معرفی چند روش جدید جهت بهبود امنیت انتقال داده با کدینگ شبکه

حسن خمامی پامساری
دانشگاه آزاد اسلامی مرکز آستانه اشرفیه
h-khomami@yahoo.com

چکیده: در این مقاله روشهای جدیدی برای بهبود امنیت ارسال با کدینگ شبکه ارائه کرده ایم. این روش استفاده همزمان از رمز نگاری کلید خصوصی هنگام ارسال با کدینگ شبکه است. در این روش حداقل تعداد کانالهای شنود شده توسط دشمن که منجر به یافتن اطلاعات ارسالی توسط دشمن میشود متناسب با مجذور ظرفیت ارسال چند مقصدی شبکه است، در حالی که این مقدار برای روشهای فعلی از مرتبه h است. همچنین برای اولین بار در مباحث امنیتی کدینگ شبکه، بحث غیر خودی بودن گره های میانی شبکه در این مقاله مورد توجه قرار گرفته است.از مزیت های دیگر این روش، عدم نیاز به استفاده از میدانی با تعداد عناصر بسیار زیاد برای حصول خواسته های امنیتی است. به علاوه پیچیدگی افزوده شده به عملیات سیستم بسیار ناچیز است زیرا کد شبکه تنها در گره منبع و گره های مقصد نیاز به اصلاح دارد. همچنین بر خلاف روش های موجود ، نیازی به فرض آگاهی قبلی از کانالهای مورد شنود توسط دشمن، برای طراحی کد امن شبکه نیست. با توجه به اینکه فرض وجود کانال خصوصی امن برای ارسال کلید خصوصی در شبکه، فرض محدود کننده ای است ، روش تدوینی به گونه ای اصلاح شده تا کلید خصوصی به کمک اجزا و پارامترهای موجود در ارسال با کدینگ شبکه تولید شود و نیاز به ارسال کلید خصوصی برطرف گردد.

واژه های کلیدی: : امنیت، دشمن غیر فعال، شنود (استراق سمع)، کدینگ شبکه، کدینگ امن ضعیف شبکه، نظریه اطلاعات، نظریه اطلاعات شبکه.

مقدمه

شانون با مقاله برجسته خود[1]، پایه ی زمینه تازه ای در انتقال داده به نام نظریه اطلاعات را بنیان نهاد. در این مقاله او به تعریف اطلاعات، مدل سازی و مطالعه مساله ارسال اطلاعات از یک نقطه، با نام منبع یا فرستنده، به نقطه دیگر، با نام گیرنده یا مقصد، پرداخت و کرانه های عملکرد در مورد چنین کانالی را بدست آورد.

در طی شصت سالی که از ارائه این مقاله می گذرد، مساله ارسال از یک نقطه به یک نقطه(P2P) تقریبا از تمامی جهات مورد بررسی قرار گرفته است. کران های ظرفیت، سیگنالینگ بهینه و انواع روش های کدینگ منبع و کدینگ کانال برای آن مطرح و بررسی گردیده است. در مقابل، در مورد ساده ترین ساختار شبکه ای، شامل بیش از دو گره (گره های منبع و مقصد)و تعدادی کانال متصل کننده این گره ها به هم، مانند شبکه رله که شامل یک فرستنده، یک گیرنده و یک رله برای تسهیل ارتباط بین فرستنده و گیرنده است، هنوز دانش و آگاهی کافی در دسترس نیست. به علاوه فاصله نتایج نظری موجود با میزان به کارگیری آنها بسیار زیاد است.

کدینگ شبکه که در مقاله ی پایه ای Li,Cai,Ahlswede و Yeung،[2]معرفی گردید، زمینه ای جدید در نظریه اطلاعات شبکه است که در آن با توجه مناسب به هدف نهایی ارسال، که انتقال اطلاعات در شبکه است، مساله ارسال چند مقصدی در شبکه ای با کانال های بدون خطا، سنکرون و بدون تاخیر ارسال بر روی کانالهای شبکه بدون تاخیر ناشی از پردازش در گره های میانی شبکه را بیان کرده و ناحیه ظرفیت آن را تعریف و بدست آورده است. این مقاله پس از گذشت تنها 8 سال به عنوان یک مقاله پایه، تاثیر گذار پذیرفته شده است. شاید اصلی ترین دلیل آن این نکته باشد که برای اولین بار به انتقال اطلاعات، به عنوان انتقال شار با ماهیت غیر فیزیکی در شبکه توجه نمود. شار با ماهیت غیر فیزیکی، در مقابل شار با ماهیت فیزیکی که محتوای آن دارای واحدهای مجزا و متمایز از یکدیگرند که قابل ترکیب یا ممزوج شدن با یکدیگر نیستند، عنوان میشود. به بیان دیگر کوچکترین ذره سازنده شار با ماهیت فیزیکی قابلیت ترکیب و تجزیه شدن را ندارد. در مقابل انتقال هایی وجود دارند که اجزای سازنده آن دارای ماهیتی غیر فیزیکی هستند که مهمترین آن سمبل های اطلاعاتی می باشند، در عین حال که دو/ چند سمبل اطلاعاتی از هم متمایز هستند، میتوان بر حسب نیاز ترکیبهای متفاوتی از آنها با محتوای انتقالی برابر محتوی هر یک از سمبلهای اولیه تولید نمود.

1- مقدمه ای بر کدینگ شبکه، مزایا و معایب

با گسترش چشمگیر استفاده و به کار گیری انواع شبکه ها، بخصوص شبکه های بی سیم، این سوال که حد نهایی ارسال و انتقال اطلاعات در یک شبکه چه میزان است، دوباره مورد توجه و اهمیت قرار گرفته است[3]. این موضوع به خصوص از این نظر شایان توجه است که پس از کاهش علاقه به مباحث ظرفیت در کانالهای چند کاربره در اوایل دهه 1980، بیشتر پژوهش ها و مطالعات انجام گرفته در زمینه بهبود عملکرد بلوک ها ورسیدن به نحو انجام بهینه عملیات هر بلوک بوده است. مقاله برجسته و پایه ای Ahlswede و همکاران[2]، باعث جلب نظر دوباره و علاقمندی به نظریه اطلاعات شبکه گردید. دلیل اصلی جایگاه و اقبال کدینگ شبکه را میتوان توجه همزمان و توام این

مقاله به منابع شبکه و محدودیت آنها بـه همـراه هـدف غـایی نظریـه اطلاعات شبکه(ارسال حداکثر ممکن اطلاعات در شبکه) دانست.

1-1 مزایای استفاده از کدینگ شبکه

بعضی از اصلی ترین مزایای استفاده از کدینگ شبکه، عموما در مقایسه با مسیریابی، عبارتند از:

1- امکان رسیدن به کران بالای استفاده از یک شبکه برای ارسال چند مقصدی(که با تعمـیم قضـیه Max-flow Min – cut به حالت چند مقصدی بدست می آید.): در [2] ثابت شده که در شبکه ای بـا کانـال هـای بـدون خطا و بدون تاخیر در ارسال و پـردازش در گـره هـای میانی که تمامی ارسال ها سـنکرون بـا یکـدیگر انجـام میشوند، مستقل از توپولوژی موجود شبکه میتـوان بـه ظرفیت ارسال چند مقصـدی شـبکه در ارسـال دسـت یافت فقط و فقط اگر از کدینگ شبکه اسـتفاده کنـیم. در غیر اینصـورت دسـتیابی بـه ظرفیـت ارسـال چنـد مقصدی به توپولوژی شبکه بستگی دارد.

نویسندگان مقاله[4] نشان دادنـد کـه کـدینگ خطـی شبکه برای رسیدن به ظرفیـت ارسـال چنـد مقصـدی شبکه کافی است. روش و فرمول بندی جبـری مطـرح شده توسط Medard و Koetter [5] ساده تر، جـذاب تر و در عین حال مناسبتر و کاراتر اسـت. البتـه نشـان داده شده که برای حالت کلـی تـر، داشـتن چنـد شـار متمایز ارسالی، برای مثال ترکیبی از شار چند مقصدی و چنـد شـار unicast ، کـدینگ خطـی شـبکه بـرای رسیدن به ظرفیت کلی نیست.

2- صرفه جـویی در مصـرف تـوان: در کلـی تـرین حالـت، باتوجه به متغیر بودن توپولوژی شبکه، محدوده ارسـال گره های شبکه، نوع تداخل بین ارسـال هـا و بسـیاری پارامترهای دیگر، پاسخ به این سوال که میـزان صـرفه جویی حاصل از بکارگیری کدینگ شبکه در مقایسه بـا عدم اسـتفاده از آن چیسـت، بنظـر ممکـن نیسـت. در موارد خاصی، مانند ثابت توپولوژی، ثابت شبکه و فرض یکسان بودن توان ارسال و برابر بودن فاصله همـه گـره ها با هم، نتایجی در[6] ارائه شده است. در مورد شبکه واقعی، توپولوژی شـبکه بـه الگـوی حرکـت کـاربران و پارامترهای متعدد دیگر وابسته اسـت و تنهـا بـا شـبیه سازی میتوان نتایجی بدست آورد.

صـرفه جـویی حاصـل از بکـارگیری کـدینگ شـبکه، بخصوص در مورد شبکه های بی سیم میتواند کارگشـا باشد. در این حالت عملکرد کـدینگ شـبکه را بایـد بـا عملکرد الگوریتم های ارسالی که از مسیریابی اسـتفاده نمی کنند، ماننـد Probabilistic Flooding مقایسـه کنیم که در این صورت کدینگ شـبکه عملکـرد بسـیار بهتری، حتی در حالاتی که میزان ارسال به گـره هـای بعدی در کدینگ شبکه بسیار کمتر از Probabilistic Flooding است، نشان میدهد.[7]

3- عدم نیاز به مسیریابی در شبکه: در[5] نشان داده شده که مسیریابی در شبکه حالت خاصی از کـدینگ شـبکه است. در این مقاله این مساله به صورت ریاضـی مـدون گردیده است. آنها همچنین به مساله مقاوم بودن شبکه در مقابل از دست دادن دایمی بعضی از کانالهای شبکه در هنگام استفاده از کدینگ شبکه، فرمول بنـدی ایـن مسئله و بررسی شرایط جواب دار بودن آن پرداخته اند. میدانیم بـا آگـاهی از توپولـوژی شـبکه، یـافتن جـواب مسئله مسیریابی در شبکه یک مسئله NP-compelet است، در حالیکه ثابت شده حل مسئله کدینگ شـبکه، یعنی یافتن بردارهای کد شبکه مناسـب بـرای تمـامی گره های شبکه که با استفاده از آنهـا حصـول ظرفیـت ارسال چند مقصدی قطعی است، دارای پیچیدگی چند جمله ای است.[8]

4- صرفه جویی پهنای بانـد:کـاهش اسـتفاده از کانالهـا در شبکه را میتوان معادل با صرفه جویی در پهنای باند در شبکه دانست.

5- کاهش تاخیر در ارسال اطلاعات شبکه

6- عبور متعادل تر شار اطلاعات بر روی کانال های شبکه

1-2 معایب استفاده از کدینگ شبکه

معایب و مشکلات زیر را در مورد استفاده از کدینگ شبکه میتـوان نـام برد :

1- نیاز به بدون تاخیر بودن شبکه.

2- وابستگی و حساسیت بیشتر اطلاعات نسبت به عدم دریافت، ناشی از عدم دریافت یا خطاهای احتمالی در کانالهای شبکه، در مقایسه با شبکه های مبتنی بر مسیر یابی: فرض معمـول در شبکه های کامپیوتری، بدون خطا بودن کانالها(لینک ها) در شبکه است. روش کدینگ شـبکه بـر مبنـای ایـن فـرض حداکثر کارایی خود را میتواند بروز دهد.

2- روش پیشنهادی برای افزایش امنیت کـدینگ شـبکه: استفاده از سیستم رمز نگاری کلید خصوصی به همراه کدینگ شبکه

نویسندگان مقاله[9] برای تامین امنیت، از نوع ضعیف، در سیستم پیشنهاد می کنند که به جای ارسال x بروی شبکه، بردار Cx، که با ترکیب سمبل های بردار x با ماتریس C بدست می آید، ارسال شود. روش پیشنهادی اولیه این مقاله برای امن تر نمودن سیستم، استفاده از یک بردار تصادفی کلید خصوصی است. به این ترتیب که بجای ارسال Cx آن را با بردار k نیز جمع نموده و نتیجه حاصل $x'=Cx+k$، را برای ارسال به عنوان بردار اطلاعات ورودی به شبکه در نظر بگیریم. مولفه های بردار $k=(k_1,k_2,\dots k_n)^T$ عناصری از میدان F_q هستند که بصورت تصادفی و با توزیع یکنواخت انتخاب می گردند. در ادامه این بخش فرض میکنیم که میدان دارای تعداد q میتواند عددی اول یا توانی از یک عدد اول $q=p\ or\ p^m$ باشد.

گره های میانی شبکه نیازی به دانستن ماتریس C وبردار k ندارند؛ آنها بر اساس کد موجود شبکه با مولفه های بردار x' سروکار دارند. برای بازیابی اطلاعات x تنها مقصدهای $\{d_1,d_2,\dots d_{|D|}\}$ نیاز به آگاهی از بردار k و ماتریس C دارند. فرض میکنیم که گره منبع و گره های مقصد قبلا بر روی بردار k و ماتریس C توافق نموده اند.

برای توضیح روش مطرح شده، شبکه مفروض در [10] پیش از استفاده از روش امنیتی را در نظر بگیرید. با توجه به استفاده از کدینگ خطی شبکه، میتوان ارسال اطلاعات x از گره منبع به هر گره مقصد d_i را بوسیله ماتریس انتقال $M_{s\to d_i}$ نمایش داد[5]. به این ترتیب در گره ی مقصد d_i اطلاعات $y_{di}=M_{s\to d_i}x_S$ دریافت میشود. منظور از $M_{s\to d_i}$ تابع انتقال شبکه از گره مبدا S به گره مقصد d_i است.در [9] برای اینکه اطلاعات خارج شونده از تمامی کانال های خروجی از گره منبع ترکیبی از سمبل های اطلاعاتی منبع باشد، ترکیب بوسیله ماتریس C بصورت

$$\begin{cases} x'=Cx, \\ y_{di}=M_{s\to d_i}x'=M_{s\to d_i}Cx \end{cases} \qquad (3\text{-}1)$$

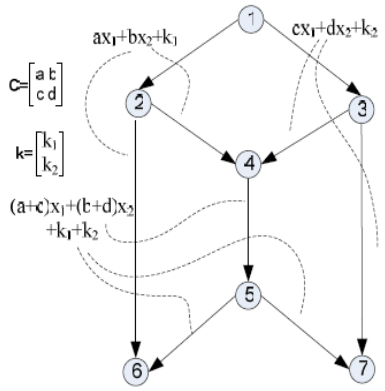
پیشنهاد شده است. روش پیشنهادی ما را میتوان به صورت زیر بیان نمود.

$$\begin{cases} x'=Cx+k, \\ y_{di}=M_{s\to d_i}x'=M_{s\to d_i}(Cx=k) \end{cases} \qquad (3\text{-}2)$$

که x' بردار اطلاعات وارد شونده به شبکه است. به کمک رابطه ی سطر اول (3-2)، بردار اطلاعات x را از دسترس مستقیم دشمن پنهان نموده ایم. به عبارت دیگر با استفاده از ماتریس ترکیب کننده C و بردار k، مولفه های x' در حال ارسال بر روی کانالهای شبکه برای دشمن شنود کننده غیر قابل فهم و مبهم گشته است. برای بازیابی اطلاعات چند مقصدی در مقصدها، با توجه به آگاهی مقصدها از کلید خصوصی k و ماتریس C، داریم.

$$x=C^{-1}(M^{-1}_{s\to d_i}y_{di}-k) \qquad (3\text{-}3)$$

مجموعه ی (C,k) را میتوان کلید خصوصی برای این سیستم ارسال چند مقصدی دانست و این سیستم را میتوان سیستم رمز نگاری کلید خصوصی- کدینگ شبکه نامید. گره منبع s و گره های مقصد D قبلا بروی (C,k) توافق نموده اند. این سیستم مزایای استفاده همزمان از رمز نگاری کلید خصوصی و کدینگ خطی شبکه را داراست. برای مثال در شکل 1-3، این روش برای مثال معروف کدینگ شبکه،بکار برده شده است.



شکل 1-3. استفاده از روش پیشنهادی برای انجام کدینگ امن شبکه.علاوه بر ماتریس ترکیب کننده C در گره منبع از بردار کلید خصوصی k هم استفاده شده است. با توجه به اینکه مولفه های بردار کلید خصوصی کاملا مستقل از اجزای دیگر و با توزیع یکنواخت از میان عناصر ممکن میدان انتخاب گردیده اند، نوع امنیت فراهم شده نظریه اطلاعاتی است. بکارگیری کلید خصوصی مزیت های امنیتی متعددی در هنگام ارسال با کدینگ شبکه فراهم می آورد.

برای این روش پیشنهادی میتوان ملاحظات زیر را بیان نمود:

1- عدم نیاز استفاده از میدانی بزرگ برای امن نمودن سیستم. در[10] با فرض اینکه دشمن میتواند n کانال از بین تمامی کانال های شبکه را برای شنود انتخاب نماید، ثابت شده حداقل اندازه میدان لازم $q\geq\binom{|E|}{n}$ است.در[9] با فرض $n=max_{A_i\varepsilon A}rank(A_i)<h$ ثابت شده یک ماتریس تبدیل $C_{h\ Xh}$ باعناصری از میدان F_q، با شرط $q^h>|A|q^n+q^{h-1}$، وجود دارد که با بکارگیری آن در گره منبع میتوان کد شبکه امن را ضعیف نمود. این در حالتیست که در مورد کدینگ شبکه بدون در نظر گرفتن ملاحظات امنیتی، اندازه میدان مورد نیاز $q\geq|D|$ است[4]. در روش پیشنهادی ما، اگر مباحث امنیتی جدید مانند احتمال شنود گره های میانی را در نظر نگیریم، نیازی به استفاده از میدانی بزرگتر از $q\geq|D|$ نیست. البته بر حسب میزان امنیت مورد انتظار و حداکثر احتمال شنود موفقیت آمیز قابل قبول در گره های میانی، میتوان مقدار مناسب اندازه میدان q را انتخاب نمود.

2- روش مقالات [10،9]تنها با این شرط که تعداد کانالهای تحت شنود توسط دشمن، یعنی n، از ظرفیت ارسال چند

مقصدی شبکه کمتر باشد امنیت ضعیف را فراهم میکنند. به بیان دیگر به محض اینکه تعداد کانالهای شنود شده بیشتر از h شود،تمامی اطلاعات ارسالی توسط دشمن قابل شنود میشود. میخواهیم در مورد روش پیشنهادی بدانیم حداکثر تعداد کانالهای شنود شونده توسط دشمن که منجر به فاش شدن اطلاعات چند مقصدی نمیشود چقدر است؟ برای پاسخ به این پرسش بحثی را ارائه میکنیم که جواب سوال مهم دیگری را نیز فراهم بیاورد.سوالاتی که میخواهیم در مورد روش مطرح شده به آنها پاسخ دهیم عبارتند از:

2-1 دشمن با شنود چه تعداد کانال از کانالهای شبکه قادر به یافتن اطلاعات ارسالی در شبکه خواهد بود؟

2-2 دشمن با نفوذ و رخنه کردن به چه تعداد گره از گره های شبکه قادر به یافتن اطلاعات ارسالی در شبکه خواهد بود؟

2-3 ظرفیت ارسال چند مقصدی امن در شبکه در روش ما چقدر است؟

به سوالات 2-1 و2-2 بصورت مشترک جواب میدهیم. در روش مطرح شده بردار ارسالی بر روی هر کانال شبکه شامل اطلاعاتی در مورد عناصر ماتریس C و بردارk،یعنی اجزای تشکیل دهنده کلید سیستم، است. میخواهیم بدانیم دشمن برای یافتن بردار پیام ارسالی ما با چه تعداد مجهول مواجه است؟

فرض کنید ظرفیت ارسال چند مقصدی شبکه برابر h است، در این صورت ماتریس C دارای ابعاد $h\times h$ و بردار k مولفه ای است. بنابراین دشمن باید به تعداد بردار مناسب و مستقل خطی از هم، از بردارهای ارسالی روی کانالهای شبکه دسترسی داشته باشد تا بتواند به محتوای بردار x دست یابد. سوالات مطرح شده این است که در اختیار داشتن چه تعداد بردار ارسالی روی کانالهای شبکه برای این منظور لازم است؟

با توجه به اینکه تعداد مجهولات دشمن در یکبار ارسال جند مقصدی، بعنی مولفه های کلید (C,k) و بردار x، دارای h^2+2h مولفه است، تعداد کافی کانال مورد نیاز برای یافتن کلید و در نتیجه پیام ارسالی برابر h^2+2h کانال با بردارهای مستقل خطی از هم است. اگر شرط مستقل خطی بودن را بیان نکنیم، با احتمال زیادی شنود تعداد بیشتری کانال مورد نیاز است.

در مورد تعداد لازم، کران پایین تعداد کانالهای مورد نیاز برای دشمن، یعنی مقدار $\frac{1}{4}h^2+2h$ برابر حداقل تعداد بردارهای مستقل خطی از هم لازم برای دشمن به منظور بدست آوردن اطلاعات کلیدی است، زیرا دشمن هم از این واقعیت که ماتریس C باید معکوس پذیر باشد آگاه است. در[11] نشان داده شده که احتمال اینکه ماتریس $h\times h$ با درایه هایی از میدان F_q معکوس پذیر باشد از $\frac{1}{4}$ بیشتر است. میتوان مقدار فوق را حداقل تعداد کانالهای لازم برای دشمنی با توانایی محاسباتی نا محدود در نظر گرفت. بنابراین دشمن باید حداقل تعداد $\frac{1}{4}h^2+2h$ کانال مناسب، یعنی با بردارهای مستقل خطی از هم، را شنود کند تا بتواند اطلاعات ارسالی را بازیابی کند.

البته توجه داریم به محض اینکه دشمن این تعداد کانال با ویژگیهای بیان شده را شنود کند، اطلاعات لازم را در مورد کلید (C,k) را بدست آورده و ظرفیت ارسال امن شبکه به صفر کاهش می یابد. این مقدار در مورد مقاله [9] $n<h$ بود یعنی حداکثر کانالهای قابل شنود با روش آنها برای باقی ماندن امنیت ضعیف در سیستم $n=h-1$ بود، در حالیکه در روش ما مقداری برابر $\frac{1}{4}h^2+2h-1$ است.

سوال 2-2 در مورد حملات شنود اطلاعات، یعنی حملات غیر فعال، به سوال 2-1 شباهت دارد، زیرا هر گره v در اختیار دشمن، با توجه به اینکه قصد دشمن غیر فعال است، تعدادی برابر با In(v) کانال در اختیار دشمن قرار میدهد. البته توجه داریم که بردارهای این کانال ها ممکن است از هم مستقل نباشند. بنابراین برای اینکه دشمن بتواند به اطلاعات لازم، یعنی اطلاعات در مورد کلیدها دست یابد، باید حداقل مجموعه ای از گره ها در شبکه را در اختیار بگیرد که مجموع کانال های مستقل وارد شونده به آن $\frac{1}{4}h^2+2h$ باشد.

یک کران لازم برای هر دو سوال 2-1 و2-2 برابر $\frac{1}{4}h^2+2h$ است، زیرا ممکن است این تعداد کانال شنود شونده دارای همه اطلاعات لازم نباشند.

در مورد سوال2-3 در روش پیشنهادی به ازای $n\langle\frac{1}{4}h^2+2h$ میتوانیم با نرخ $r=h$ اطلاعات را به صورت امن ارسال کنیم. در این مورد نتایج مقالات به صورت خلاصه در جدول 3-1 آمده اند:

مقاله	حداقل تعداد کانال مورد شنود	ظرفیت ارسال چند مقصدی	نوع امنیت
[10]Secure NC	$n<h$	$r=h-n$	امن
Weakly Secure [9] NC	$n<h$	$r=h$	امن ضعیف
روش بخش 3	$n\langle\frac{1}{4}h^2+2h$	$r=h$	امن

جدول 1- مقایسه نتایج مقالات موجود از نظر تعداد کانال های مجاز برای شنود توسط دشمن و نوع امنیت ارسال

3- کاهش احتمال حدس زده شدن سمبل های اطلاعاتی توسط گره های میانی شبکه : آیا گره های میانی شبکه همچنان میتوانند متوجه اطلاعات ارسالی بروی شبکه و عبور از آن شوند؟ این نقیصه در بیشتر سیستمهای طرح شده، بخصوص [10,9] وجود دارد، به بیان دیگر بیشتر روشهای موجود، گره های شبکه را گره ی خودی فرض میکنند. این فرض در حالت کلی، فرض ساده انگارانه ای است. اگر خود را محدود به دشمن غیر فعال

کنیم، این دشمن با حضور در گره های میانی شبکه چه تهدیدهایی به امنیت ارسال تحمیل میکند؟ مهمترین تهدید امنیتی این است که یک گره میانی در شبکه میتواند همه یا بخشی از اطلاعات ارسالی را بدست آورد. در حالت عادی هم اگر یک گره میانی فعالیت مخربی برای جلوگیری از ارسال ما انجام ندهد، حداکثر خواست قابل انتظار از او این است که مطابق پروتکل تدوینی ارسال عمل کند. این گره میتواند نسبت به شنود اطلاعات ارسالی عبوری از خود، اقدام کند.

از مزایای روش پیشنهادی ما جلوگیری از شنود موثر اطلاعات ارسالی توسط گره های میانی شبکه است. با توجه به نیاز ، آگاهی از کلید خصوصی ارسال، یعنی بردار k، برای بازیابی اطلاعات، در حالت عادی تنها گره های مقصد قادر به ارزیابی اطلاعات هستند. یک گره میانی برای دست یابی به اطلاعات ارسالی ناچار است کلیدها را حدس بزند. بطور خاص در روش ما، با توجه به استفاده از کلید خصوصی و بحث قبلی، حداکثر احتمال شنود موفقیت آمیز اطلاعات چند مقصدی توسط گره میانی v برابر $P\text{int}erception = \frac{4}{q^{(ln(v))^2}}\frac{1}{q^{ln(v)}}$ است، زیرا دشمن تنها در صورتی که زیر بخشهای مناسبی از کلیدهای خصوصی، یعنی C و k را درست حدس بزند قادر به یافتن اطلاعات ارسالی است.

4- افزایش امنیت سیستم : با توجه به اینکه بردار کلید خصوصی، کاملا مستقل از بردار پیام، انتخاب میشود، امنیت سیستم مطرح شده امنیت نظریه اطلاعاتی است. زیرا با توجه به اضافه شدن بخش کلید به هر مولفه بردار، هر مولفه بردار با احتمال یکسانی میتواند یکی از عناصر میدان F_q باشد.

5- اگر میزان امنیت مطرح شده در [9] را بصورت I(ACx;x)=I(Cx;x) در نظر بگیریم، امنیت روش ما را میتوان به صورت I(A(Cx+k);x)=I(Cx+k;x) نمایش داد که با توجه به فرض استقلال کلید k از بردار اطلاعات x و ماتریس ترکیب کننده C میتوان نوشت:

$$I(A(Cx+k);x) = I(Cx+k;x) = \\ = I(k;x) + I(Cx;x\,|\,k) = I(Cx;x) \qquad (3\text{-}4)$$

پس با فرضهای انجام شده، امنیت روش مطرح شده حداقل برابر با امنیت روش[9]،I(Cx;x) است. زیرا اطلاعات متقابل تابعی نا منفی است. در [9] معادله معرفی شرط امنیت ضعیف، یعنی $I(\{x_i(t)\}_{t=1}^{\infty};M)=0$ تنها بردار x وجود دارد و اثری از ماتریس C و اثر آن بر اطلاعات متقابل این ترکیب ماتریسی، یعنی Cx نشده است. در حالیکه باتوجه به استفاده از ترکیب Cx باید در مورد I(Cx;x) بررسی و بحث میشد.

6- روش پیشنهادی به پیچیدگی کد گشایی از کد شبکه و بازیابی اطلاعات اصلی منبع نمی افزاید. با توجه به رابطه(3-3)، عملیات اضافی مورد نیاز کم کردن $C^{-1}k$ از $C^{-1}M^{-1}{}_{s\to d}y_{d_i}$ است. با توجه به ثابت بودن $C^{-1}k$، تنها یکبار به محاسبه آن نیاز است.

7- بر خلاف روش مقالات [10،9]، در روش پیشنهادی نیازی به آگاهی از کانالهای مورد شنود توسط دشمن، یعنی مجموعه A، پیش از طراحی کد امن شبکه نیست. در مقاله [10] روش پیشنهادی برای امنیت بخشی، باید از اعضای مجموعه A پیش از تولید کد امن شبکه آگاه باشد، زیرا کد امن شبکه در کانال های تحت شنود باید به گونه ای طرح شوند که شامل اطلاعات چند مقصدی نباشند. در روش [9] نیز انتخاب ماتریس C وابسته به آگاهی از این مجموعه است. در حالیکه روش پیشنهادی این مقاله، مستقل از انتخابهای مختلف ممکن مجموعه A از مجموعه E است و تنها تعداد اعضای مجموعه A تاثیر گذار است.

8- روش ما حالت کلی تر شده روش [9] است، با در نظر نگرفتن بردار کلید، یعنی k=0، در رابطه(2-3)روش پیشنهادی به روش [9] کاهش می یابد. روش [9] نیز خود حالت عام تری از روش [10] است. روش [10] نیز تعمیمی از روش secret sharing مطرح شده توسط Sharmir،[10] است.

توجه داریم در روش پیشنهادی این بخش برای هر بار ارسال چند مقصدی نیاز به توافق بر یک بردار کلید k، هم اندازه با بردار اطلاعات ارسالی یعنی برداری بطول h داریم. میتوان فرض نمود پیش از شروع ارسال بروی یک کلید خصوصی بزرگ K توافق نموده ایم و در لحظه t ام ارسال از بخش متناظر آن، برای مثال $k(t)=K((t-1)h+1,th)$ استفاده می کنیم. اما در این صورت، روش پیشنهادی مزیتی بر استفاده صرف رمزنگاری کلید خصوصی ندارد. راه حل ارسال کلید خصوصی بروی یک کانال امن نیز قابل قبول نیست، چون در صورت وجود چنین کانالی میتوان اطلاعات اصلی را روی آن ارسال نمود زیرا حجم اطلاعات کلید برابر با حجم اطلاعات ارسالی است. به علاوه باید این کانال خصوصی امن بین گره منبع و تمامی گره های مقصد وجود داشته باشد. روشی پیشنهادی در این بخش با فرض توافق بروی یک بردار کلید خصوصی k، تنها قابلیت استفاده برای یک ارسال را دارد.در بخش بعدی مزایا و معایب استفاده از این روش برای چندین ارسال را مورد بررسی قرار میدهیم.

3- آیااز روش بخش 3 میتوان برای چند ارسال استفاده نمود؟

در مورد روش پیشنهادی در بخش قبل مزایا و معایب آن بحث گردید. با فرض ثابت بودن ماتریس ترکیب کننده C و عدم توافق بر بیش از یک بردار کلید خصوصی k، میخواهیم مزایا و معایب سیستم را برای چندارسال چند مقصدی بررسی کنیم. در ادامه مقاله، در مورد تمامی بردارها وماتریس ها برای ارجاع دادن به زمانی مشخص از اندیس زمانی (t) استفاده میکنیم که t از 1 آغاز میشود. روابط اصلاحی مورد نظر را میتوان به فرم زیر بیان نمود.

$$\begin{cases} x'(t) = Cx(t) + k, \\ y_{d_i}(t) + M_{s\to d_i} x'(t) = M_{s\to d_i}(Cx(t)+k) \\ \sec retkey = \{C, k\} \end{cases} \quad (3\text{-}5)$$

در مورد روش بخش قبل اگر امنیت نظریه اطلاعاتی مورد نظر باشد، روش تنها برای یکبار ارسال قابل استفاده است. اگر امنیتی از نوع ضعیف قابل قبول باشد برای تعداد T ارسال بروی شبکه میتوان بحث زیر را بیان نمود. اگر تعداد کانالهای شنود شده توسط دشمن در t امین ارسال را با n_t نمایش دهیم با توجه به اینکه در T ارسال تعداد پارامترها (سمبلها)ی تزریق شده به شبکه برابر $h^2+h+T.h$ است، سیستم تا زمانی امنیت ضعیف دارد که :

$$\sum_i n_i \langle h^2 + h + T.h$$

با فرض تعریف پارامتر $\bar{n}$ بعنوان میانگین تعداد شنودهای دشمن در هر ارسال برای امن ضعیف بودن سیستم باید داشته باشیم :

$$\sum_i n^i = T.\bar{n}\langle \frac{1}{4}h^2 + h + T.h \to \bar{n}\langle h\left(1+\frac{1}{4}\frac{h}{t}+\frac{1}{T}\right)$$

بنابراین در حالت حدی و برای تعداد خیلی زیاد ارسال، شرط $\bar{n}\langle h$ در مورد تعداد شنودها باید برآورده شود. مشاهده میشود که این روش از نظر تعداد کانالهای مجاز برای شنود شدن توسط دشمن دارای عملکرد مشابه روش [9] است. البته مزایای دیگر این روش، یعنی مزایایی مشابه بخش قبل در،[9] موجود نیست. معایب این روش عبارتند از:

1- امنیت سیستم دیگر امنیت نظریه اطلاعاتی نیست بلکه امنیتی از نوع ضعیف است.
2- با توجه به اینکه بردار کلید در ارسالهای مختلف ثابت است، دشمن میتواند با حمله تفاضلی به بردارهایی تنها شامل ترکیبی از سمبل های گره منبع دسترسی پیدا کند.

برای برطرف نمودن نقص دوم از سیستم باید از یک بردار کلید متغیر با زمان استفاده کنیم. بعلاوه توجه داریم که نمیخواهیم این کلید خصوصی را بین گره منبع و گره های مقصد مبادله کنیم. در بخش بعدی روشی برای حصول این خواسته ها ارائه می کنیم.

4- سیستم تلفیقی کلید خصوصی – کدینگ شبکه

با فرض ثابت بودن ماتریس ترکیب کننده C، عیب عمده روش بخش 3 نیاز به توافق قبلی بروی بردار کلید خصوصی k برای هر ارسال است. زیرا کلید خصوصی برداری هم اندازه بردار اطلاعات چند مقصدی است. میتوان فرض نمود پیش از شروع ارسال، بروی کلید خصوصی به اندازه کافی بزرگ بین گره منبع و گرههای مقصد توافق شده است. در این بخش از مقاله میخواهیم بهبودی در روش مطرح شده در بخش 3 ارائه دهیم تا دیگر نیازی به ارسال قبلی با توافق بروی کلید به صورت خصوصی نباشد. در واقع میخواهیم ببینیم آیا با توجه به رابطه (3-2) میتوان بنحوی نیاز به ارسال یا توافق قبلی بروی کلید خصوصی را برطرف کنیم؟ بعلاوه روش مطرح شده قابلیت استفاده برای چندین ارسال چند مقصدی را دارا باشد.

روش پیشنهادی در این بخش از مزایای مشاهده شده در استفاده از یک سیستم کلید خصوصی در حین ارسال با کدینگ شبکه، بنحوی از این مزایا بهره میجوید و در عین حال نیاز به داشتن کانال خصوصی برای ارسال امن کلید خصوصی k را نیز برطرف میکند. روشی مفید خواهد بود که از پارامترهای موجود در سیستم برای تولید کلید خصوصی استفاده نماید بنحوی که کلید توسط گیرنده ها نیز قابل تولید باشد.

روش پیشنهادی در بخش 3 را بصورت زیر تصحیح می کنیم که در آن دیگر نیاز به ارسال کلید بردار کلید خصوصی نیست و هر گیرنده کست d_i با توجه به آگاهی از ماتریس C، که خصوصی است و بردارهای اطلاعات قبلی دریافت شده، قادر است کلید خصوصی ارسال در لحظه t ام را بدست آورد. این روش با معادلات زیر قابل توصیف است:

$$\begin{cases} x'(t) = Cx(t) + k(t), \\ y_{d_i}(t) = M_{s\to d_i} x'(t) = M_{s\to d_i}(Cx + k(t)) \\ \sec retkey = \{C\}, \end{cases} \quad (3\text{-}6)$$

$$\text{K(t)=diverd from Characteristicequation of} \begin{cases} 1.(Cx(t-i).(Cx(t-i))^T) \\ 2.CX\ (t-i)C \\ 3.CX(t-i)C+D \end{cases}$$

منظور از ماتریس X ماتریسی به شکل :

X=[x(t-i);x(ŧ (i+1));x(t-(i+2));…;x(t-(i+(h-1)))] است ،که از بردارهای اطلاعاتی ارسالی در زمانهای قبلی ساخته می شود. از بین سه شکل پیشنهادی، تنها در مورد شکل دوم به بحث می پردازیم. در مورد شکل پیشنهادی داخلی سوم برای تولید کلید خصوصی، یعنی استفاده از CX(ŧ i)C+D ، ماتریس D هم جزو کلیدهای خصوصی سیستم خواهد بود.

به بیان دیگر برای تولید کلید خصوصی از معادله مشخصه ماتریس CX(t-i)C استفاده کرده ایم. در این حالت مطمئن هستیم تمامی ضرایب معادله مشخصه در میدان F_q قرار دارند. منظور از (3-6) این است که از معادله مشخصه حاصل $\varphi(\lambda) = \lambda^h + k_{h-1}\lambda^{h-1} + \ldots + k_1\lambda + k_0$ بردار $k=(k_{h-1},k_{h-2},\ldots,k_0)^T$ را بدست آوریم و به عنوان کلید خصوصی استفاده نماییم.

هدف اصلی طراحی روش فوق، قابلیت استفاده از آن برای چندین ارسال بروی شبکه است. بعلاوه برای هر ارسال کلید خصوصی متمایزی تولید و استفاده می کنیم. مهمترین مزیت روش فوق این است که بر خلاف تمامی مقالات موجود ، دیگر نیازی به فرض ثابت با زمان بودن مجموعه کانال های تحت شنود دشمن، یعنی $\forall t : A(t) = fix$ نیست. هر چند امنیت بدست آمده با این روش، امنیت نظریه اطلاعاتی نیست. هنچنین 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 به سمبلی صرفا شامل ترکیبی از اطلاعات ارسالی دسترسی پیدا کند. در مورد اینکه شنود چه تعدا کانال از شبکه

در طی T ارسال میتواند منجر به یافتن اطلاعات لازم برای شکستن سیستم دشمن شود میتوان نوشت:

$$\sum_i n_i \langle h^2 + h^2 + h + T.h + T.h = 2h^2 + h + 2T.h \rightarrow \bar{n}\langle h(2 + \frac{1}{2}\frac{h}{T} + \frac{1}{T})$$

بنابراین در حالت حدی و بطور متوسط دشمن برای دستیابی به اطلاعات لازم برای شکستن سیستم نیاز به شنود $2h$ کانال در شبکه از هر ارسال چند مقصدی دارد.

5- نتیجه گیری

در این مقاله روش جدیدی برای امن نمودن ارسال چند مقصدی در شبکه با استفاده از کدینگ شبکه ارائه نموده ایم. روش اول به کارگیری رمز نگاری کلید خصوصی به همراه ارسال با کدینگ خطی شبکه است. در مورد مزیت های این روش در مقایسه با روش های موجود، بخصوص مقالات [9، 10] مباحثی ارائه کردیم. امنیت این روش با فرض توافق فرستنده و گیرنده ها بروی کلید خصوصی امنیت نظریه اطلاعاتی است. مانند مقالات [9، 10] فرض بر شنود تعدادی کانال توسط دشمن نمودیم. در این روش حداقل تعداد لازم کانال های شنود شده توسط دشمن که منجر به یافتن اطلاعات چند مقصدی توسط دشمن میشود از مرتبه h^2 است، در حالیکه در مقالات [10،9] این مقدار از مرتبه h بود. بعلاوه برای اولین بار در مباحث امنیتی کدینگ شبکه بحث غیر خودی بودن گره های میانی شبکه مورد توجه قرار گرفته است. در روشهای موجود امن کردن کدینگ شبکه عموما فرض بر خودی بودن تمامی گره های میانی شبکه میشود. در این مورد نتایجی درباره حداقل و حداکثر احتمال بازیابی موفقیت آمیز همه یا بخشی از اطلاعات ارسالی چند مقصدی در یک گره میانی ارائه گردیده است. در مورد امنیت سیستم مطرح شده، تعداد کلیدها در آن و فاصله قابل شکست نیز بحثی مطرح کردیم. از جمله مهمترین مزیت های روش پیشنهادی، عدم نیاز به استفاده از میدانی بسیار بزرگ برای حصول خواسته های امنیتی است.

با توجه با اینکه فرض وجود کانال خصوصی امن برای ارسال کلید در شبکه فرض مناسبی نیست، در بخش 5 روشی ارائه کردیم تا به کمک اجزا وپارامترهای موجود در ارسال با کدینگ شبکه نیاز به ارسال کلید خصوصی برطرف گردد. در مورد این روش مزیت ها مورد بررسی قرار گرفته و احتمال بازیابی اطلاعات در گره های میانی و احتمال شنود موفقیت آمیز اطلاعات بر حسب تعداد کانال از کانال های شبکه بدست آمده است.

مراجع

[1] C. E. Shannon, "A mathematical theory of communication," *Bell Systems Technical Journal*, vol.27, pp.379-423 and 623-656,1948

[2] R. Ahiswede, N. Cai, S. -Y. R. Li, and R. W. Yeung" Network Information Flow," *IEEE Transacation on Information Theory*, vol.46, pp.1204-1216,2000

[3] A. R. Lehman, "Network Coding , "Ph.D.Thesis, Dept .Elect . Eng.and Comp. Sci.,MIT,2005

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

[5] R. Koetter and M. Medard, "An algebraic approach to network coding" , *ACM/IEEE Transactions on Networking* , 2003

[6] J. Widmer, C. Fragouli, and J. -Y. L. Boudec, "Low-complexity energy-efficient broadcasting in wireless ad-hoc networks using network coding," in *Proc.of the 1st Conf. on Network Coding* Trentino,Italy,2005.

[7] J. Widmer and J. -Y. L. Boudec, "Network coding for efficient communication hn extreme networks," in *Proc. Of workshop on delay tolerant networking and related networks (WDYN-05)*. Philadelphia, PA, 2005.

[8] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, "Polynomial time algorithms for multicast network code costruction," *IEEE Transactions on Information Theory*, vol.51, pp.1973-1982, 2003.

[9] K. Bhattad and K .Narayanan, "Weakly secure network coding," in *Proc. of the 1st Conf. on network Coding (NetCod05)*. Trentino,Italy, 2005.

[10] N. Cai and R. W. Yeung, "Secure network coding," in *proc. of ISIT'02*, Lausanne. Switzerland, 2002.

[11] Y. X. Li, D. X. Li, C. K. Wu, "How to generate a random nonsingular matrix in McEliece public-key cryptosystem." In *pro. Of ICCS/ISITA IEEE,* Singapore,1992.

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

[13] Plamondon, R., Lorette, G., "Automatic Signature Verification and Writer Identification - The State of the Art", *Pattern Recognition*, Vol. 22, pp. 107-131, 1989.

[14] Object Management Group. *Unified Modeling Language: Superstructure*, Version 2.0, ptc/03-07-06, July 2003, http://www.omg.org/cgi-bin/doc?ptc/2003-08-02.