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

تحلیل ظرفیت امن کانال شنود دوطرفه متقارن

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

چکیده

بحث امنیت در تئوری اطلاعات با پیدایش کانال‌های شنود آغاز شد. کانال‌های شنود کانال‌هایی هستند که در آنها گیرنده‌های غیرمجاز نیز قادرند اطلاعات فرستنده‌ها را دریافت و بهره‌برداری می‌کنند. بطور کلی میزان نرخ اطلاعات قابل ارسال توسط فرستنده‌ها که بوسیله هیچ گیرنده‌ای جز گیرنده‌های مجاز قابل پردازش نباشد، تحت عنوان ظرفیت امن شناخته می‌شود. در ابتدا دستیابی به ظرفیت امن مثبت تنها با فرض نازل بودن کانال شنودکننده امکان داشت. همچنین مدل کانال شنود برای گیرنده‌های مجاز و غیرمجاز نامتقارن بود. سپس طرح کانال شنود به مدل کانال پخش با پیام محرمانه تعمیم داده شد. با طرح کانال گفتگوی همگانی برای ارتباط بین فرستنده و گیرنده‌مجاز نشان داده شد که ظرفیت امن در حالتی که کانال دشمن کاراتر باشد، اکیدا مثبت خواهد شد. در این مقاله مدل کلی‌تری از کانال‌های ارتباطی بین فرستنده و گیرنده‌مجاز به صورت دوطرفه در نظر گرفته می‌شود که از مدل‌های قبلی مطرح شده عملی‌تر است. همچنین نشان داده می‌شود که n-تعامل پشت سرهم هیچ مزیتی بر تعامل اول ندارد، در ضمن شرط جدیدی برای لزوم ظرفیت امن مثبت بدست خواهد آمد.

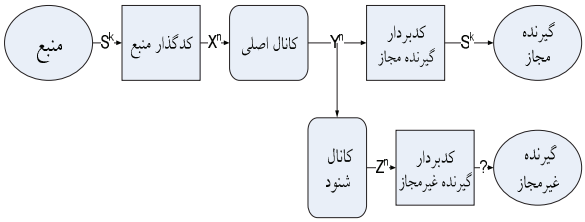
واژه‌های کلیدی

امنیت تئوری اطلاعاتی، کانال شنود دوطرفه متقارن، ظرفیت امن کانال، کانال گفتگوی همگانی، کانال پخش با پیام محرمانه.

۱- مقدمه

یکی از زمینه‌های جدید در تئوری اطلاعات ظرفیت امن کانال‌های شنود (Secrecy Capacity of Wiretap Channels) است. بطور کلی میزان اطلاعات پیامی که فرستنده قادر است مخابره کند، تا بطور امن بدست گیرنده مجاز برسد و گیرنده غیرمجاز هیچ اطلاعی از آن بدست نیاورد، به عنوان ظرفیت امن کانال شنود شناخته می‌شود. اول بار مدل کانال شنود بدون‌حافظه گسسته (Discrete Memoryless) توسط Wyner مطرح شد [۱] که در آن شنودکننده قادر نبود پیامی را کدبرداری کند.

مدل کانال شنود گسسته بدون حافظه Wyner در شکل ۱ نشان داده شده است. پیام S^k بعد از عمل کدگذاری به X^n تبدیل می‌شود، که با عبور از کانال اصلی Y^n به گیرنده مجاز خواهد رسید و Y^n با عبور از کانال شنود بصورت Z^n به گیرنده غیرمجاز می‌رسد. تابع احتمال شرطی کانال معادل شنودکننده به صورت $P(Z^n|X^n)=P(Z^n|Y^n).P(Y^n|X^n)$ خواهد بود.



شکل ۱ : مدل کانال شنود بدون حافظه گسسته Wyner

شنودکننده در مدل کانال شنود Wyner به اطلاعاتی که از کانال اصلی و کانال شنود (در شکل۱) عبور می‌کند یا همان Z^n، دسترسی دارد یا کانال معادل شنودکننده، ترکیب کانال اصلی و کانال شنود است که این کانال معادل یک نسخه نازل از کانال اصلی است. در اینجا فرض شده است که شنودکننده اطلاعات را کمی نویزی‌تر دریافت می‌کند. فرق کانال فوق با کانال پخش نازل [۲] در این است که در اینجا بایستی اطلاعات بدست آمده توسط شنودکننده کمینه شود و درعوض اطلاعات دریافتی گیرنده مجاز بیشینه شود.

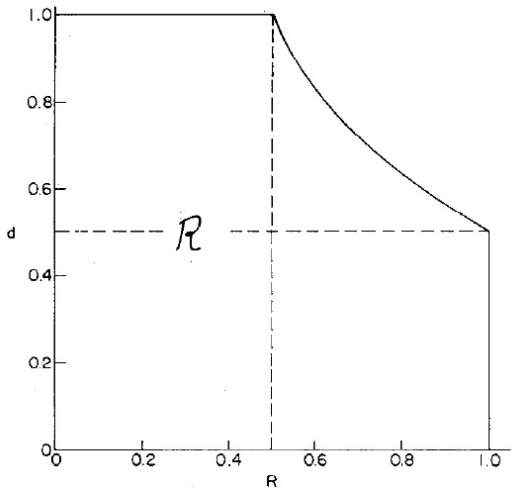
با توجه به مدل شکل ۱، اگر بردارهای S^k، X^n، Y^n و Z^n بردارهای باینری بترتیب با طول‌های k، n، n و n در نظر گرفته شوند. اگر کانال اصلی کانال باینری بدون نویز باشد و کانال شنود کانال باینری متقارن حاوی نویز با نرخ خطای بیت $p>0$ باشد. در واقع می‌توان $Y=X$ و $Z=X+e$ فرض کرد. میزان ابهام گیرنده غیرمجاز $H(S|Z)$ است. یک جفت (R,d) قابل حصول تعریف می‌شود [۱]، اگر برای تمام $\varepsilon > 0$ به دلخواه کوچک کدگذار-کدبردار با پارامترهای n و k موجود باشد که:

$$R - \varepsilon \le \frac{k}{n}, \qquad d - \varepsilon \le \frac{H(S|Z)}{k}, \qquad P_e \le \varepsilon \qquad (۱)$$

که Pe همان نرخ خطای کدبرداری بیت توسط گیرنده مجاز است. آقای Wyner از یک کدگذاری تصادفی ولی معکوس‌پذیر برای گیج‌کردن دشمن استفاده کرد و در این حالت خاص نشان داد که جفت (R,d) قابل حصول است، اگر و تنها اگر رابطه زیر برقرار باشد:

$$h(p) = -p.\log(p) - (1-p).\log(1-p)$$
$$Rd \le h(p); 0 \le R \le 1, 0 \le d \le 1 \qquad (۲)$$

ناحیه قابل حصول جفت نرخ (R,d) برای h(p)=0.5 در شکل۲ رسم شده است. توجه کنید که در اینجا ناحیه ظرفیت مقعر نیست بلکه محدب است. تسهیم زمانی (Time-Sharing) بین گیرنده مجاز و گیرنده غیرمجاز بصورت تابع هموگرافیک (R.d=cte) است، یعنی اگر $R_1.d_1=R_2.d_2=cte$ باشد، آنگاه R بین R_1 و R_2 همچنین d بین d_1 و d_2 یافت می‌شود که R.d=cte باشد. جفت نرخ قابل حصول (R,d) برای کانال شنود بدون‌حافظه گسسته توسط Wyner در حالت کلی بدست آمد و نشان داده شد که در اکثر موارد ظرفیت امن $C_s>0$ وجود دارد، وقتی که جفت نرخ $(R,d)=(C_s,1)$ قابل حصول باشد.

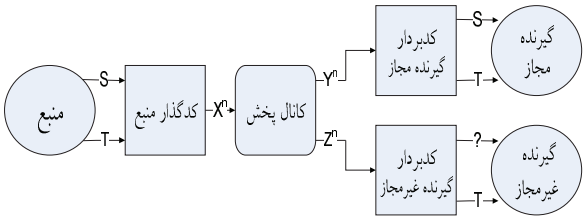


شکل ۲ : ناحیه ظرفیت کانال شنود باینری با h(p)=0.5 [۳]

بر این اساس در بخش بعد کانال پخش با پیام محرمانه بیان می‌شود و در ادامه ظرفیت امن کانال شنود با گفتگوی همگانی بدست می‌آید. با توجه به مقدمات ذکر شده در بخش چهارم تحلیل ظرفیت امن گفته شده تحلیل می‌شود و ظرفیت مدل کلی کانال شنود باینری با گفتگوی همگانی بدست آمده و شرط داشتن ظرفیت امن مثبت استنتاج می‌شود.

۲- کانال پخش با پیام محرمانه

فرض نازل بودن کانال شنودکننده در مدل پیشنهادی توسط Wyner در بسیاری از موارد نقض می‌شود، لذا مدل کانال شنود Wyner به مدل عمومی‌تر کانال‌های پخش دلخواه با پیام محرمانه [۴] توسط Csiszar و Korner توسیع داده شد. ماتریس انتقال کانال در این حالت به صورت $P(Y^n,Z^n|X^n)$ خواهد بود. مدل کانال پخش با پیام محرمانه در شکل۳ به همراه مقادیر خروجی مشخص شده است.



شکل ۳ : مدل کانال پخش با پیام محرمانه

در مدل شکل۳، پیام $s \in S$ پیام خصوصی است که باید تنها به دست گیرنده مجاز برسد و پیام $t \in T$ پیام عمومی است که هر دو گیرنده آن را دریافت می‌کنند. گیرنده مجاز Y^n و گیرنده غیرمجاز Z^n را بدست می‌آورد. هدف طراحی نگاشت کدگذار $f: S*T \to X^n$ و جفت نگاشت کدبردار $g: Y^n \to S*T$ و $h: Z^n \to T$ است، بطوریکه پیام خصوصی بطور مجزا توسط گیرنده مجاز بازیابی شود و پیام عمومی توسط هر دو گیرنده دریافت شود.

برای ایجاد امنیت بیشتر توصیه می‌شود که از نگاشت کدگذار تصادفی بجای کدگذار معین استفاده شود. کدگذار تصادفی f با طول بلوک n-بیتی برای مدل شکل۳ با ماتریس احتمالات شرطی $f(x^n|s,t)$ مشخص می‌شود که $\sum_{x^n} f(x^n|s,t) = 1$ است و $f(x^n|s,t)$ احتمال کدگذاری (s,t) بصورت x^n به عنوان ورودی کانال پخش است. حال برای هر $s \in S$ ، $t \in T$ و $\varepsilon > 0$ به دلخواه کوچک، احتمال خطا برای هر کدبردار بر روی نگاشت کدگذار تصادفی و توزیع احتمال انتقال کانال بصورت زیر تعریف می‌شود:

$$\sum_{x^n \in X^n} f(x^n|s,t).P^n_{Y|X}(g(y^n) \ne (s,t)|x^n) \le \varepsilon$$
$$\sum_{x^n \in X^n} f(x^n|s,t).P^n_{Z|X}(h(z^n) \ne t\,|x^n) \le \varepsilon \qquad (۳)$$

در نتیجه سه‌تایی (f,g,h) سبب می‌شود که ارسال-(n,ε) بر روی کانال پخش با پیام محرمانه انجام شود. بعلاوه نرخ سه‌تایی (R_1,R_e,R_0) برای کانال فوق قابل حصول است، اگر و تنها اگر دنباله‌ای از مجموعه‌های پیام‌های S_n و T_n و دنباله‌ای از سه‌تایی-

های کدگذار-کدبردار (f_n,g_n,h_n)، ارسال-(n,ε_n) را نتیجه می‌دهد، چنانچه روابط زیر برقرار باشد: $(\varepsilon_n \to 0)$

$$\lim_{n\to\infty}\frac{1}{n}\log\|S_n\| = R_1$$
$$\lim_{n\to\infty}\frac{1}{n}\log\|T_n\| = R_0 \qquad (۴)$$
$$\lim_{n\to\infty}\frac{1}{n}H(S^n|Z^n) \geq R_e$$

که R_1 نرخ پیام خصوصی، R_0 نرخ پیام مشترک و R_e نرخ ابهام دشمن در مورد پیام خصوصی را نشان می‌دهد. بدون کاسته شدن از کلیت مساله در اینجا فرض شده است که جفت پیام‌ها به صورت یکنواخت انتخاب و ارسال می‌شوند. قضیه۱ در زیر نتیجه اصلی [۴] است که ناحیه ظرفیت کانال پخش با پیام محرمانه را بیان می‌کند.

قضیه۱: ناحیه ظرفیت R مجموعه بسته مقعر شامل تمام سه‌تایی-های مرتب (R_1,R_e,R_0) است که برای آن‌ها متغیرهای کمکی U و V با زنجیره مارکف $U \leftrightarrow V \leftrightarrow X \leftrightarrow (Y,Z)$ وجود دارد (X، Y و Z مربوط به مدل شکل۳) که در روابط زیر صدق می‌کنند: (اثبات در [۴])

$$0 \leq R_e \leq R_1 \,,\ \|U\| \leq \|X\| + 3 \,,\ \|V\| \leq \|X\|^2 + 4\|X\| + 3$$
$$R_e \leq I(V;Y|U) - I(V;Z|U) = H(V|Z,U) - H(V|Y,U) \qquad (۵)$$
$$R_1 + R_0 \leq I(V;Y|U) + \min\{I(U;Y), I(U;Z)\}$$
$$0 \leq R_0 \leq \min\{I(U;Y), I(U;Z)\}$$

اگر میزان ابهام در مورد S^n بعد از مشاهده Z^n برابر نرخ ابهام $H(S|T)$ باشد، پیام S با امنیت کامل (Perfect Secrecy) مخابره می‌شود. اگر پیام مشترکی ارسال نشود، $R_0=0$ خواهد بود و ناحیه نرخ قابل حصول به صورت خلاصه‌تر $R_{1e} = \{(R_1,R_e): (R_1,R_e,0) \in R\}$ درمی‌آید. ظرفیت امن بیشترین نرخ ارسال پیام به گیرنده مجاز با امنیت کامل بصورت $C_s = \max_{(R_1,R_1)\in R_{1e}} R_1$ تعریف می‌شود. توجه کنید که ماکزیمم‌گیری R_1 روی جفت نرخ (R_1,R_e) است که در آن‌ها $R_e=R_1$ است، که این شرط امنیت کامل را ارضا می‌کند. همچنان که Wyner نشان داد، امکان مخابره با امنیت کامل در صورت نازل‌بودن کانال معادل شنودکننده وجود دارد. در نتیجه۱ مدل کانال پخش با پیام محرمانه [۴] نشان داده شده است که چنانچه کانال دشمن از کانال گیرنده مجاز نویزی‌تر باشد (I(X;Y)>I(X;Z))، ظرفیت امن مقداری مثبت خواهد بود.

نتیجه۱: برای جفت نرخ $(R_1,R_e) \in R_{1e}$ اگر و تنها اگر متغیرهای تصادفی کمکی U و V با زنجیره مارکف به صورت $U \leftrightarrow V \leftrightarrow X \leftrightarrow (Y,Z)$ وجود داشته باشند که:

$$I(U;Y) \leq I(U;Z) \quad , \quad 0 \leq R_e \leq I(V;Y|U) - I(V;Z|U)$$

در اینصورت ظرفیت امن در حالت کلی برابر خواهد بود با:

$$C_s = \max_{V\leftrightarrow X\leftrightarrow(Y,Z)} [I(V;Y) - I(V;Z)] \qquad (۶)$$

و اگر کانال اول از کانال دوم کاراتر باشد یعنی $I(X;Y) \geq I(X;Z)$، در اینصورت ظرفیت امن به صورت $C_S = \max[I(X;Y) - I(X;Z)]$ ساده می‌شود.

۳- ظرفیت امن کانال پخش با گفتگوی همگانی

در بخش‌های قبلی با فرض اینکه دشمن پیام فرستنده را از کانال نویزی‌تر دریافت کند، ظرفیت امن مثبت خواهد شد. در این بخش نشان داده می‌شود که فرض فوق لزومی ندارد و فرستنده و گیرنده مجاز می‌توانند با وجود کانال ارتباطی نویزی‌تر با کمک کانال گفتگوی همگانی بدون نویز (Noiseless Public Discussion Channel) به ظرفیت امن مثبت دست یابند. اگر در مدل شکل۳ کانال پخش، باینری متقارن در نظر گرفته شود و احتمالات شرطی به صورت $P_{Y|X}(y=x|x)=1-a$ و $P_{Z|X}(z=x|x)=1-b$ باشد، باتوجه به تعاریف و قضایای بخش قبلی می‌توان ظرفیت امن کانال پخش باینری را به صورت $C_s\big(D(a,b)\big) = [h(a) - h(b)]^+$ بدست آورد. در نتیجه اگر a>b باشد ظرفیت امن صفر خواهد شد. در این حالت Maurer در [۵] پیشنهاد می‌کند که فرستنده و گیرنده مجاز از طریق یک کانال عمومی بدون نویز گفتگو کنند. مهاجم قادر است که تمام مکالمات فرستنده و گیرنده مجاز بر روی کانال گفتگوی همگانی را شنود کند.

پیشنهاد Maurer برای حالت کانال پخش باینری متقارن این است که برای مثال فرستنده X را روی کانال پخش بفرستد و گیرنده مجاز Y=X+A را دریافت کند که P(A=1)=a و گیرنده غیرمجاز Z=X+B را دریافت کند که P(B=1)=b است. حال گیرنده مجاز سمبل اطلاعات مخفی V را تولید می‌کند و W=V+Y را از طریق کانال گفتگوی همگانی بدون نویز ($P_{Y|X}(y=x|x)=1$) برای فرستنده می‌فرستد. در این صورت دشمن مقدار Z و W را در اختیار خواهد داشت. فرستنده با محاسبه W+X=V+A قادر است V را با احتمال 1-a بدست می‌آورد. ولی دشمن برای بدست آوردن V تنها W+Z=V+A+B را دراختیار دارد و در نتیجه با احتمال a(1-b)+b(1-a) می‌تواند V را محاسبه کند. در این حالت ظرفیت امن کانال پخش باینری متقارن با گفتگوی همگانی برابربا رابطه۷ است. در اینجا ظرفیت امن اکیدا مثبت است مگر در حالات خاص a=0.5، b=0 و b=1 که صفر می-شود.

$$\hat{C}_s\big(D(a,b)\big) = h(a+b-2ab) - h(a) \qquad (۷)$$

توجه کنید که در پایان انجام پروتکل مطرح شده، فرستنده و گیرنده مجاز می‌توانند مشترکا قسمتی از متغیر V را به طور امن به عنوان کلید مخفی مشترک تسهیم کنند. اگر مراحل مختلف پروتکل به صورت $C_1,C_2,\ldots,C_n$ نمایانده شود. فرستنده کلید S

اشتراکی را از روی $C^n=(C_1,C_2,\dots,C_n)$ و X محاسبه می‌کند و گیرنده مجاز کلید S' را از روی C^n و Y بدست می‌آورد.

قضیه۲: برای پروتکل توافق کلیدی که در روابط زیر صدق می‌کند

$$H(C_i|C^{i-1},X)=0$$
$$H(C_i|C^{i-1},Y)=0$$
$$H(S|C^{n-1},X)=0$$
$$H(S'|C^{n-1},Y)=0$$
$$P(S\neq S')\leq \varepsilon, I(S;C^n,Z)\leq \delta$$

به ازای ε و δ کوچک داریم: (اثبات در [۵])

$$\begin{aligned} H(S) &\leq I(X;Y|Z)+H(S|S')+I(S;C^n,Z)\\ H(S) &\leq \min[I(X;Y),I(X;Y|Z)]+\delta+h(\varepsilon)\\ &\quad +\varepsilon.\log_2(|S|-1)\end{aligned} \qquad (۸)$$

نرخ کلید مخفی X و Y با توجه به Z بصورت $S(X;Y||Z)$ نمایش داده می‌شود و برابر بیشترین نرخ ممکن است که فرستنده و گیرنده‌مجاز قادرند بر روی کلید مخفی S توافق کنند بطوریکه نرخ بدست آمده توسط دشمن به اندازه کافی کوچک باشد.

قضیه۳: نرخ کلید مخفی X و Y با توجه به Z به صورت زیر محدود می‌شود: (اثبات در [۵])

$$\begin{aligned}\max\,[I(Y;X)-I(Z;X),I(X;Y)-I(Z;Y)]&\\ \leq S(X;Y||Z)&\\ \leq \min\,[I(X;Y),I(X;Y|Z)]&\end{aligned} \qquad (۹)$$

باند پایینی نرخ کلید مخفی بطور کلی باند باریکی (tight) نیست یعنی سناریوهایی وجود دارد تعامل فرستنده و گیرنده‌مجاز (ارتباط دوطرفه) برای بدست آمدن ظرفیت امن نامنفی لازم است. درعوض باند بالایی اگر $P_{XZ|Y}=P_{X|Y}.P_{Z|Y}$ یا $P_{YZ|X}=P_{Y|X}.P_{Z|X}$ باشد، کاملا باریک است.

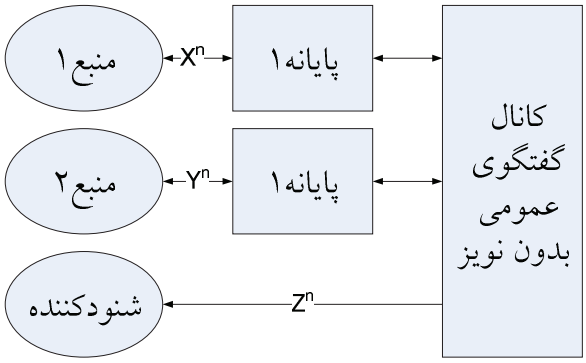
قضیه۴: ظرفیت امن با کانال پخش حاوی گفتگوی همگانی ($P_{YZ|X}$) بصورت زیر محدود می‌شود: [۵]

$$\begin{aligned}\max_{P_X} S(X;Y||Z)&\leq \hat{C}_s(P_{YZ|X})\\ &\leq \min\,[\max_{P_X} I(X;Y),\max_{P_X} I(X;Y|Z)]\end{aligned} \qquad (۱۰)$$

نرخ کلید مخفی برای حالت متغیرهای باینری اکیدا مثبت است. همچنین تعامل بین فرستنده و گیرنده‌مجاز از ارتباط یکطرفه بین فرستنده و گیرنده‌مجاز قوی‌تر است. در نتیجه با استفاده از کانال پخش گفتگوی همگانی همواره ظرفیت امن اکیدا مثبت خواهیم داشت.

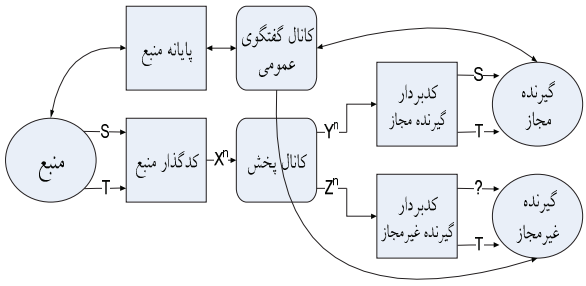
۴- تحلیل ظرفیت امن کانال شنود دوطرفه متقارن

مدل بیان شده در بخش قبل را به مدل نوع-منبع با شنودکننده و نوع-کانال با شنودکننده توسط Ahlswede و Csiszar [۶] تعمیم داده شد. همانطور که در شکل۴ نمایش داده شده است، در حالت منبع یک مدل منبع چندگانه بدون حافظه گسسته (Discrete Memoryless Multiple Source) با سه منبع و متغیرهای عمومی (X,Y,Z) در نظر گرفتند که خروجی‌های X^n، Y^n و Z^n را منبع۱، منبع۲ و شنودکننده به ترتیب می‌بینند.



شکل ۴: مدل نوع -منبع با شنودکننده

مدل نوع-کانال با شنودکننده مشابه مدل Maurer [۵] است. مدل کانال (شکل۵) از یک کانال بدون حافظه گسسته استفاده می‌کند که منبع سمبل X^n را تولید می‌کند و گیرنده مجاز Y^n و گیرنده غیرمجاز Z^n را دریافت می‌کند و فرستنده و گیرنده مجاز از یک کانال گفتگوی همگانی برای ارتباط پایانه‌های خود بهره می‌گیرند. نتایج تحلیل دو مدل فوق در [۶] آمده است. همچنین تعمیم مدل نوع-منبع به حالت n-منبع و شنودکننده توسط Csiszar و Narayan [۷] انجام شده است.



شکل ۵: مدل نوع کانال با شنودکننده

تعریف۱: کانال باینری با پارامتر a از متغیر تصادفی باینری X به Y ($X \xrightarrow{a} Y$) تعریف می‌شود، بطوریکه احتمالات شرطی آن P(y=x|x)=1-a و P(y=x+1|x)=a به ازای x=0,1 باشد. (بدون کاسته شدن از کلیت فرض می‌شود که a<0.5 است.)

تعریف۲: عملگر * برای احتمال‌های جزئی a و b را بصورت زیر تعریف می‌کنیم:

$$a*b=b*a=a.(1-b)+b.(1-a)$$

لم۱: اگر a و b احتمالات جزئی دلخواه باشند، بطوریکه 0<b<a<0.5 داریم:

$$0<b<a<a*b<a*a<0.5$$
$$0<b*b<a*b<0.5$$

لم۲: اگر a و b احتمالات جزئی دلخواه باشند، بطوریکه 0<b<a<0.5 داریم:

$$0 < h(b) < h(a) < h(a*b) < h(a*a) < 1$$
$$0 < h(b*b) < h(a*b) < 1$$

لم۳: اگر a و b و c احتمالات جزئی دلخواه باشند، بطوریکه 0<a,b,c<0.5 داریم:

$$|a*a-b*b| < |a-b|$$
$$|a*c-b*c| < |a-b|$$

لم۴: اگر a و b و c احتمالات جزئی دلخواه باشند، بطوریکه 0<a,b,c<0.5 داریم:

$$|h(a*a)-h(b*b)| < |h(a)-h(b)|$$
$$|h(a*c)-h(b*c)| < |h(a)-h(b)|$$

اثبات ۱و۲و۳و۴: به دلیل کمبود صفحات از اثبات ساده جبری لم-ها صرف‌نظر می‌شود!

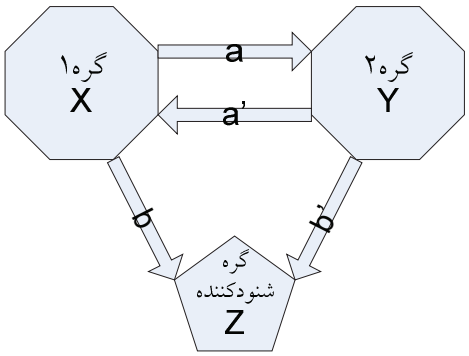
اگر تعاملات بین فرستنده و گیرنده مجاز در مدل نوع کانال با شنودکننده (شکل۵) به تعداد n-بار تکرار شود، نشان می‌دهیم که بهبودی در میزان ظرفیت امن حاصل نمی‌شود. با توجه به فرضیات بخش۳ در مورد کانال پخش باینری، چنانچه در مرحله دوم پروتکل توافق کلید، فرستنده مقدار V+A را بهمراه Xی جدید روی کانال پخش بفرستد. گیرنده مجاز $X+V+A_1+A_2$ را دریافت خواهد کرد که $A_1=A$ است. در نتیجه گیرنده مجاز قادر است که با داشتن V (خودش تولید کرده) مقدار $X+A_1+A_2$ را محاسبه کند. گیرنده غیرمجاز هم با داشتن مقدار $V+A_1+B_1$ (که $B_1=B$) می‌تواند $X+B_1+B_2$ را بدست آورد. با n بار تکرار تعامل، به استقراء براحتی می‌توان دید که گیرنده مجاز $X+\sum_{i=1}^{n} A_i$ و گیرنده غیرمجاز $X+\sum_{i=1}^{n} B_i$ را دریافت خواهد کرد. حال اگر گیرنده مجاز مقدار تصادفی جدید V تولید کرده و $V+X+\sum_{i=1}^{n} A_i$ را برای فرستنده ارسال کند. مقدار ظرفیت امن یا نرخ کلید مخفی توافقی از رابطه۷ بدست می‌آید.

قضیه۵: افزایش تعاملات پروتکل فوق الذکر مقدار ظرفیت امن یا نرخ کلید مخفی توافقی را افزایش نمی‌دهد یا به عبارت دیگر به ازای m<n داریم:

$$\hat{C}_s^m(D(a,b)) < \hat{C}_s^n(D(a,b))$$
$$\hat{C}_s^i(D(a,b)) = h\left(*_{k=1}^{i}(a*b)\right) - h(*_{k=1}^{i} a)$$

اثبات: مقدار ظرفیت امن را از رابطه۷ بدست آورده و با کمک لم‌های ۱و۲و۳و۴ نتیجه‌گیری کنید.

حال کانال مورد بحث را مطابق تعریف۱ تعمیم می‌دهیم. در شکل۶ پارامترهای کانال باینری بین گره‌های شبکه مشخص شده است که گره‌های X و Y فرستنده-گیرنده‌هایی هستند که قصد برقراری ارتباط دارند و گره Z شنودکننده کانال ارتباطی دوطرفه بین X و Y است.



شکل ۶: مدل کانال شنود باینری

چنانچه در شکل۶ نشان داده شده، P(X=1)=P(Y=1)=0.5، P(A=1)=a، P(A'=1)=a'، P(B=1)=b و P(B'=1)=b' است. گره۱ مقدار تصادفی X را به سمت گره۲ می‌فرستد. گره۲ مقدار $X+A_1$ و شنودکننده $X+B_1$ را دریافت می‌کند. حال گره۲ مقدار تصادفی Y بهمراه $X+A_1$ را برای گره۱ می‌فرستد. در نتیجه گره۱ مقدار $Y+X+A_1+A_1'$ را دریافت کرده و مقدار $Y+A_1+A_1'$ را محاسبه می‌کند. شنودکننده نیز مقدار $Y+X+A_1+B_1'$ را دریافت می‌کند و مقدار $Y+A_1+B_1+B_1'$ را می‌تواند محاسبه کند. در اینجا نیز براحتی مشابه قضیه۵ می‌توان نشان داد که تعامل بیشتر مقدار ظرفیت امن را افزایش نمی‌دهد. ولی شروع‌کننده تعامل در میزان ظرفیت امن تاثیر دارد.

قضیه۶: ظرفیت امن مدل کانال شنود باینری (شکل۶) برابر است با:

$$C_s = \max\left[h(a*b*b') - h(a*a'),\ h(a'*b*b') - h(a*a')\right]$$

اثبات: با کمک رابطه۷ و تعمیم قضیه۵ با توجه به شروع کننده تعامل ظرفیت امن نتیجه می‌شود.

نتیجه۲: شرط مثبت بودن ظرفیت امن مدل کانال شنود باینری (شکل۶) برابر است با:

$$min[a,a'] < b*b'$$

اثبات: بلافاصله از قضیه۶ نتیجه می‌شود.

روابط بیان شده در این بخش را می‌توان براحتی به حالت کانال شنود بدون حافظه گسسته تعمیم داد. تنها کافیست که بجای احتمال جزئی بردار احتمالات جزئی درنظرگرفته شود و عملگر ▮ تبدیل به عملگر کانولوشن خطی بردارها می‌شود و یا می‌توان ماتریس گردشی احتمالات جزئی را تشکیل داد و عملگر ▮ معادل ضرب ماتریس‌گردشی متناظر با بردار احتمالات جزئی می‌شود. در اینصورت لم‌های ۱و۲و۳و۴ برای بردارهای احتمالات جزئی برقرار خواهد بود و همچنین قضایای مشابه قضیه ۵و۶

بدست می‌آید. تنها نکته باقیمانده این است که در حالت کانال شنود بدون‌حافظه گسسته نامتقارن مقادیر ویژه ماتریس گردشی معادل مختلط می‌شود. مقادیر ویژه ماتریس گردشی را می‌توان متناظر با ماتریس کوواریانس یک کانال گوسی درنظر گرفت، لذا ادعای زیر را می‌توان بیان کرد.

۶- نتیجه‌گیری

مدل کانال شنود Wyner با فرض نازل بودن کانال شنودکننده به ظرفیت امن مثبت می‌رسید که این فرض چندان عملی نیست. مدل کانال پخش با پیام محرمانه تعمیم مناسبی از کانال شنود Wyner است و ناحیه ظرفیت کانال برای نرخ پیام خصوصی و عمومی توسط Csiszar و Korner بدست آمد. اما تنها در حالتی که کانال دشمن نویزی‌تر باشد می‌توان انتظار داشت که نرخ پیام خصوصی مثبت شود. برای حل این مشکل Maurer استفاده از کانال گفتگوی همگانی بدون‌نویز (ولی قابل شنود) را پیشنهاد کرده است. با استفاده از پروتکل توافق کلید خصوصی می‌توان همواره نرخ کلید خصوصی یا ظرفیت امن اکیدا مثبت داشت. وجود کانال گفتگوی همگانی بدون نویز همواره در عمل امکان‌پذیر نیست، لذا در این مقاله به بررسی کانال شنود دوطرفه متقارن پرداخته شد. با استفاده از لم‌های مربوط به ترکیب کانال‌های گسسته در قضیه‌ای نشان داده شد که افزایش تعداد تعاملات پروتکل توافق کلید خصوصی بین گره‌های شبکه لزوما باعث افزایش ظرفیت امن نمی‌شود. همچنین در حالت کانال بدون‌حافظه گسسته متقارن مشابه حالت باینری با برقراری شرط بدست آمده در قضیه آخر ظرفیت امن مثبت خواهد بود. تعمیم حالت گسسته به گوسی نیز ادعایی است که به عنوان پژوهش آتی پیشنهاد می‌شود.

۷- سپاس‌گزاری

نویسنده این مقاله لازم می‌دانند تا از همکاری استاد ارجمند جناب آقای دکتر محمدرضا عارف به خاطر مشاوره دلسوزانه ایشان سپاسگزاری کنند.

مراجع

[1] A. D. Wyner, "The Wiretap Channel", Bell System Technical Journal, 54(8):1355-1387, October 1975.
[2] J. Korner and K. Marton, "General Broadcast Channels with Degraded Message Sets", IEEE Transactions on Information Theory, Vol. IT-23, No. 1, pp. 60-64, 1977.
[3] A. B. Carleial and M. E. Hellman, "A Note on Wyner's Wiretap Channel", IEEE Transactions on Information Theory, May 1977.
[4] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages", IEEE Transactions on Information Theory, 24(3):339-348, May 1978.
[5] U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE Transactions on Information Theory, vol. 39, pp. 733–742, May 1993.
[6] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography, part I: Secret sharing," IEEE Transactions on Information Theory, vol. 39, pp. 1121–1132, July 1993.
[7] I. Csiszar and P. Narayan, "Secrecy Capacities for Multiple Terminals", IEEE Transactions on Information Theory, Vol. 50, No. 12, December 2004.