گره‌ها، یعنی گره‌های مقصد، است، فرض اطلاع این گره‌ها از کلیدهای خصوصی، فرض

معقول و قابل دفاعی است. امنیت سیستم را بررسی، و تعداد کلیدها و احتمال شنود موفقیت آمیز را نیز محاسبه کرده‌ایم.

امنیت و کدگذاری شبکه در حالتی که کدگذاری شبکه در گره‌های میانی به صورت تصادفی انجام می‌شود، و استفاده از کدگذاری غیرخطی، زمینه‌های مناسبی برای پژوهش‌های آتی هستند. به علاوه تمرکز این مقاله بر مباحث و چالش‌های امنیتی ارسال با کدگذاری شبکه در حضور دشمن غیر فعال بود. محور مناسب دیگر برای پژوهش، بررسی چالش‌های امنیتی ارسال با کدگذاری شبکه در حضور دشمن فعال و ارائه روش‌های مناسب ارسال در چنین شبکه‌هایی است. مطالعه به منظور تدوین حملات رمزنگاری به روش‌های ارسال امن اطلاعات با کدگذاری شبکه نیز موضوعی جذاب برای مطالعات آتی است.

مراجع

[۱] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. on Information Theory*, vol. 46, pp. 1204-1216, 2000.

[۲] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, pp. 371-381, 2003.

[۳] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782-795, October 2003.

[٤] T. Ho, *Networking from a Network Coding Perspective*. PhD Dissertation, MIT, 2004.

[٥] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp.1973-1982, June 2003.

[٦] N. Cai and R. W. Yeung, "Secure network coding," *Proceedings of the ISIT 2002*, Lausanne, Switzerland, 2002.

[۷] E. Shamir, "How to share a secret," *Comm. ACM*, vol. 22, pp. 612-613, 1979.

[۸] K. Bhattad and K. Narayanan, "Weakly secure network coding," *Proceedings of the NetCod 2005*, Italy, April 2005.

[۹] C. Fragouli, J.-Y. L. Boudec, and J. Widmer, "Netwrok coding: an instant primer," *ACM Computer Communication Review*, vol. 36, pp. 63-68, 2006.

[۱۰] J. Feldman, T. Malkin, R. A. Servedio, and C. Stein, "On the capacity of secure network coding," *Proceedings of the 42nd Annual Allerton Conferance on Comm. Cont. and Comp.*, Monticello, IL., 2004.

[۱۱] S. Jaggi, M. Langberg, T. Ho, and M. Effros, "Correction of adversarial errors in networks," *Proceedings of the International Symposium in Information Theory and its Applications*, Adelaide, Australia, 2005.

[۱۲] C. Gkantsidis and P. Rodriguez, "Cooperative security for network coding file distribution," *Proceedings of the IEEE INFOCOM*, 2006.

[۱۳] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Medard, *Resilient network coding in the presence of Byzantine adversaries*, MIT Computer Science and Artificial Intelligence Laboratory Technical Report 2006.

[۱٤] Y. X. Li, D. X. Li, and C. K. Wu, "How to generate a random nonsingular matrix in McEliece public-key cryptosystem," *Proceedings of the IEEE ICCS/ISITA*, Singapore, 1992.

[۱٥] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. R. Karger, "Byzantine modification detection in multicast networks using randomized network coding," *Proceedings of ISIT'04*, Chicago, 2004.

[۱٦] D. Charles, K. Jain, and K. Lauter, "Signatures for network coding," *Proceedings of the 40th Annual Conference on Information Sciences and Systems (CISS),* Princeton, NJ, USA, 2006.

[1] Security
[2] Weak Security
[3] Intercept
[4] Secure Network Coding (SNC)
[5] Network Coding (NC)
[6] Field
[7] Deterministic Network Coding
[8] Polynomial
[9] Linear Network Coding

[10] Malicious
[11] Modification
[12] Jamming
[13] Passive
[14] Active
[15] Redundancy
[16] Transformation
[17] Trade off
[18] Unity Distance
[19] Characteristic Equation