نشریه علمی «پدافند الکترونیکی و سایبری»
سال هشتم، شماره ۲، تابستان ۱۳۹۹؛ ص ۴۹-۳۵

علمی–پژوهشی

توافق کلید امن مبتنی بر مکان‌یابی نسبی بر پایه تئوری اطلاعات

نرگس کاظم‌پور[۱]، مهتاب میرمحسنی[۲*]، محمدرضا عارف[۳]

۱- دانشجوی دکتری، ۲- استادیار، ۳- استاد، آزمایشگاه تئوری اطلاعات و مخابرات امن، دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران

(دریافت: ۹۸/۳/۵، پذیرش: ۹۸/۷/۱۰)

چکیده

اشتراک‌گذاری کلید امن یک پیش‌نیاز ضروری در رمزنگاری کلید متقارن است و یکی از راه‌های اشتراک آن، توافق بر کلیدی امن می‌باشد. در این مقاله، به بررسی توافق کلید بر پایه نظریه اطلاعات با مدل منبع، مبتنی بر فاصله بین گره‌های مجاز می‌پردازیم. توافق کلید امن بر پایه نظریه اطلاعات، بر خلاف مدل‌های مبتنی بر پیچیدگی محاسباتی، امنیت کامل را تضمین می‌کند، یعنی هیچ اطلاعات مؤثری به شنودگر نمی‌رسد. مدل مورد بررسی در این مقاله، سامانه پایه‌ای شامل دو کاربر مجاز و یک شنودگر است. گره‌های مجاز تلاش می‌کنند تا با استفاده از مشاهدات (همراه با خطای) خود از فاصله‌شان، بر کلیدی امن و قابل اطمینان توافق کنند. شنودگر نیز مشاهداتی از این فاصله دارد. از آن‌جا که فاصله بین گره‌ها تحت کنترل هیچ یک از آن‌ها نیست، مدل توافق کلید، مدل منبع است. ابتدا تخمین فاصله توسط گره‌ها را مدل‌سازی می‌کنیم تا بتوان عملکرد سامانه (کران‌های ظرفیت کلید امن) را بررسی کرد. خطای تخمین فاصله با یک فرآیند گوسی با میانگین صفر و واریانسی برابر کران کرامر-رائو مدل می‌شود. دو روش را برای بهبود عملکرد سامانه پیشنهاد می‌دهیم: ۱) گسیل نویز مصنوعی، ۲) ارسال سیگنال در جهت‌های مختلف (ارسال چند آنتنی). در روش اول نویز مصنوعی برای خراب کردن تخمین شنودگر از فاصله استفاده می‌شود و در روش دوم سیگنال‌های راهنما در جهت‌های تصادفی مختلف ارسال می‌گردند و فاصله‌های مجازی، که معادل فاصله‌ای است که سیگنال راهنما طی کرده، به عنوان منابع تصادفی برای تولید کلید استفاده می‌شوند. ما نشان می‌دهیم که اگر شنودگر مجهز به آرایه آنتن نباشد، آن‌گاه استفاده از گسیل نویز مصنوعی روش مفیدی است و اگر شنودگر مجهز به آرایه آنتن باشد، روش گسیل نویز مصنوعی اطلاعات بیشتری به شنودگر نشت می‌دهد، در نتیجه روش مؤثری در این شرایط نیست. هنگامی که گره‌ها مجهز به آرایه آنتن هستند، ارسال در جهت‌های تصادفی مختلف روش مناسبی برای افزایش نرخ کلید امن می‌باشد، چراکه شنودگر اطلاعات کمی در مورد فاصله‌های مجازی به‌دست می‌آورد و اغلب مشاهدات گره‌های مجاز و شنودگر مستقل از یکدیگر هستند.

کلیدواژه‌ها: توافق کلید امن، مکان‌یابی، امنیت نظریه اطلاعاتی، گسیل نویز مصنوعی، ظرفیت کلید امن

۱- مقدمه

امروزه استفاده از شبکه‌های بی‌سیم افزایش یافته است، از تلفن همراه، رایانه، تبلت تا کاربردهای پزشکی، نظامی، ورزشی و .... به دلیل رشد روزافزون شبکه‌های بی‌سیم و ماهیت پخشی این شبکه‌ها، تأمین امنیت به مسأله چالش‌برانگیزی تبدیل شده است. به‌کارگیری قراردادهای[1] امنیتی بر پایه پیچیدگی محاسباتی پرکاربردترین روش در تأمین امنیت می‌باشد. به این معنی که پیچیدگی آن‌ها از مرتبه چندجمله‌ای نمی‌باشد و به همین دلیل شکستن امنیت آن‌ها با پردازش‌گرها و ابزارهایی که اکنون در دسترس است امکان‌پذیر نمی‌باشد. اما با پیشرفت روزافزون فناوری امکان شکسته شدن این روش‌ها وجود دارد، به همین دلیل توجه به مفاهیم نظریه اطلاعاتی در حال گسترش است [۱].

شانون در سال ۱۹۴۸ مفهوم نظریه اطلاعات را معرفی کرده [۲] و سپس یک سال بعد در [۳] امنیت از دیدگاه نظریه اطلاعات را بررسی می‌کند. پس از شانون افراد بسیاری بر روی امنیت از دیدگاه نظریه اطلاعات کار کردند و مفاهیم آن را گسترش دادند [۵-۴]. امنیت از دیدگاه نظریه اطلاعات را می‌توان به دو مسأله انتقال پیام امن و توافق کلید امن تقسیم کرد. در مسأله انتقال پیام امن، هدف ارسال قابل اطمینان پیام به گیرنده‌های مجاز است، به گونه‌ای که شنودگر نتواند به اطلاعات پیام دست یابد. در مسأله توافق کلید امن گره‌های مجاز با استفاده از مشاهدات خود از منبعی تصادفی، بر روی کلیدی امن توافق می‌کنند که از شنودگر مخفی است.

*رایانامه نویسنده پاسخگو: mirmohseni@sharif.edu

[1] Protocol

قراردادهای امنیتی مبتنی بر رمزنگاری کلید مخفی به کلیدی امن که از قبل بین طرفین به اشتراک گذاشته شده باشد، برای رمزگذاری داده‌ها نیاز دارند. روش‌های بسیاری از جمله تولید کلید دیفی-هلمن [۶-۷] بر پایه پیچیدگی محاسباتی کلید را به اشتراک می‌گذارند. روش دیگر تولید کلید، توافق کلید بر پایه نظریه اطلاعات می‌باشد که در لایه فیزیکی صورت می‌گیرد. توافق کلید بر پایه نظریه اطلاعات برخلاف مدل‌های محاسباتی به کلیدی از پیش به اشتراک گذاشته شده و یا زیرساخت کلید همگانی[1] نیاز ندارد و امنیت آن اثبات‌پذیر است (ایجاد امنیت در لایه فیزیکی با استفاده از داده‌های تصادفی صورت می‌پذیرد، یعنی از این داده‌های تصادفی به گونه‌ای استفاده می‌شود که هم اطلاعات موردنظر به درستی به گره‌های مجاز برسد و هم شنودگر به اطلاعات مفیدی دسترسی پیدا نکند). توافق کلید امن در دو مدل منبع و کانال در [۵ و ۸] معرفی شد، که نشان داده می‌شود اگر گره‌های مجاز مشاهدات همبسته‌ای از منبع تصادفی داشته باشند می‌توانند بر کلیدی امن توافق کنند، به گونه‌ای که این کلید از شنودگر مخفی بماند. نویسندگان [۵ و ۸] کران‌هایی برای ظرفیت کلید امن به‌دست آورده‌اند اما کران‌های دیگری نیز برای ظرفیت کلید در شرایط مختلف به‌دست آمده است [۱۰-۹].

از منابع تصادفی مختلفی می‌توان به عنوان منبع مشاهدات همبسته استفاده کرد. از مهم‌ترین این منابع اطلاعات حالت کانال[2] (ضریب کانال) بین گره‌های مجاز می‌باشد که در [۱۱-۱۲] مورد مطالعه قرار گرفته است. توافق کلید با استفاده از اطلاعات حالت کانال بر پایه متقابل بودن[3] کانال است و در بسیاری از موارد به هیچ زیرساخت اضافی نیاز ندارد چرا که اطلاعات حالت کانال به دلیل قرارداد مورد استفاده در دسترس است. البته در بعضی از حالات مانند تغییرات کم در کانال بی‌سیم و یا اطلاعات اضافی در شنودگر (مانند اطلاعات مکان) کلید تولید شده، امن نیست [۱۳]. هم‌چنین پژوهش‌های مختلف به دنبال امن‌تر کردن کلید تولیدشده از اطلاعات حالت کانال و افزایش ظرفیت آن هستند، به‌عنوان مثال [۱۴] از نویز مصنوعی برای تولید کلید کمک گرفته است.

منبع دیگری که می‌تواند در نظر گرفته شود، فاصله بین گره‌های مجاز است (البته برای حفظ امنیت و بالا رفتن نرخ کلید، این منبع تصادفی در شبکه‌هایی که گره‌ها متحرک هستند و پویایی گره‌ها زیاد است، کاربرد دارد). از آن‌جا که فاصله بین دو گره در هر دو گره یکسان است، شرط متقابل بودن برقرار است. اندازه‌گیری فاصله با استفاده از امکانات مختلفی از جمله مادون قرمز، سیگنال‌های نوری، رادار، آنتن‌های بی‌سیم و ابزارهای دیگری صورت می‌پذیرد [۱۵] که می‌توان با توجه به ابزارهای موجود و یا شرایط مورد استفاده از هر یک از این ابزارها استفاده کرد. هم‌چنین زیرساخت و ابزارهای مورد نیاز برای اندازه‌گیری فاصله در بسیاری از شرایط و سامانه‌ها در دسترس است و بسیاری از سامانه‌های بی‌سیم فاصله را اندازه‌گیری می‌کنند. به همین دلیل اندازه‌گیری فاصله بار سخت‌افزاری زیادی بر شبکه نمی‌گذارد. روش‌های مختلفی برای تخمین فاصله وجود دارد [۱۶]، مانند اندازه‌گیری زمان رسیدن سیگنال[4]، اندازه‌گیری تفاوت زمان رسیدن سیگنال[5]، اندازه‌گیری زاویه سیگنال دریافتی[6] و اندازه‌گیری توان سیگنال دریافتی[7]. در این پژوهش به دلیل عمومیت و سهولت محاسبات، تخمین فاصله با استفاده از تخمین زمان رسیدن سیگنال انجام می‌گیرد.

ایده استفاده از اطلاعات مکان به‌عنوان منبع تصادفی برای تولید کلید امن در [۱۷] مطالعه شده است که توافق کلید بین کاربر در حال حرکت و زیرساخت بی‌سیم مورد مطالعه قرار گرفته و منبع تصادفی شناسه ایستگاه پایه‌ای[8] است که کاربر به آن متصل است. ایده استفاده از فاصله به عنوان منبع تصادفی برای توافق کلید امن بر پایه نظریه اطلاعات در [۱۸] بررسی شده است. مدل مورد مطالعه در [۱۸] شامل دو کاربر مجاز متحرک، گره ۱ و گره ۲، و یک شنودگر، e، است. دو گره مجاز تلاش می‌کنند با استفاده از مشاهدات فاصله و مکالمه عمومی بر کلیدی امن توافق کنند. در مدل [۱۸]، کانال عمومی با ظرفیت نامحدود در نظر گرفته شده است و نشان داده شده است که اگر شنودگر اطلاعات زاویه را داشته باشد، یعنی بتواند زاویه سیگنال دریافتی را اندازه بگیرد، آن‌گاه ظرفیت کلید امن متناهی است، یعنی با افزایش توان سیگنال راهنما نمی‌توان ظرفیت کلید امن را افزایش داد. اما، اگر شنودگر اطلاعات زاویه را نداشته باشد، آن‌گاه افزایش نرخ کلید به میزان دلخواه با افزایش توان سیگنال راهنما امکان‌پذیر است. [۱۹] راه‌کارهایی را برای افزایش ظرفیت این مدل پیشنهاد داده است. در این مقاله به این راه‌کارها می‌پردازیم. نویسندگان [۲۰] نتایج [۱۸] را به سامانه‌ای با سه کاربر متحرک گسترش دادند. هر جفت از این کاربرها در تلاش هستند تا بر کلیدی امن بر پایه اطلاعات مکانی توافق کنند، به‌گونه‌ای که از کاربر سوم مخفی بماند. کانال عمومی در دو حالت ظرفیت محدود و ظرفیت نامحدود بررسی شد و کران‌های ظرفیت نرخ کلید امن مطالعه گردید.

[1] Public Key Infrastructure
[2] Channel State Information (CSI)
[3] Reciprocity

[4] Time of arrival
[5] Time difference of arrival
[6] Angle of arrival
[7] Received signal strength
[8] Base station

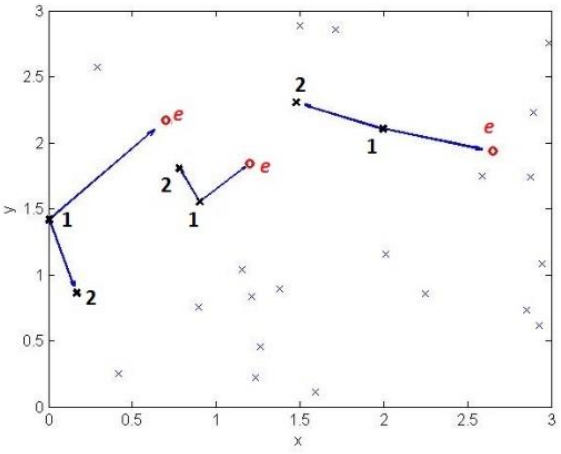
این مقاله نسخه گسترش‌یافته [۱۹] است که به بیان دقیق اثبات‌ها و قضایا می‌پردازد که جزییات اثبات در [۱۹] بیان نشده بود. همچنین، در این نسخه، شبیه‌سازی‌های کامل‌تری انجام می‌شود و بحث و تحلیل در مورد آن‌ها ارایه می‌گردد. با در نظر گرفتن مدل [۱۸]، می‌توان دو مسأله را در نظر گرفت: چگونه ظرفیت کلید را افزایش دهیم و چگونه محدودیت بنیادین که در [۱۸] وجود دارد را حل کنیم (محدود بودن ظرفیت کلید حتی با افزایش توان سیگنال راهنما). این مسأله با در نظر گرفتن دو چالش مهم مدل چالش‌برانگیز است. چالش اول حافظه‌دار بودن سامانه است، چرا که مکان هر گره در هر لحظه به مکانش در لحظات قبل وابسته است و در نتیجه الگوی حرکتش دارای حافظه می‌باشد. چالش دوم نویز وابسته به سیگنال است، یعنی نویز تخمین فاصله به خود فاصله وابسته است. در این پژوهش دو روش جدید برای بالا بردن عملکرد سامانه پیشنهاد شده است: گسیل نویز مصنوعی[1] (ANF) و ارسال سیگنال‌های راهنما در جهت‌های مختلف. روش اول هنگامی مناسب است که گره‌ها، به خصوص شنودگر، آنتن همه‌جهته دارند و روش دوم هنگامی مناسب است که گره‌ها مجهز به آرایه آنتن باشند و امکان ارسال به جهت‌های مختلف را داشته باشند. هدف بررسی تغییرات نرخ کلید امن هنگام استفاده از این روش‌ها است. وقتی گره‌ها مجهز به آنتن همه‌جهته هستند، اثر استفاده از روش ANF بر کران پایین نرخ کلید (برای مشاهدات مستقل و توزیع یکسان[2] و بر کران بالای نرخ کلید بررسی می‌کنیم و نشان می‌دهیم که استفاده از ANF می‌تواند ظرفیت کلید امن را افزایش دهد چرا که تخمین شنودگر از فاصله را خراب می‌کند. شبیه‌سازی نیز نتایج به‌دست‌آمده را تأیید می‌کند. برای حالتی که گره‌ها مجهز به آرایه آنتن باشند، ابتدا تأثیر استفاده از ANF بر عملکرد سامانه مطالعه می‌شود و نشان می‌دهیم که اگر شنودگر از امکاناتش به‌طور مؤثر استفاده کند، استفاده از نویز مصنوعی باعث نشت اطلاعات بیشتری به شنودگر می‌شود. این نتیجه نشان می‌دهد که اگر شنودگر بتواند زاویه همه سیگنال‌های دریافتی را اندازه بگیرد، آن‌گاه ANF روش مؤثری نیست. به همین دلیل معیار جدیدی را با نام بردار فاصله مجازی تعریف می‌کنیم. در این روش هر کدام از گره‌های مجاز، سیگنال‌های راهنما را در جهت‌های مختلف ارسال می‌کنند که برخی از آن‌ها با بازتاب از برخورد با موانع مختلف در محیط به گره مجاز دیگر می‌رسند، فاصله مجازی معادل تمام فاصله‌ای است که سیگنال راهنما طی کرده و بردار فاصله مجازی، برداری شامل فاصله‌های مجازی معادل سیگنال‌های راهنمای مختلف است. این روش مانند استفاده از اثر چندمسیری[3] است، که برای مکان‌های مختلف، مسیرها متفاوت است. به این معنی که مسیرهایی وجود دارند که گره‌های مجاز آن‌ها را دریافت می‌کنند ولی شنودگر آن‌ها را مشاهده نمی‌کند. به همین دلیل تفاوت اساسی بین مشاهدات شنودگر و مشاهدات گره‌های مجاز وجود دارد. تغییرات کران‌های نرخ کلید هنگام استفاده از این روش مطالعه می‌شود و نشان می‌دهیم که با وجود این‌که شنودگر اطلاعات زاویه را در اختیار دارد، می‌توان ظرفیت کلید را به طور نامتناهی با افزایش توان سیگنال راهنما افزایش داد که در [۱۸] چنین امکانی وجود نداشت.

بقیه ساختار مقاله به این صورت است: در ادامه در بخش ۲ مدل سامانه معرفی می‌شود و نحوه تخمین فاصله بررسی می‌شود. سپس در بخش ۳، تحلیل عملکرد دو روش پیشنهادی و تأثیرات آن بر عملکرد سامانه و کران‌های ظرفیت کلید امن بررسی می‌شود. نتایج شبیه‌سازی در بخش ۴ ارائه می‌شود و تحلیل و بحث درباره نوآوری‌ها و مزایای روش‌های پیشنهادی در بخش ۵ صورت می‌گیرد. نتیجه‌گیری مقاله و ارائه پیشنهادهای پژوهشی در بخش ۶ انجام می‌گیرد.

نشان‌گذاری‌ها: اطلاعات متقابل بین X و Y با $I(X;Y)$ نشان داده می‌شود و $H(X)$ نشان‌دهنده آنتروپی X است. $f(.)$ بیان‌گر تابع چگالی احتمال است. $[x]^+$ نشان‌دهنده $\max\{x,0\}$ است.

۲- مدل سامانه

یک شبکه بزرگ از کاربران متحرک در نظر گرفته شده است که حرکت آن‌ها طبق فرآیند مارکوف[4] می‌باشد. در هر زمان کاربران مطابق فرآیند نقطه‌ای پواسون[5] با پارامتر λ توزیع شده‌اند. نمونه این شبکه در شکل (۱) نشان داده شده است.



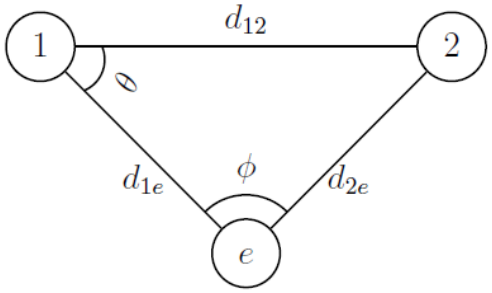
شکل (۱): شبکه‌ای بزرگ با $\lambda = 4$.

توافق کلید به‌صورت چندگامی می‌باشد و هر کاربر به ارتباطی امن با نزدیک‌ترین همسایه‌اش نیاز دارد. به همین دلیل هر کاربر در تلاش است تا کلیدی امن با نزدیک‌ترین همسایه‌اش

[1] Artificial Noise Forwarding
[2] Independent and Identicaly Distributed (i.i.d)
[3] Multipath
[4] Markov
[5] Poisson Point Proccess (P.P.P)

به اشتراک بگذارد تا بتواند ارتباطی امن را میسر سازد. در این مقاله ما یک زوج تصادفی از همسایه‌ها را در نظر می‌گیریم و نرخ کلید امن برای آن‌ها و روش‌هایی برای بهبود نرخ کلید را بررسی می‌کنیم؛ در این حالت هر کاربر دیگری می‌تواند شنودگر باشد که نزدیک‌ترین آن‌ها بیشترین محدودیت را بر نرخ کلید می‌گذارد. این سامانه پایه در شکل (۲) نشان داده شده است. این سامانه پایه از دو گره مجاز، گره ۱ و گره ۲، و یک شنودگر، e، تشکیل شده است.

نکته ۱: همان‌طور که در شکل (۱) نشان داده شده است، نزدیک‌ترین گره به کاربر ۱ پس از کاربر ۲، شنودگر در نظر گرفته شده است. اما ممکن است گره دیگری وجود داشته باشد که در مجموع در مکان بهتری از نظر کسب اطلاعات نسبت به گره مشخص شده باشد. این موضوع تأثیری در کارآمدی روش‌های پیشنهادی که بخش‌های ۳ و ۴ معرفی شده‌اند، نخواهد داشت. تنها، برای برخی محاسبات نرخ کلید چنین فرضی شده است.



شکل (۲): مدل سامانه، گره ۱ و گره ۲ گره‌های مجاز هستند، e شنودگر می‌باشد.

گره‌ها می‌توانند قادر به اندازه‌گیری زاویه باشند و یا نباشند. به همین دلیل دو سناریو را در نظر می‌گیریم: ۱) گره‌های مجهز به آنتن‌های همه‌جهته، ۲) گره‌های مجهز به آرایه آنتن (ارسال توسط آنتن‌های چند جهته). در ادامه این دو سناریو را بررسی می‌کنیم.

گره‌های مجهز به آنتن‌های همه‌جهته: در این حالت همه گره‌ها (یعنی گره‌های مجاز و شنودگر) فقط آنتن همه‌جهته دارند و گره‌های مجاز در تلاشند تا کلیدی امن را به اشتراک بگذارند. اغلب راهبردهای توافق کلید از سه مرحله جمع‌آوری داده‌های تصادفی، اصلاح اطلاعات[1] و تقویت امنیت[2] تشکیل شده‌اند [۱۰]. راهبرد توافق کلید پیشنهادی از سه مرحله تشکیل شده است: تخمین فاصله، اصلاح اطلاعات و تقویت امنیت.

تخمین فاصله: در این گام، گره‌های مجاز در n بازه زمانی سیگنال‌های راهنما برای تخمین فاصله را ارسال می‌کنند. در هر بازه زمانی ابتدا گره ۱ سیگنال راهنما، $X_{b1}(t)$، را با محدودیت توان $\mathbb{E}\{X_{b1}^2(t)\} \le P$ ارسال می‌کند. گره ۲ $X_{b1}(t-\tau)$ را دریافت می‌کند و می‌تواند با استفاده از روش اندازه‌گیری زمان سیگنال دریافتی، تأخیر سیگنال راهنما دریافتی، τ، را تخمین بزند. سپس، با ضرب تأخیر تخمین زده شده در سرعت نور، گره ۲ فاصله خود از گره ۱ را تخمین می‌زند (فاز ۱). سپس گره ۲ سیگنال راهنما، $X_{b2}(t)$، را با محدودیت توان $\mathbb{E}\{X_{b2}^2(t)\} \le P$ ارسال می‌نماید تا گره ۱ فاصله‌اش از گره ۲ را تخمین بزند (فاز ۲). هر بازه زمانی به گونه‌ای طراحی شده که گره‌های ۱ و ۲ امکان تخمین فاصله بین خود، d_{12}، را داشته باشند و در ضمن تغییر فاصله در هنگام ارسال سیگنال راهنما ناچیز باشد. در این حالت هر دو گره فاصله یکسانی را مشاهده می‌نمایند و شرط متقابل بودن برقرار است. سیگنال‌های راهنما فرآیندهای تصادفی گوسی هستند. شنودگر این سیگنال‌های راهنما را در هر دو فاز مشاهده می‌کند و می‌تواند فاصله خود از گره‌های ۱ و ۲ را تخمین بزند؛ سپس با استفاده از مشاهدات خود تلاش می‌کند تا d_{12}، را تخمین بزند (مشاهدات شنودگر را با O نشان می‌دهیم). فاصله بین گره j و l در بازه زمانی i برای $j,l \in \{1,2,e\}$ را با $d_{jl}[i]$ نشان می‌دهیم. هم‌چنین، $\hat{d}_1$ نشان‌دهنده تخمین d_{12} در گره ۱ و $\hat{d}_2$ نشان‌دهنده تخمین d_{12} در گره ۲ می‌باشد، $\hat{d}_{1e}$ تخمین d_{1e} در شنودگر و $\hat{d}_{2e}$ تخمین d_{2e} در شنودگر است. حروف ضخیم برای یک متغیر نشان‌دهنده بردار آن متغیر در n بازه زمانی است.

اصلاح اطلاعات: از آن‌جا که تخمین فاصله در گره‌های ۱ و ۲ با خطا می‌باشد و در نتیجه تخمین‌های گره‌های ۱ و ۲ یکسان نبوده و این عدم یکسان بودن در کلید نهایی تأثیرگذار است، راه‌کاری برای حل این مسأله مورد نیاز است، تا کاربران ۱ و ۲ با استفاده از اطلاعات تصادفی مشترکی که به آن دسترسی دارند به کلیدی امن دست یابند. به همین دلیل در این گام، گره‌های ۱ و ۲ از طریق کانال عمومی بدون نویز با یک‌دیگر ارتباط برقرار می‌کنند، تا اختلافات موجود در اطلاعات خود را تصحیح نمایند، از آن‌رو، به آن کانال عمومی می‌گویند که شنودگر نیز به آن دسترسی دارد. در نهایت گره‌های ۱و ۲ با احتمال بالا بر کلیدی توافق می‌یابند که آن را کلید میانی می‌نامیم.

تقویت امنیت: شنودگر در هر دو گام قبلی اطلاعاتی در مورد کلید میانی به‌دست می‌آورد، در نتیجه کلید میانی به‌طور کامل امن نمی‌باشد. هدف از تقویت امنیت استخراج اطلاعاتی امن از کلید میانی می‌باشد. به همین دلیل در این گام تابع چکیده‌ساز

[1] Information reconciliation
[2] Privacy amplification

عمومی[1] بر کلید میانی اعمال می‌شود و کلید نهایی را نتیجه می‌دهد تا شنودگر اطلاعات ناچیزی از کلید نهایی داشته باشد [۱۰].

کلید نهایی، K، که گره‌های مجاز بر آن توافق می‌کنند باید این سه ویژگی را داشته باشند: قابلیت اطمینان[2]، امنیت[3] و تصادفی بودن[4]. این سه ویژگی برقرارند اگر:

$$\lim_{n\to\infty} \mathbb{P}(K_1 \neq K_2) = 0 \qquad (۱)$$

$$\lim_{n\to\infty} \frac{1}{n} I(K_j; O) = 0 \quad j \in \{1,2\} \qquad (۲)$$

$$\lim_{n\to\infty} \frac{1}{n} \big(R - H(K_j)\big) = 0 \quad j \in \{1,2\} \qquad (۳)$$

که K_1 و K_2 به ترتیب کلیدهای نهایی در گره ۱ و گره ۲ هستند و R نرخ کلید می‌باشد.

گره‌های مجهز به آرایه آنتن: در این حالت، مدل سامانه مثل قبل می‌باشد فقط با این تفاوت که گره‌ها مجهز به آرایه آنتن هستند. در این صورت تمامی گره‌ها می‌توانند زاویه سیگنال دریافتی را نسبت به جهت مشخصی به‌دست آورند؛ به‌ویژه شنودگر قادر به تخمین زاویه ϕ نشان داده شده در شکل (۲) می‌باشد. تخمین ϕ را با $\hat{\phi}$ نمایش می‌دهیم.

هم‌چنین فرستنده سیگنال راهنما در هر فاز، گره ۱ یا گره ۲، می‌تواند سیگنال‌های راهنما را در جهت‌های مختلف ارسال نماید. از این ویژگی می‌توان برای بهبود عملکرد سامانه استفاده کرد که در بخش ۴ آن را بررسی می‌کنیم.

۲-۱- خطای تخمین فاصله

در این زیربخش، تخمین فاصله بین یک فرستنده و یک گیرنده بر اساس زمان سیگنال دریافتی را مطالعه می‌کنیم. نتایج به‌دست‌آمده برای سامانه پایه استفاده خواهند شد. درواقع فرستنده می‌تواند گره ۱ باشد و گیرنده گره ۲ و e باشند و یا فرستنده می‌تواند گره ۲ باشد و گره ۱ و e گیرنده باشند. فرض می‌کنیم فرستنده سیگنال $s(t)$ با تبدیل فوریه $\mathcal{S}(\omega)$ را ارسال می‌کند. سیگنال دریافتی در گیرنده برابر است با:

$$r(t) = d^{-\frac{\alpha}{2}} s(t-\tau) + n(t) \qquad (۴)$$

که $\tau = d/c$ تأخیر کانال، d فاصله بین فرستنده و گیرنده، c سرعت نور و α مؤلفه تضعیف مسیری[5] است. برای بهره کانال تنها مؤلفه تضعیف مسیری در نظر گرفته شده است و از محوشوندگی صرف‌نظر شده است. هم‌چنین $n(t)$ نویز گوسی مختلط جمع‌شونده با چگالی طیف توان دو طرفه برابر با $\frac{N_0}{2}$ می‌باشد.

به‌عنوان معیاری برای خطای تخمین فاصله از کران پایین کرامررائو[6] (CRLB) استفاده می‌کنیم [۲۱]. CRLB کران پایینی را برای واریانس تخمین یک پارامتر قطعی[7] مشخص می‌کند.

تعریف ۱: (کران پایین کرامر-رائو (CRLB)). فرض کنید می‌خواهیم پارامتر X را با استفاده از مشاهدات Y تخمین بزنیم. واریانس تخمین X، یعنی $\hat{X}$، در رابطه زیر صدق می‌کند:

$$\mathrm{Cov}_X(\hat{X}) \geq I_X^{-1} \qquad (۵)$$

که $\mathrm{Cov}_X(\hat{X}) = \mathbb{E}_X\{(\hat{X}-X)(\hat{X}-X)^T\}$ تابع کواریانس و $I_{\{X\}}$ ماتریس اطلاعات فیشر[8] می‌باشد که به‌صورت $I_X = \mathbb{E}_X\left\{(\frac{\partial}{\partial X}\log f_X(Y))(\frac{\partial}{\partial X}\log f_X(Y))^T\right\}$ تعریف می‌شود. در روابط بالا $(.)^{\mathrm{T}}$ بیان‌گر ترانهاده[9] است.

در مسأله ما پارامتری که باید تخمین زده شود، فاصله بین فرستنده و گیرنده یعنی d است و مشاهده، سیگنال دریافتی (r) است که در رابطه (۴) بیان شده است. تابع چگالی احتمال، $f_d(r)$، برابر $\frac{1}{\pi N_0}\exp\left\{-\frac{1}{N_0}\int\left|r(t)-d^{-\frac{\alpha}{2}}s(t-\tau)\right|^2 dt\right\}$ است، در نتیجه $I_d = \gamma R_b$ که در آن $\gamma = \frac{8\pi^2\beta^2}{c^2}$ و $R_b = \frac{\int\left|d^{-\frac{\alpha}{2}}s(t)\right|^2 dt}{N_0}$ و β پهنای باند مؤثر سیگنال می‌باشد که برابر است با $\sqrt{\int \omega^2\left|\mathcal{S}(\omega)\right|^2 d\omega}$. با در نظر گرفتن رابطه (۵)، داریم:

$$\mathbb{E}_d\{(d-\hat{d})^2\} \geq \frac{1}{\gamma R_b} = \frac{N_0 d^\alpha}{\gamma P} \qquad (۶)$$

که $P = \int|s(t)|^2 dt$ توان سیگنال ارسالی است.

نکته ۲: خطای به‌دست‌آمده در رابطه (۶) برابر با موارد مشابه از جمله روابط به‌دست‌آمده در [۲۲] می‌باشد.

حال به مسأله اصلی که مدل‌سازی تخمین فاصله است، می‌رسیم. با در نظر گرفتن فاصله تخمین‌زده شده به‌صورت مجموع فاصله اصلی و نویز مشاهدات، حال مسأله به مدل‌سازی نویز مشاهدات تغییر پیدا می‌کند. نویز مشاهدات، w، را به‌صورت فرآیند گوسی با میانگین 0 و واریانسی برابر با کران کرامر-رائو در نظر می‌گیریم. در این‌صورت برای فاصله داریم:

$$\hat{d} = d + w, \quad w \sim \mathcal{N}\left(0, \frac{N_0 d^\alpha}{\gamma P}\right) \qquad (۷)$$

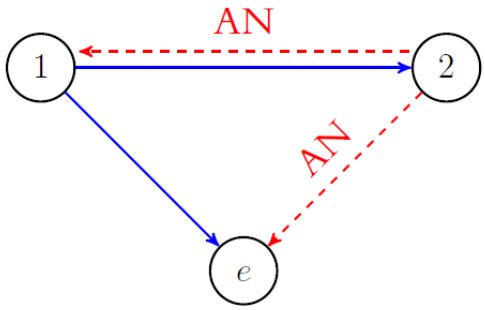
[1] Universal hash function
[2] Reliability
[3] Secrecy
[4] Randomness
[5] Path loss coefficient
[6] Cramer-Rao Lower Bound
[7] Deterministic
[8] Fisher information matrix
[9] Transpose

این مدل مطابق با مدل [۱۸] می‌باشد.

نکته ۳: در نظر گرفتن کران پایین کرامر-رائو برای واریانس $\hat{d}$، بدترین حالت برای هنگامی است که شنودگر گیرنده است؛ چرا که کمترین مقدار واریانس خطا در نظر گرفته می‌شود. اما هنگامی که گیرنده گره مجاز است، باید تخمین‌گر آن کاملا کارآمد باشد وگرنه مقدار واریانس خطای تخمین بیشتر از این کران خواهد بود.

۳- تحلیل عملکرد

در این بخش دو سناریو گره‌های مجهز به آنتن همه‌جهته و گره‌های مجهز به آرایه آنتن در نظر گرفته می‌شوند و برای هر کدام روشی برای افزایش نرخ کلید امن پیشنهاد می‌شود.



شکل (۳): فاز اول: پیکان‌های مشکی نشان‌دهنده سیگنال راهنما و خطوط تیره قرمز نشان دهنده نویز مصنوعی هستند.

۳-۱- گره‌های مجهز به آنتن‌های همه‌جهته

در این حالت تمامی گره‌ها تک آنتنی فرض شده‌اند و راه‌کاری برای بهبود عملکرد سامانه (یعنی افزایش نرخ کلید امن) پیشنهاد می‌شود. راه‌کار پیشنهادی بر پایه ارسال نویز مصنوعی شکل گرفته است. ابتدا روش پیشنهادی به همراه نحوه مدل‌سازی فاصله هنگام استفاده از نویز بررسی می‌شود و با استفاده از آن تأثیر راه‌کار پیشنهادی بر کران‌های ظرفیت کلید امن از طریق محاسبات تئوری مطالعه می‌شود.

همان طور که گفته شد، به دنبال راه‌کاری هستیم تا بتوانیم نرخ کلید امن را افزایش دهیم. برای این منظور دو راه وجود دارد: ۱) داده‌های تصادفی که در اختیار گره‌های مجاز قرار می‌گیرد بیشتر شوند و یا دقت بالاتری داشته باشند، ۲) اطلاعاتی که شنودگر به‌دست می‌آورد کاهش یابند یا با خطای بیشتری در اختیار شنودگر قرار گیرند. با در نظر گرفتن راه دوم، استفاده از گسیل نویز مصنوعی پیشنهاد می‌شود. در ANF با استفاده از ارسال نویز مصنوعی در زمان مناسب، تخمین شنودگر از فاصله بین گره‌های مجاز خراب می‌شود تا بتوان هم امنیت را تضمین نمود و هم نرخ کلید امن را افزایش داد اما نویز مصنوعی تأثیری بر اطلاعات گره‌های ۱ و ۲ نداشته باشد. برای این منظور طرح زیر را پیشنهاد می‌کنیم. طرح پیشنهادی مبتنی بر ANF از دو فاز تشکیل می‌شود: در فاز اول هنگامی که گره ۱ سیگنال راهنما را ارسال می‌کند، گره ۲ همزمان نویز مصنوعی را می‌فرستد و در فاز دوم هنگامی که گره ۲ سیگنال راهنما را ارسال می‌کند، گره ۱ همزمان نویز مصنوعی را می‌فرستد تا تخمین شنودگر را از فاصله بین خودشان خراب کند. نحوه عملکرد گره‌ها در فاز اول در شکل (۳) نشان داده شده است. ایده این است که گیرنده هر سیگنال راهنما، نویز مصنوعی بفرستد تا بتواند تخمین شنودگر را خراب کند. با استفاده از «حذف تداخل خودی»[1] [۲۳] در گره‌ای که نویز مصنوعی تولید می‌کند، گره ۲ در فاز اول و گره ۱ در فاز دوم، می‌تواند اثر نویز مصنوعی را حذف کند تا تأثیری بر تخمین آن از فاصله نداشته باشد. به این معنی که، چون سیگنال ارسال‌کننده نویز مصنوعی از مقدار و توزیع آن خبر دارد، می‌تواند آن را از سیگنال دریافتی خود حذف کند و در نتیجه سیگنال باقی‌مانده، سیگنال راهنما توسط گره دیگر است (البته باید توجه داشت که حذف سیگنال به ابزارهایی نیاز دارد ولی از نظر عملی امکان‌پذیر است). به همین دلیل استفاده از ANF با تقریب نسبتا خوبی تأثیری بر تخمین‌های گره‌های مجاز ندارد و عملکرد آن‌ها مانند حالتی که از ANF استفاده نمی‌کنیم، باقی می‌ماند. اما بر تخمین شنودگر از فاصله تأثیرگذار است چرا که شنودگر نویز مصنوعی را نمی‌داند. ابتدا، نشان می‌دهیم استفاده از ANF چگونه بر تخمین شنودگر اثر می‌گذارد. سیگنال دریافتی در شنودگر هنگام استفاده از نویز مصنوعی برابر است با:

$$r_e(t) = d^{-\frac{\alpha}{2}} s(t-\tau) + d_n^{-\frac{\alpha}{2}} s_n(t-\tau_n) + n(t) \qquad (۸)$$

$d^{-\frac{\alpha}{2}} s(t-\tau) + n(t)$ همان رابطه‌ای است که در (۴) در حالت بدون نویز مصنوعی برقرار است. d_n فاصله تولیدکننده نویز مصنوعی از شنودگر و $s_n(t)$ نویز مصنوعی ارسال شده با توان P_n و τ_n تأخیر کانال از فرستنده نویز مصنوعی تا شنودگر می‌باشد. در [۲۴] برای کران کرامر-رائو هنگام تداخل (بدون توافق کلید) اثر نویز مصنوعی را همانند نویز در نظر گرفته و توان آن‌ها را با یکدیگر جمع کرده. با در نظر گرفتن این موضوع و روند زیربخش ۲-۱، که خطای تخمین فاصله را گوسی فرض کرده و واریانس نویز را برابر کران کرامر-رائو قرار داده، خطای مشاهدات در رابطه (۷) به $w \sim \mathcal{N}\left(0, \frac{d^\alpha}{\gamma P}(N_0 + \frac{P_n}{d_n^\alpha})\right)$ تغییر پیدا می‌کند. درواقع تداخل ناشی از نویز مصنوعی در شنودگر به عنوان نویز در نظر گرفته شده است و با نویز کانال جمع شده است گویا نویز دریافتی در شنودگر $d_n^{-\frac{\alpha}{2}} s_n(t-\tau_n) + n(t)$ است. به این

[1] Self interference cancellation

ترتیب مشاهدات فاصله در گره‌های مختلف هنگامی که از ANF استفاده می‌شود، به‌صورت زیر می‌شود:

$$\hat{d}_1 = d_{12} + w_1, \quad w_1 \sim \mathcal{N}\left(0, \frac{N_0 d^\alpha}{\gamma P}\right) \qquad (۹)$$

$$\hat{d}_2 = d_{12} + w_2, \quad w_2 \sim \mathcal{N}\left(0, \frac{N_0 d^\alpha}{\gamma P}\right) \qquad (۱۰)$$

$$\hat{d}_{1e} = d_{1e} + w_{1e}, w_{1e} \sim \mathcal{N}\left(0, \frac{d_{1e}^\alpha}{\gamma P}(N_0 + \frac{P_n}{d_{2e}^\alpha})\right) \qquad (۱۱)$$

$$\hat{d}_{2e} = d_{2e} + w_{2e}, w_{2e} \sim \mathcal{N}\left(0, \frac{d_{2e}^\alpha}{\gamma P}(N_0 + \frac{P_n}{d_{1e}^\alpha})\right) \qquad (۱۲)$$

در ادامه نشان می‌دهیم که استفاده از ANF می‌تواند نرخ کلید امن را افزایش بدهد.

۳-۱-۱- کران‌های ظرفیت کلید امن

با توجه به نتایج به‌دست‌آمده در بخش قبل و مدل‌سازی فاصله بین گره‌ها، ابزار لازم برای بررسی روش پیشنهادی را در اختیار داریم. در ابتدا کران‌های نرخ کلید امن را با توجه به [۱۸] مشخص می‌کنیم. برای کران پایین ظرفیت کلید داریم:

$$R_L = \max\left\{\lim_{n\to\infty}\frac{1}{n}[I(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_2) - I(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e})]^+, \right. \qquad (۱۳)$$
$$\left. \lim_{n\to\infty}\frac{1}{n}[I(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_2) - I(\hat{\mathbf{d}}_2;\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e})]^+\right\}$$

و کران بالای ظرفیت کلید امن برابر است با:

$$R_U = \lim_{n\to\infty}\frac{1}{n}\min\{I(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_2), I(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_2|\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e})\} \qquad (۱۴)$$

در رابطه (۱۳)، بیشینه‌سازی بین دو رابطه انجام می‌گیرد. رابطه اول اختلاف $I(\hat{d}_1;\hat{d}_2)$ که مقدار اطلاعاتی است که می‌توان از طریق $\hat{d}_1$ درباره $\hat{d}_2$ به‌دست آورد، و $I(\hat{d}_1;\hat{d}_{1e},\hat{d}_{2e})$ می‌باشد. $I(\hat{d}_1;\hat{d}_{1e},\hat{d}_{2e})$ مقدار اطلاعاتی است که می‌توان از طریق مشاهدات شنودگر درباره $\hat{d}_1$ به‌دست آورد، یا به عبارتی اطلاعات متقابل بین مشاهدات گره ۱ و مشاهدات شنودگر است. رابطه دوم همانند رابطه اول است با این تفاوت که جای نمایه‌های ۱ و ۲ جابه‌جا شده است. رابطه (۱۴) کمینه‌سازی بین دو رابطه می‌باشد. رابطه اول در (۱۳) نیز وجود دارد و رابطه دوم $I(\hat{d}_1;\hat{d}_2|\hat{d}_{1e},\hat{d}_{2e})$ می‌باشد، که میزان اطلاعاتی است که می‌توان از طریق $\hat{d}_1$ راجع به $\hat{d}_2$ به‌دست آورد هنگامی که $\hat{d}_{1e}$ و $\hat{d}_{2e}$ معلوم هستند، یا به عبارتی اطلاعات متقابل بین مشاهدات گره‌های ۱ و ۲ هنگامی که مشاهدات شنودگر در دسترس است.

لم ۱: اگر مشاهدات فاصله در حالت عادی، یعنی بدون استفاده از ANF، را با $\hat{\bullet}$ مانند قبل، نشان دهیم و مشاهدات فاصله هنگام استفاده از نویز مصنوعی را با $\hat{\hat{\bullet}}$ نشان دهیم و فرض کنیم واریانس (۱۱) به $\frac{N_0 d_{1e}^\alpha}{\gamma P} + \frac{\hat{d}_{1e}P_n}{\gamma P d_{2e}^\alpha}$ و واریانس (۱۲) به $\frac{N_0 d_{2e}^\alpha}{\gamma P} + \frac{\hat{d}_{2e}P_n}{\gamma P d_{1e}^\alpha}$ تغییر پیدا کند، آن‌گاه استفاده از ANF نرخ کلید امن برای گره‌های مجهز به آنتن‌های همه‌جهته را افزایش می‌دهد.

اثبات: ابتدا نشان می‌دهیم که چه عامل‌هایی بر کران‌های بالا و پایین نرخ کلید امن تأثیرگذار هستند تا تغییرات آن‌ها را هنگام استفاده از ANF بررسی کنیم. ابتدا کران بالای نرخ کلید را در نظر می‌گیریم. از آن‌جا که که ANF فقط بر روی تخمین‌های شنودگر، یعنی $\hat{d}_{1e}$ و $\hat{d}_{2e}$، تأثیرگذار است، جمله اول در (۱۴) تغییر نمی‌کند. به همین دلیل، جمله دوم را در نظر می‌گیریم (البته باید توجه داشت که اگر جمله اول عامل محدودکننده کمینه‌سازی کران بالا باشد، آن‌گاه استفاده از ANF تأثیرگذار نخواهد بود چرا که این جمله تغییری نمی‌کند):

$$\begin{aligned}
R_U &= \lim_{n\to\infty}\frac{1}{n}\left[\mathrm{I}(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_2\,|\,\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e})\right] \\
&= \lim_{n\to\infty}\frac{1}{n}\left[h(\hat{\mathbf{d}}_1\,|\,\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e}) - h(\hat{\mathbf{d}}_1\,|\,\hat{\mathbf{d}}_2,\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e})\right] \\
&\overset{(i)}{\leqslant} \lim_{n\to\infty}\frac{1}{n}\left[h(\hat{\mathbf{d}}_1\,|\,\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e}) - h(\hat{\mathbf{d}}_1\,|\,\mathbf{d}_{12})\right] \\
&\overset{(ب)}{\leqslant} \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\left[h(\hat{d}_1[i]\,|\hat{d}_{1e}[i],\hat{d}_{2e}[i]) - h(\hat{d}_1[i]\,|d_{12}[i])\right] \\
&\overset{(پ)}{=} h(\hat{d}_1\,|\hat{d}_{1e},\hat{d}_{2e}) - h(\hat{d}_1\,|d_{12})
\end{aligned}$$

که (آ) به دلیل زنجیره مارکوف $\hat{d}_1 \to d_{12} \to \hat{d}_2, \hat{d}_{1e}, \hat{d}_{2e}$ برقرار است. (ب) به دلیل استقلال $\hat{\mathrm{d}}_1[\mathrm{i}]$ از $\mathrm{d}_{12}[\mathrm{i}-1]$ به شرط $\mathrm{d}_{12}[\mathrm{i}]$ است. (پ) نیز به دلیل توزیع ایستان[1] متغیرهای تصادفی $\hat{\mathrm{d}}_1[\mathrm{i}]$، $\hat{d}_2[i]$، $\hat{d}_{1e}[i]$ و $\hat{d}_{2e}[i]$ می‌باشد. عبارت دوم، یعنی $h(\hat{d}_1|d_{12})$، هنگام استفاده از ANF تغییری نسبت به حالتی که از ANF استفاده نمی‌شود، پیدا نمی‌کند. پس، تنها $h(\hat{d}_1|\hat{d}_{1e},\hat{d}_{2e})$ را در نظر می‌گیریم.

$f(\hat{d}_1) = f(\hat{d}_2)$ و $f(\hat{d}_1,\hat{d}_{1e},\hat{d}_{2e}) = f(\hat{d}_2,\hat{d}_{1e},\hat{d}_{2e})$ به همین دلیل تنها یکی از دو عبارت در R_L را در نظر می‌گیریم با این فرض که $\hat{d}_1[i]$، $\hat{d}_2[i]$، $\hat{d}_{1e}[i]$ و $\hat{d}_{2e}[i]$ همگی متغیرهای تصادفی **i.i.d** باشند:

$$\begin{aligned}
R_L &= \lim_{n\to\infty}\frac{1}{n}\left[\mathrm{I}(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_2) - \mathrm{I}(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e})\right] \\
&= \lim_{n\to\infty}\frac{1}{n}\left[h(\hat{\mathbf{d}}_1\,|\,\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e}) - h(\hat{\mathbf{d}}_1\,|\,\hat{\mathbf{d}}_2)\right] \\
&\overset{(ا)}{=} h(\hat{d}_1\,|\,\hat{d}_{1e},\hat{d}_{2e}) - \lim_{n\to\infty}\frac{1}{n}h(\hat{\mathbf{d}}_1\,|\,\hat{\mathbf{d}}_2)
\end{aligned}$$

[1] Stationary distribution

باید توجه داشت که (آ) در حالت i.i.d برقرار است. عبارت دوم هنگام ANF تغییر نمی‌کند، چرا که ANF تأثیری بر تخمین گره‌های ۱ و ۲ ندارد، به همین دلیل تنها عبارت اول را در نظر می‌گیریم. در نتیجه برای هر دو کران بالا و کران پایین در حالت i.i.d تغییرات $h(\hat{d}_1|\hat{d}_{1e},\hat{d}_{2e})$ تأثیرگذار و مهم است.

با توجه به فرض مسأله زنجیره مارکوف $\hat{d}_1 \to \hat{d}_{1e},\hat{d}_{2e} \to \hat{\hat{d}}_{1e},\hat{\hat{d}}_{2e}$ برقرار است و طبق نامساوی پردازش داده $h(\hat{d}_1|\hat{d}_{1e},\hat{d}_{2e}) \le h(\hat{d}_1|\hat{\hat{d}}_{1e},\hat{\hat{d}}_{2e})$ برقرار است و در نتیجه می‌بینیم با استفاده از ANF می‌توان کران‌های نرخ کلید را افزایش داد. ■

اگر فرض مسأله برقرار نباشد، آن‌گاه باید مقدار $h(\hat{d}_1|\hat{d}_{1e},\hat{d}_{2e})$ را به‌دست آورد. برای به‌دست آوردن $h(\hat{d}_1|\hat{d}_{1e},\hat{d}_{2e})$، باید توزیع مشترک $\hat{d}_1$، $\hat{d}_{1e}$ و $\hat{d}_{2e}$ را به‌دست آورد. برای این منظور ابتدا $X_1 = d_{12}$، $X_2 = d_{1e}$ و $X_3 = \theta$ در نظر می‌گیریم. باید توجه داشت که توابع چگالی d_{12} و d_{1e} با توجه به P.P.P بودن توزیع گره‌ها مشخص هستند. از آن‌جا که گره‌های مجاز نزدیک‌ترین همسایه‌های یکدیگرند، d_{12} توزیع نمایی دارد. هم‌چنین شنودگر نزدیک‌ترین گره به گره ۱ پس از گره ۲ می‌باشد، به همین دلیل توزیع ارلانگ-۲ دارد و بر این اساس می‌توان $f(d_{12},d_{1e})$ را به‌دست آورد. θ نیز هر مقداری را با احتمال یکسان می‌تواند داشته باشد، به همین دلیل دارای توزیع یکنواخت بین $[0,\pi]$ فرض شده است. پس داریم $f(d_{12},d_{1e}) = \lambda^2 e^{-\lambda d_{1e}}$ و $f(\theta) = \frac{1}{\pi}$. حال با در نظر گرفتن $Y_1 = d_{12}$، $Y_2 = d_{1e}$ و $Y_3 = d_{2e}$ (d_{12},d_{1e},d_{2e} تشکیل مثلث می‌دهند) و استفاده از دترمینان ژاکوبی با فرض این‌که d_{12} و d_{1e} از θ مستقل هستند، می‌توان $f(d_{12},d_{1e},d_{2e})$ را به‌دست آورد. حال می‌توان با در نظر گرفتن این‌که $\hat{d}_1 = d_{12} + w_1$، $\hat{d}_{1e} = d_{1e} + w_{1e}$ و $\hat{d}_{2e} = d_{2e} + w_{2e}$، توزیع مشترک $\hat{d}_1$، $\hat{d}_{1e}$ و $\hat{d}_{2e}$ را به‌دست آورد. این توزیع در [۱۹، رابطه (۱۶)] نشان داده شده است. از آن‌جا که $h(\hat{d}_1|\hat{d}_{1e},\hat{d}_{2e}) = \int f(\hat{d}_1,\hat{d}_{1e},\hat{d}_{2e}) \log\frac{f(\hat{d}_{1e},\hat{d}_{2e})}{f(\hat{d}_1,\hat{d}_{1e},\hat{d}_{2e})} d\hat{d}_1 d\hat{d}_{1e}\, d\hat{d}_{2e}$، به مقدار $f(\hat{d}_{1e},\hat{d}_{2e})$ نیاز داریم که می‌توان از $\int f(\hat{d}_{12},\hat{d}_{1e},\hat{d}_{2e})\, d\hat{d}_{12}$ آن را به‌دست آورد. در نتیجه مقدار دقیق $h(\hat{d}_1|\hat{d}_{1e},\hat{d}_{2e})$ را می‌توان به طور عددی محاسبه کرد. حتی برای توابع چگالی دیگر که مربوط به مدل‌های حرکتی متفاوت است، این مقدار می‌تواند محاسبه شود. حل عددی این رابطه زمان‌بر است و توان محاسباتی بالایی را می‌طلبد. اما اگر وابستگی نویز مشاهدات فاصله به فاصله، یعنی خود سیگنال، را در نظر نگیریم. آن‌گاه از آن‌جا که هنگام استفاده از ANF واریانس نویز بیشتر شده، پس طبق نتایج [۲۵] می‌توان نتیجه گرفت $f(\hat{d}_{12},\hat{d}_{1e},\hat{d}_{2e})$ هنگام استفاده از ANF بیشتر می‌شود و در نتیجه کران‌های ظرفیت کلید امن افزایش می‌یابد.

۳-۲- گره‌های مجهز به آرایه آنتن

در این زیربخش با ادامه روند زیربخش پیش گره‌های مجهز به آرایه آنتن را در نظر می‌گیریم و نحوه عملکرد سامانه را در این شرایط بررسی می‌کنیم. ابتدا تأثیر استفاده از نویز مصنوعی بررسی می‌شود و نشان می‌دهیم اگر شنودگر راهبرد مناسبی در استفاده از آرایه آنتن به‌کار گیرد، آن‌گاه استفاده از ANF اطلاعات بیش‌تری به شنودگر نشت خواهد داد و بنابراین در ادامه روش دیگری برای افزایش نرخ کلید معرفی می‌شود. روش جدید بر مبنای ارسال سیگنال راهنما در جهت‌های مختلف می‌باشد. چرا که گره‌ها توانایی ارسال در جهت‌های مختلف را دارند. در این صورت مفهوم جدیدی به نام فاصله مجازی[1] را معرفی می‌کنیم. فاصله مجازی یعنی کل مسافتی که سیگنال راهنما در جهت‌های مختلف طی می‌کند و این مسافت می‌تواند مسافت مسیر مستقیم نباشد. سپس تأثیر استفاده از این روش را بر نرخ کلید امن بررسی می‌کنیم. با استفاده از شبیه‌سازی نیز روش پیشنهادی ارزیابی می‌شود. نتایج محاسبات نشان می‌دهند که می‌توان با استفاده از روش پیشنهادی نرخ کلید را افزایش داد و حتی عوامل محدودکننده در نرخ کلید، مشاهدات شنودگر، از بین می‌روند و با وجود این‌که شنودگر اطلاعات زاویه را دارد نرخ کلید نامتناهی امکان‌پذیر است.

۳-۲-۱- نویز مصنوعی و گره‌های مجهز به آرایه آنتن

همان‌طور که گفته شد، از آن‌جا که گره‌ها مجهز به آرایه آنتن هستند، توانایی اندازه‌گیری زاویه سیگنال دریافتی را نیز دارند. به خصوص شنودگر که می‌تواند زاویه سیگنال دریافتی را اندازه‌گیری کند و در نتیجه می‌تواند زاویه ϕ را هم اندازه بگیرد. اندازه‌گیری ϕ عاملی محدودکننده در نرخ کلید است و همان‌طور که در [۱۸، قضیه ۲] بیان شده اگر شنودگر بتواند زاویه ϕ را تخمین بزند، آن‌گاه کران بالای نرخ کلید مقداری متناهی دارد و در نتیجه ظرفیت کلید مقداری متناهی است، یعنی حتی نمی‌توان با افزایش توان سیگنال راهنما ظرفیت کلید امن را از حدی بیشتر کرد.

در زیربخش پیش روش ANF معرفی شد و این نتیجه به‌دست آمد که برای گره‌هایی که قادر به اندازه‌گیری زاویه نیستند، این روش مؤثر می‌باشد و باعث افزایش نرخ کلید می‌شود. در ادامه اثر این روش بر گره‌هایی که به آرایه آنتن

[1] Virtual Distance

مجهزند بررسی می‌شود. وقتی شنودگر مجهز به آرایه آنتن است، دو حالت پیش می‌آید: ۱) شنودگر تنها قادر به اندازه‌گیری زاویه دریافتی سیگنال باشد ولی اگر سیگنال‌هایی به طور هم‌زمان به او برسند، قادر به تمیز دادن آن‌ها از یکدیگر نباشد، ۲) شنودگر هم می‌تواند زاویه سیگنال دریافتی را تشخیص دهد و هم سیگنال‌های هم‌زمان را از یکدیگر تشخیص می‌دهد. در لم‌های ۲ و ۳ این دو حالت بررسی می‌شوند.

نکته ۴: منظور از این‌که شنودگر نمی‌تواند سیگنال‌های هم‌زمان را از هم تمیز دهد، یعنی اگر هم‌زمان سیگنال راهنما و نویز مصنوعی به شنودگر برسند، شنودگر نمی‌تواند آن‌ها را از هم تشخیص دهد و مثل حالت آنتن همه‌جهته، نویز مصنوعی بر تخمین شنودگر از فاصله و هم‌چنین زاویه اثر می‌گذارد و تخمین آن را خراب می‌کند، روابط (۱۱) و (۱۲)، و شنودگر توانایی جداسازی آن‌ها را ندارد. این شرایط ممکن است به دلیل ابزارهای ضعیف شنودگر مانند تفکیک‌پذیری پایین، تعداد آنتن‌ها و یا به‌کارگیری روش نامناسب باشد. البته با توجه به فناوری‌های جدید این اتفاق غیرمعمول است.

منظور از جداسازی این است که چون شنودگر مجهز به آرایه آنتن است، می‌تواند زاویه هر سیگنالی که به او می‌رسد را تشخیص دهد و در نتیجه با اتخاذ راه‌کار مناسب، اثر نویز مصنوعی را حذف نماید.

لم ۲: فرض کنید شنودگر می‌تواند زاویه ϕ در شکل (۳) را اندازه بگیرد، ولی نتواند سیگنال‌هایی که به طور هم‌زمان به او می‌رسند را از هم تمیز دهد، آن‌گاه $\lim_{P,P_n\to\infty} R_U \le \infty$.

اثبات: با توجه به روند [۱۸، پیوست B] و در نظر گرفتن اثر ANF داریم: $R_U \le \log \mathbb{E}\left[\frac{u+P_n}{P}\right] - \mathbb{E}\left[\log\frac{v}{P}\right]$، که به ∞ میل می‌کند، هنگامی که $P \to \infty$ و $P_n \to \infty$. u و v توابعی از فواصل بین گره‌ها و زاویه ϕ هستند. پس کران بالای نرخ کلید امن می‌تواند نامتناهی شود چرا که علاوه بر توان سیگنال راهنما توان نویز مصنوعی نیز نامتناهی می‌شود. ■

حال اگر شنودگر بتواند سیگنال‌هایی که هم‌زمان به او می‌رسند را تمیز دهد، که معمولا این اتفاق می‌افتد، آن‌گاه اطلاعات نشت یافته به شنودگر هنگامی که از ANF استفاده می‌کنیم بیشتر از زمانی است که از آن استفاده نمی‌شود.

تعریف ۲: با در نظر گرفتن X^n، Y^n و Z^n به‌ترتیب به عنوان مشاهدات گره ۱، مشاهدات گره ۲و مشاهدات شنودگر در طی n بازه زمانی، میزان اطلاعات نشتی به شنودگر از مشاهدات گره‌های مجاز برابر با $L = I(X^n, Y^n; Z^n)$ است.

حال می‌توان میزان اطلاعات نشتی را مقایسه نمود.

لم ۳: اگر شنودگر مجهز به آرایه آنتن باشد و بتواند سیگنال‌هایی که هم‌زمان به او می‌رسند را از هم تمیز داده و زاویه هر کدام را اندازه بگیرد، یعنی قدرت تفکیک‌پذیری بالایی داشته باشد، آن‌گاه اطلاعات نشتی مشاهدات گره‌های مجاز به شنودگر هنگام استفاده از ANF بیشتر از زمانی است که از ANF استفاده نمی‌شود.

اثبات: میزان اطلاعات نشتی در حالت معمولی، بدون ANF، با توجه به مدل مسأله برابر است با:

$$L_n = I(\hat{\boldsymbol{d}}_1, \hat{\boldsymbol{d}}_2; \hat{\boldsymbol{d}}_{1e}, \hat{\boldsymbol{d}}_{2e}, \hat{\boldsymbol{\phi}}) \qquad (۱۵)$$

و با استفاده از ANF هنگامی که شنودگر می‌تواند سیگنال‌های هم‌زمان را از هم جدا کند، میزان اطلاعات نشتی برابر است با:

$$L_{ANF} = I\left(\hat{\boldsymbol{d}}_1, \hat{\boldsymbol{d}}_2; \hat{\boldsymbol{d}}_{1e}, \hat{\boldsymbol{d}}_{2e}, \hat{\phi}, \tilde{\boldsymbol{d}}_{1e}, \tilde{\boldsymbol{d}}_{2e}, \tilde{\phi}\right) \qquad (۱۶)$$

که $\tilde{\boldsymbol{d}}_{1e}$ تخمین شنودگر از $\boldsymbol{d}_{1e}$ با استفاده از سیگنال نویز مصنوعی، $\tilde{\boldsymbol{d}}_{2e}$ تخمین شنودگر از $\boldsymbol{d}_{2e}$ هنگام استفاده از نویز مصنوعی و $\tilde{\boldsymbol{\phi}}$ تخمین شنودگر از $\boldsymbol{\phi}$ با استفاده از زاویه دو سیگنال نویز مصنوعی است که توسط گره‌های ۱ و ۲ ارسال می‌شود. بدیهی است که (۱۵) از (۱۶) بیشتر نیست. ■

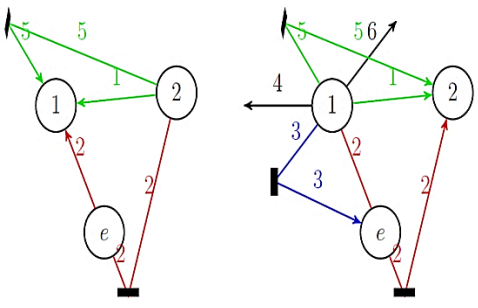
نتیجه‌ای که در لم ۳ به‌دست آمد، قابل انتظار بود، چراکه وقتی شنودگر بتواند سیگنال‌هایی که هم‌زمان به او می‌رسند را تشخیص دهد، می‌تواند به گونه‌ای عمل کند که سیگنال نویز مصنوعی را حذف کند. در این صورت همان شرایط بدون استفاده از ANF پیش می‌آید و استفاده از ANF موجب اتلاف توان می‌شود. هم‌چنین شنودگر می‌تواند اطلاعات هر دو سیگنال، سیگنال راهنما و سیگنال نویز مصنوعی، را به‌کار گرفته و در این شرایط به تخمین بهتری از فاصله بین گره‌های مجاز دست یابد. دیدیم که معمولا استفاده از ANF برای گره‌های مجهز به آرایه آنتن نه تنها مؤثر نمی‌باشد، بلکه اطلاعات بیشتری به شنودگر نشت می‌دهد. پس باید به دنبال روش دیگری برای افزایش نرخ کلید امن باشیم. در زیربخش بعدی راه‌کاری برای این شرایط پیشنهاد می‌شود.

۳-۲-۲- روش پیشنهادی چند آنتنه

در زیربخش ۳-۱ اشاره شد که برای افزایش نرخ کلید دو راه وجود دارد: ۱) افزایش داده‌های تصادفی که گره‌های مجاز، مشاهده می‌کنند (یا افزایش دقت داده‌ها)، ۲) کاهش اطلاعات دریافتی شنودگر (یا افزایش خطای داده‌های شنودگر). روش پیشنهادی در زیربخش ۳-۱ بر پایه راه دوم است، اما در ۳-۲-۱

نشان داده شد که این روش هنگامی که شنودگر مجهز به آرایه آنتن باشد، مفید نیست پس راه اول را در نظر می‌گیریم، یعنی روشی پیشنهاد می‌شود تا اطلاعات دریافتی گره‌های مجاز افزایش یابد بدون آن‌که تأثیر قابل توجهی در اطلاعات دریافتی شنودگر داشته باشد. روش پیشنهادی بر پایه ارسال سیگنال‌های راهنما در جهت‌های مختلف می‌باشد. به‌طور دقیق‌تر در فاز اول ارسال سیگنال راهنما در بازه زمانی i، گره ۱ سیگنال‌های راهنما را در N جهت تصادفی مختلف ارسال می‌کند. N سیگنال راهنمای ارسالی توسط گره ۱ با $X_{b1}^{1}(t)$، $X_{b1}^{2}(t)$، ⋯ و $X_{b1}^{N}(t)$ نشان داده می‌شوند .که دارای محدودیت توان $\left(X_{b1}^{l}\right)^2 \le P$ برای $l \in \{1,\cdots,N\}$ می‌باشند. M_i تا از سیگنال‌های راهنمای ارسال‌شده فوق، توسط گره ۲ و Q_i تا از آن‌ها توسط شنودگر دریافت می‌شود. نمایه i نشان‌دهنده بازه زمانی است. تعداد و الگوی سیگنال‌های دریافتی به جهتی که ارسال می‌شوند، ساختار محیط، مکان قرارگیری گره‌ها و ویژگی‌های سیگنال ارسالی بستگی دارد. M_i سیگنال دریافتی توسط گره ۲ را با $Y_{b1}^{1}(t-\tau_1)$، $Y_{b1}^{2}(t-\tau_2)$، ⋯ و $Y_{b1}^{M_i}(t-\tau_{M_i})$ نشان می‌دهیم . گره ۲ با پردازش بر روی سیگنال دریافتی و تخمین تأخیر زمان دریافت هر سیگنال، فاصله‌ای که آن سیگنال طی کرده است را با استفاده از رابطه $d = c\tau$ محاسبه می‌کند، که c سرعت نور و τ تأخیر زمان دریافت سیگنال موردنظر است. در فاز دوم، گره ۲ تعداد M_i سیگنال راهنما را دقیقا در همان جهتی که آن‌ها را دریافت کرده ارسال می‌کند. به دلیل برقرار بودن شرایط متقابل بودن کانال، سیگنال‌های راهنمای ارسالی توسط گره ۲ همان مسیری را که طی کردند، بازمی‌گردند و در نتیجه فاصله‌ای که گره‌های مجاز مشاهده می‌کنند یکسان است و گره ۱ تمام M_i سیگنال راهنمای ارسالی توسط گره ۲ را دریافت می‌کند. در این فاز نیز شنودگر تعدادی از M_i سیگنال ارسالی را دریافت می‌کند که ممکن است هیچ اطلاعات مشترکی با اطلاعاتی که در فاز قبلی به‌دست آورده نداشته باشند. مقدار M_i و Q_i در بازه‌های زمانی مختلف متفاوت است چرا که مکان گره‌ها در بازه‌های زمانی متفاوت، فرق دارد. پس از به‌دست آوردن داده‌های تصادفی در فازهای اول و دوم، ادامه روند همانند بخش ۲ است، یعنی گره‌های مجاز با استفاده از مکالمه عمومی بر کلیدی میانی توافق می‌یابند و پس از آن از تابع چکیده‌ساز عمومی برای تقویت امنیت استفاده می‌شود.

گره‌های ۱ و ۲ کلید را بر اساس مسافت مسیرهای مختلف که سیگنال‌های راهنما طی می‌کنند، *بردار فاصله مجازی*، تولید می‌کنند. بردار فاصله مجازی بر اساس M_i بردار فاصله‌ای که دو گره مجاز در اختیار دارند ساخته می‌شود که هر مؤلفه آن معادل فاصله‌ای است که سیگنال ارسالی در آن جهت خاص طی می‌کند. اندازه فاصله از مدت زمانی که طول می‌کشد تا سیگنال از فرستنده به گیرنده برسد، به‌دست می‌آید و روابط فاصله همانند بخش ۲ می‌باشد، چرا که از همان روند استفاده شده است. در مکالمه عمومی گره‌های مجاز با یکدیگر توافق می‌کنند که چگونه از n بردار فاصله مجازی برای تولید کلید میانی استفاده کنند. برای شنودگر، تعداد سیگنال‌های دریافتی و فاصله مجازی آن‌ها متفاوت است. به دلیل ساختار محیط و مکانی که شنودگر در آن قرار گرفته است. پس مشاهدات شنودگر می‌تواند به اندازه کافی از گره‌های مجاز متفاوت باشد تا نرخ کلید امن بالایی را تضمین کند. در واقع در این روش از گوناگونی فضایی[1] استفاده شده تا اطلاعات دریافتی گره‌هایی که در مکان‌های متفاوت قرار دارند متفاوت باشد. نمونه‌ای از این سامانه در شکل (۴) نشان داده شده است. گره ۱ ابتدا ۶ سیگنال راهنما را در ۶ جهت مختلف ارسال می‌کند. سیگنال‌های ۱ و ۵ فقط توسط گره ۲ دریافت می‌شوند و سیگنال ۳ فقط توسط شنودگر دریافت می‌شود. سیگنال ۲ را هم گره ۲ و هم شنودگر دریافت می‌کنند اما فاصله مجازی آن برای دو گره متفاوت است. سیگنال ۴ و ۶ را هیچ‌کدام از گره‌ها دریافت نمی‌کنند. سپس در فاز دوم گره ۲ سیگنال‌های ۱، ۲ و ۵ را در همان جهتی که دریافت کرده است، می‌فرستد و گره ۱ نیز تمام آن‌ها را دریافت می‌کند. پس در بردار فاصله مجازی، فاصله معادل مسیرهای ۱،۲ و ۵ وجود دارند و بقیه مسیرها چون توسط گره ۲ دریافت نمی‌شوند، در بردار فاصله مجازی ظاهر نمی‌شوند. شنودگر در این مثال حتی نمی‌تواند مسیر مستقیم ۱ را با استفاده از مشاهداتش همانند روند بخش‌های قبل تخمین بزند چرا که سیگنال مستقیمی از گره ۲ دریافت نکرده است. هم‌چنین نمی‌تواند اطلاعاتی راجع به مسیرهای ۲ و ۵ به‌دست آورد. چون نمی‌داند چه مسیری را طی کرده‌اند. علاوه بر آن، نمی‌داند گره ۲ آن‌ها را دریافت کرده یا نه.



(آ) فاز اول (ب) فاز دوم

شکل (۴): نمونه‌ای از شبکه چند آنتنی با $N = 6$، $M_1 = 3$ و $Q_1 = 2$.

در شکل (۴- الف)، در فاز اول گره ۱، سیگنال‌های راهنما را در ۶ جهت مختلف ارسال می‌کند که گره ۲، سه تا از آن‌ها را دریافت می‌کند. و در قسمت (۴- ب)، در فاز دوم گره ۲، دقیقا در

[1] Spatial diversity

همان سه جهتی که سیگنال‌های راهنما را دریافت کرده، سیگنال راهنما ارسال می‌کند. با در نظر گرفتن عوامل فوق، در زیربخش بعدی به ارزیابی روش پیشنهادی پرداخته و تأثیر آن را بر نرخ کلید بررسی می‌کنیم.

۳-۲-۳- کران‌های ظرفیت کلید امن

در این زیربخش اثر استفاده از ارسال سیگنال راهنما در جهت‌های مختلف را بر کران‌های ظرفیت کلید امن بررسی می‌کنیم و نشان می‌دهیم که استفاده از این روش شرط محدودکننده نرخ کلید که مشاهدات شنودگر است را از بین می‌برد. برای ارزیابی این ساختار، سیگنال‌های راهنما را به دو گروه دید مستقیم[1] (LoS) و دید غیرمستقیم[2] (NLos) تقسیم می‌کنیم. سیگنال‌های دید مستقیم، مسیر مستقیم را تشکیل می‌دهند، مانند مسیر ۱ در شکل (۴) ، و گره‌های مجاز و شنودگر می‌توانند همانند قبل فاصله معادل آن‌را حدس بزنند. سیگنال‌های دید غیرمستقیم مانند سیگنال‌های چندمسیری عمل می‌کنند، و شنودگر حتی نمی‌داند کدام یک از سیگنال‌های راهنما توسط گره مجاز دیگر دریافت شده. هم‌چنین شنودگر فاصله مجازی هر مسیر برای گره‌های مجاز را نمی‌داند. باید توجه داشت که مسیرهای مختلف از یکدیگر مستقل هستند. در نتیجه فاصله مجازی معادل آن‌ها نیز از یکدیگر مستقل است. هم‌چنین مشاهدات فاصله برای مسیرهای دید غیرمستقیم در زمان‌های مختلف از یکدیگر مستقلند. میانگین تعداد مسیرهای دریافتی در n بازه زمانی توسط گره‌های مجاز را با M نشان می‌دهیم. تمامی مشاهدات شنودگر با O نشان داده می‌شود. با توجه به رابطه (۱۴) برای رابطه اول تابع کمینه در کران بالای ظرفیت کلید داریم:

$$\begin{aligned}\mathrm{I}(\mathbf{d}_1;\mathbf{d}_2) &\overset{(ا)}{=} \mathrm{I}(\mathbf{d}_{1_{LoS}};\mathbf{d}_{2_{LoS}}) + \mathrm{I}(\mathbf{d}_{1_{NLoS}};\mathbf{d}_{2_{NLoS}}) \\ &\overset{(ب)}{=} \mathrm{I}(\mathbf{d}_{1_{LoS}};\mathbf{d}_{2_{LoS}}) + Mn\,\mathrm{I}(\hat{d}_{1_{NLoS}};\hat{d}_{2_{NLoS}})\end{aligned}$$

اندیس LoS مشاهدات مربوط به دید مستقیم و NLoS مشاهدات مربوط به دید غیرمستقیم را نشان می‌دهند. (آ) به دلیل استقلال مشاهدات مربوط به فاصله مجازی متناسب با دید مستقیم و فاصله مجازی معادل دید غیر مستقیم برقرار است و (ب) به دلیل استقلال مشاهدات مربوط به دید غیر مستقیم از یکدیگر است که توزیع ایستان آن در نظر گرفته شده است. در این رابطه $\mathrm{I}(\mathbf{d}_{1_{LoS}};\mathbf{d}_{2_{LoS}})$ دقیقا همانند حالت استفاده از آنتن همه‌جهته می‌باشد. و $Mn\,\mathrm{I}(\hat{d}_{1_{NLoS}};\hat{d}_{2_{NLoS}})$ مقداری است که افزوده می‌گردد. برای رابطه دوم تابع کمینه داریم:

$$\begin{aligned}\mathrm{I}(\mathbf{d}_1;\mathbf{d}_2\,|\mathrm{O}) &\overset{(ا)}{=} \mathrm{I}(\mathbf{d}_{1_{LoS}};\mathbf{d}_{2_{LoS}}\,|\mathrm{O}) + \mathrm{I}(\mathbf{d}_{1_{NLoS}};\mathbf{d}_{2_{NLoS}}\,|\mathrm{O}) \\ &\overset{(ب)}{=} \mathrm{I}(\mathbf{d}_{1_{LoS}};\mathbf{d}_{2_{LoS}}\,|\mathrm{O}) + \mathrm{I}(\mathbf{d}_{1_{NLoS}};\mathbf{d}_{2_{NLoS}}) \\ &= \mathrm{I}(\mathbf{d}_{1_{LoS}};\mathbf{d}_{2_{LoS}}\,|\mathrm{O}) + Mn\,\mathrm{I}(\hat{d}_{1_{NLoS}};\hat{d}_{2_{NLoS}})\end{aligned}$$

که (آ) به دلیل استقلال مشاهدات مربوط به دید مستقیم و دید غیر مستقیم برقرار است و (ب) به دلیل این‌که مشاهدات دید غیر مستقیم و مشاهدات شنودگر از یکدیگر مستقل هستند. در این رابطه $\mathrm{I}(\mathbf{d}_{1_{LoS}};\mathbf{d}_{2_{LoS}}\,|\mathrm{O})$ مانند حالت آنتن همه‌جهته است به دلیل آن‌که توزیع مشاهدات دقیقا مانند وضعیت آنتن همه‌جهته است و $Mn\,\mathrm{I}(\hat{d}_{1_{NLoS}};\hat{d}_{2_{NLoS}})$ نیز اضافه می‌شود. از آن‌جا که هر دو مقدار تابع کمینه افزایش دارند، پس شاهد افزایش در کران بالای ظرفیت کلید به میزان $Mn\,\mathrm{I}(\hat{d}_{1_{NLoS}};\hat{d}_{2_{NLoS}})$ هستیم.

در کران پایین ظرفیت کلید امن (رابطه (۱۳)) توزیع آماری توابع چگالی دو رابطه تابع بیشینه یکسان است، به همین دلیل برای بررسی کران پایین نرخ، رابطه اول را در نظر می‌گیریم.

$$\begin{aligned}\mathrm{I}(\mathbf{d}_1;\mathbf{d}_2) - \mathrm{I}(\mathbf{d}_1;O) &\overset{(ا)}{=} \mathrm{I}(\mathbf{d}_{1_{LoS}};\mathbf{d}_{2_{LoS}}) + \mathrm{I}(\mathbf{d}_{1_{NLoS}};\mathbf{d}_{2_{NLoS}}) \\ &\quad -\mathrm{I}(\mathbf{d}_{1_{LoS}};O) - \mathrm{I}(\mathbf{d}_{1_{NLoS}};O) \\ &\overset{(ب)}{=} \mathrm{I}(\mathbf{d}_{1_{LoS}};\mathbf{d}_{2_{LoS}}) - \mathrm{I}(\mathbf{d}_{1_{LoS}};O) + \mathrm{I}(\mathbf{d}_{1_{NLoS}};\mathbf{d}_{2_{NLoS}}) \\ &\overset{(پ)}{=} \mathrm{I}(\mathbf{d}_{1_{LoS}};\mathbf{d}_{2_{LoS}}) - \mathrm{I}(\mathbf{d}_{1_{LoS}};O) + Mn\,\mathrm{I}(\hat{d}_{1_{NLoS}};\hat{d}_{2_{NLoS}})\end{aligned}$$

(آ) به دلیل استقلال مشاهدات مربوط به دید مستقیم و دید غیرمستقیم برقرار است، (ب) به دلیل استقلال مشاهدات مربوط به دید غیر مستقیم گره‌های مجاز و شنودگر برقرار است و (پ) به دلیل مستقل بودن مشاهدات خط غیرمستقیم از یکدیگر است که توزیع ایستان درنظر گرفته شده است. پس در نهایت مقدار $Mn\,\mathrm{I}(\hat{d}_{1_{NLoS}};\hat{d}_{2_{NLoS}})$ هنگام استفاده از آرایه آنتن به کران پایین ظرفیت کلید امن افزوده می‌گردد.

مشخص است هر دو کران بالا و پایین ظرفیت کلید امن افزایش خواهند داشت که می‌تواند به اندازه $M\,\mathrm{I}(\hat{d}_{1_{NLoS}};\hat{d}_{2_{NLoS}})$ باشد. می‌بینیم که هر چه تعداد جهت‌های مختلفی که سیگنال راهنما ارسال می‌گردد بیشتر باشد، میزان افزایش کران‌ها نیز بیشتر خواهد بود. اما نکته مهم دیگر از بین رفتن شرط محدود کننده نرخ در روابط می‌باشد. چرا که مشاهدات شنودگر در $M\,\mathrm{I}(\hat{d}_{1_{NLoS}};\hat{d}_{2_{NLoS}})$ وجود ندارد و می‌توان با افزایش توان سیگنال راهنما نرخ کلید را افزایش داد. پس در این شرایط که شنودگر اطلاعات زاویه را داشت و همین باعث متناهی شدن ظرفیت کلید می‌شد، اما حالا این محدودیت اساسی از بین رفته است و می‌توان نرخ کلید امن را به میزان دلخواه افزایش داد.

[1] Line of Sight
[2] Non Line of Sight

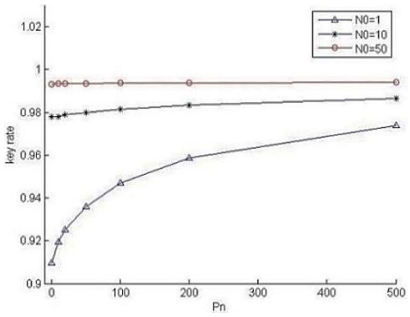
۴- شبیه‌سازی

برای تأیید نتایجی که در زیربخش ۳-۱ به‌دست آمد و ارزیابی روش پیشنهادی از شبیه‌سازی مونت کارلو استفاده می‌کنیم. به همین دلیل، شبکه پایه متشکل از دو گره مجاز، گره ۱ و گره ۲، و یک شنودگر، e، در نظر می‌گیریم که در ناحیه‌ای $m \times m$ با $m = 20$ به طور تصادفی قرار گرفته‌اند. این ناحیه شبکه به مربع‌های 1×1 چندی شده است به این صورت که اگر گره‌ای در هر کدام از این مربع‌ها قرار گرفته باشد، مختصات گره را وسط آن مربع در نظر می‌گیریم. حرکت گره‌ها طبق فرآیند مارکوف می‌باشد و در پایان هر بازه زمانی آن‌ها با احتمال مساوی $\frac{1}{4}$ به یکی از جهت‌های شمال، جنوب، شرق و غرب حرکت می‌کنند (اگر در گوشه‌های ناحیه مورد نظر باشند با احتمال مساوی به یکی از جهت‌هایی که امکان حرکت به آن را دارند، حرکت می‌کنند). مشاهدات فاصله بدون استفاده از ANF مطابق رابطه (۷) است و هنگام استفاده از ANF مطابق روابط (۱۲-۹) می‌باشد، که $\beta = 20MHz$ و $\alpha = 2$ در نظر گرفته شده‌اند. با وجود این‌که اطلاعات زاویه، زاویه ϕ در شکل (۲)، در اختیار شنودگر نمی‌باشد، در شبیه‌سازی فرض می‌کنیم شنودگر مقدار دقیق ϕ را بدون خطا در اختیار دارد و فاصله بین گره‌های مجاز را از طریق رابطه $\hat{d}_e = \sqrt{\hat{d}_{1e}^2 + \hat{d}_{2e}^2 - 2\hat{d}_{1e}\hat{d}_{2e}\cos\phi}$ محاسبه می‌کند. سپس اطلاعات فاصله را چندی می‌کنیم (اطلاعات فاصله در هر بازه زمانی به داده‌های ۱۶، $q = 16$، بیتی تبدیل می‌شود). از اطلاعات چندی‌شده برای محاسبه نرخ عدم مطابقت بیت[1] (BMR) بین تخمین گره ۱ و تخمین شنودگر استفاده می‌شود. اگر اطلاعات گره ۱ که به باینری تبدیل شده را با $\mathbf{v_1}$ و اطلاعات شنودگر را که تبدیل باینری شده با $\mathbf{v_e}$ نشان دهیم، آن‌گاه $\mathrm{BMR} = \frac{\sum_{i=1}^{i=qn} \mathbf{1}(v_1[i] \neq v_e[i])}{qn}$. برای محاسبه نرخ کلید از نرخ ابهام[2] استفاده شده است، $R^* = \frac{1}{n} h\left(K_1 | O, A^r, B^r\right)$، که K_1 کلید تولید شده توسط گره ۱، O تمام مشاهدات شنودگر از منبع تصادفی، A^r اطلاعاتی که گره ۱ هنگام مکالمه عمومی ارسال می‌کند و B^r اطلاعاتی است که گره ۲ هنگام مکالمه عمومی ارسال می‌کند. به دلیل چندی کردن و برخی محدودیت‌های عملی از ظرفیت کلید امن استفاده نکرده و نرخ ابهام به کار برده می‌شود، به همین دلیل هر نرخ $R \leq R^*$ را می‌توان به کار برد. اما محاسبه R^* پیچیدگی بالایی دارد. برای این منظور، R^* را تخمین می‌زنیم. در T مرحله مکالمه عمومی نهایتا شنودگر T بیت از اطلاعات خود را می‌تواند تصحیح کند، یعنی در بهترین حالت برای شنودگر، T بیت از کلید میانی نشت پیدا می‌کند، در نتیجه $R^* \geqslant \frac{1}{n}\left(h(\mathbf{v_1}|\mathbf{v_e}) - T\right)$. برای تخمین $h(\mathbf{v_1}|\mathbf{v_e})$، فرض می‌شود $\mathbf{V}e$ از عبور $\mathbf{V_1}$ از کانال باینری متقارن با احتمال تقاطع BMR تشکیل شده است. در نتیجه می‌توان به جای R^* از $R^{**} = -\mathrm{BMR}\log(\mathrm{BMR}) - (1-\mathrm{BMR})\log(1-\mathrm{BMR}) - \frac{T}{n}$ که T تعداد دفعات مکالمه عمومی است، استفاده کرد. برای محاسبه نرخ از رابطه R^{**} با $T = 0$ استفاده می‌کنیم.

شکل (۵) نرخ کلید امن را به‌ازای توان نویز مصنوعی، P_n، برای توان‌های مختلف نویز، N_0 نشان می‌دهد. $P_n = 0$ همان حالت ساده بدون استفاده از ANF است. همان‌طور که می‌بینیم با افزایش توان نویز مصنوعی، طبق انتظار، نرخ کلید امن افزایش پیدا می‌کند و در همه حالات بیشتر از زمانی است که از نویز مصنوعی استفاده نشده است. به این دلیل که نویز مصنوعی تخمین شنودگر از فاصله را خراب می‌کند، ولی تأثیری بر تخمین گره‌های مجاز ندارد. از طرفی با افزایش N_0 نیز شاهد افزایش نرخ کلید امن در هر دو حالت استفاده از ANF و عدم استفاده از ANF هستیم با وجود این‌که افزایش توان نویز اثر مخربی بر تخمین همه گره‌ها، گره‌های ۱ و ۲ و شنودگر، دارد. شنودگر از طریق تخمین d_{1e} و d_{2e} فاصله بین گره‌های ۱ و ۲ را تخمین می‌زند. به همین دلیل اثر مخرب نویز در شنودگر در دو جا ظاهر می‌شود در حالی که در گره‌های مجاز تخمین به‌صورت مستقیم انجام می‌پذیرد.

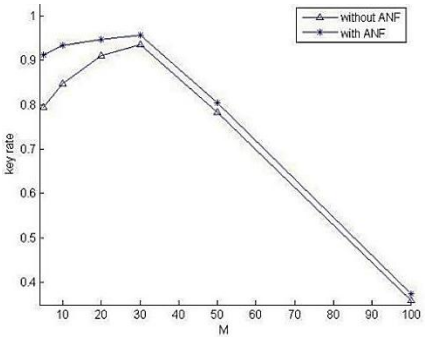
از این رو، به دلیل تأثیر بیشتر توان نویز بر تخریب تخمین شنودگر نسبت به گره‌های مجاز، با افزایش توان نویز نرخ کلید امن افزایش می‌یابد؛ و این نشان می‌دهد استفاده از ANF در محیط‌های نویزی بهتر است. مسأله دیگر که در شکل (۵) قابل مشاهده است، تأثیر بیشتر روش ANF بر بهبود نرخ کلید هنگامی که توان نویز کمتر می‌باشد. چرا که هنگامی که توان نویز بالا باشد، تأثیر خطای ناشی از نویز مصنوعی کمتر دیده می‌شود. در واقع چون ابهام بیشتر می‌باشد، استفاده از نویز مصنوعی تأثیر خود را کمتر نشان می‌دهد.

[1] Bit Mismatch Rate
[2] Equivocation rate

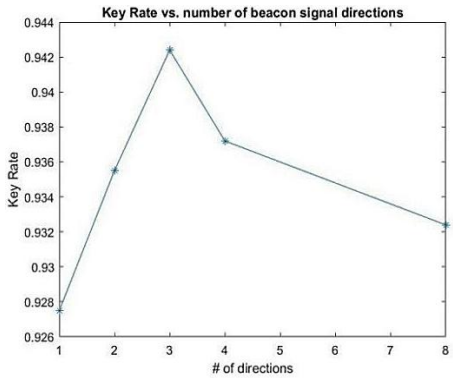


شکل (۵): نرخ کلید امن برای توان‌های مختلف نویز مصنوعی و برای توان‌های مختلف نویز، برای یک شبکه کوانتیزه شده ۲۰×۲۰ با توان سیگنال راهنما برابر با ۱۰۰.

شکل (۶)، نرخ کلید امن برای مساحت‌های مختلف، m متفاوت، را نشان می‌دهد. چون در شبکه بزرگ‌تر ابهام فاصله بیشتر است با افزایش m تا حدی نرخ کلید امن افزایش می‌یابد. چرا که پراکندگی بیشتر داده‌ها ابهام بیشتری را نتیجه می‌دهد. هم‌چنین هرچه m کوچک‌تر باشد تأثیر استفاده از ANF بیشتر است. چراکه که ابهام موجود کمتر است و با استفاده از نویز مصنوعی می‌توان تأثیر بیشتری گذاشت. اما از آن‌جا که با افزایش m اطلاعات مشترک بین گره‌های مجاز کاهش می‌یابد، این اثر باعث کاهش نرخ کلید امن می‌شود. هم‌چنین طبق انتظار در همه حالات نرخ کلید امن هنگام استفاده از نویز مصنوعی بیشتر از زمانی است که از آن استفاده نمی‌شود.



شکل (۶): نرخ کلید امن برای شبکه با مساحت‌های مختلف با $N_0 = 1$ و $P = P_n = 100$.



شکل (۷): نرخ کلید امن برای شبکه با $m = 100$ و توان سیگنال راهنما برابر ۱۰۰ برای تعداد سیگنال‌های ارسالی متفاوت.

در ادامه برای ارزیابی روش پیشنهادی و نتایجی که در زیربخش ۳-۲ به‌دست آمد، از شبیه‌سازی مونت کارلو استفاده می‌شود. شبکه‌ای کوانتیزه $m \times m$ با $m = 100$ در نظر می‌گیریم که طول هر کدام از مربع‌ها ۰/۴متر است. دو گره مجاز، گره ۱ و گره ۲، و یک شنودگر، e، در آن به طور تصادفی قرار گرفته‌اند و هرگاه در مربعی قرار داشته باشند، مختصات گره مختصات نقطه وسط مربع خواهد بود. مدل حرکت گره‌ها همانند قبل است و در انتهای هر بازه زمانی آن‌ها با احتمال مساوی به یکی از جهت‌های شمال، جنوب، شرق و غرب می‌روند. فرض می‌شود هنگامی که شنودگر در یک بازه زمانی در کنار یکی از گره‌های مجاز باشد، یعنی در یک سلول قرار بگیرند، آن‌گاه بردار فاصله مجازی که شنودگر باید تخمین بزند، همانند بردار فاصله مجازی گره‌های مجاز است. هم‌چنین فرض شده تمام جهت‌های ارسالی توسط گره مجاز دریافت می‌گردد. تخمین فاصله نیز مانند قبل است. پس از آن اطلاعات فاصله به داده‌های باینری ۱۶ بیتی تبدیل می‌گردد و نرخ عدم تطابق بیت و نرخ کلید امن محاسبه می‌شود. شکل (۷) نرخ کلید را برای تعداد سیگنال‌های راهنمای ارسالی در جهت‌های مختلف نشان می‌دهد. تعداد جهت ۱ همان حالت ساده بدون استفاده از ارسال در جهت‌های مختلف می‌باشد. همان‌طور که در شکل دیده می‌شود، طبق انتظار در ابتدا با افزایش تعداد جهت‌ها نرخ کلید امن افزایش می‌یابد. چرا که داده‌های بیشتری بین دو گره مجاز به اشتراک گذاشته می‌شود که شنودگر اطلاعاتی در مورد آن ندارد یا اطلاعات کمی می‌تواند به‌دست آورد. اما با افزایش تعداد جهت‌ها شاهد کاهش نرخ کلید هستیم. حدس زده می‌شود که مشاهدات گره‌های مجاز به‌صورت خطی با تعداد مسیرها افزایش می‌یابد و مشاهدات (همبسته با مشاهدات گره‌های مجاز) شنودگر به‌صورت توانی از تعداد مسیرها افزایش می‌یابد، به همین دلیل با افزایش تعداد مسیرها ، نرخ کلید امن کاهش می‌یابد.

۵- تحلیل و بحث

در این بخش به بررسی عملکرد روش‌های پیشنهادی برای بهبود نرخ کلید امن (نسبت به نرخ‌های به‌دست‌آمده در [۱۸]) می‌پردازیم.

همان‌طور که لم ۱ نتیجه می‌دهد، با استفاده از ANF می‌توان نرخ کلید را افزایش داد. اما اگر شنودگر قادر به اندازه‌گیری زاویه سیگنال دریافتی باشد، این روش دیگر مؤثر نخواهد بود و نرخ کلید امن محدود می‌باشد (مشکلی که در [۱۸] نیز وجود داشت). به همین دلیل روش ارسال در جهت‌های

متفاوت و استفاده از فاصله مجازی مطرح شد. در این حالت اغلب مشاهدات گره‌های مجاز و شنودگر مسقل از یکدیگر هستند و در ۳-۲-۳ نشان داده شد که می‌توان شاهد افزایش چشم‌گیری در نرخ کلید امن بود. هم‌چنین مشکل محدود بودن نرخ که در [۱۸] مطرح شد برطرف می‌شود و می‌توان با افزایش توان سیگنال ارسالی، نرخ کلید را به میزان دلخواه افزایش داد.

هم‌چنین نتایج شبیه‌سازی‌ها نیز این نتایج را تأیید می‌کند و نشان می‌دهد که روش ANF د رحالتی که شنودگر قادر به اندازه‌گیری زاویه نباشد، باعث افزایش نرخ کلید می‌شود و روش ارسال در جهات مختلف در حالتی که گره‌ها مجهز به آرایه آنتن باشند، باعث افزایش نرخ کلید می‌شود.

۶- نتیجه‌گیری

ما دو روش برای بهبود توافق کلید مبتنی بر مکان‌یابی ارائه دادیم. روش اول ارسال نویز مصنوعی است که در آن یکی از گره‌ها برای خراب کردن تخمین شنودگر از فاصله نویز ارسال می‌کند. نشان داده می‌شود که اگر شنودگر به آرایه آنتن مجهز نباشد و یا نتواند زاویه سیگنال‌هایی که هم‌زمان به او می‌رسند را از هم تمیز دهد، استفاده از ارسال نویز مصنوعی روشی مؤثر است. در غیر این صورت اگر شنودگر مجهز به آرایه آنتن باشد اطلاعات نشت یافته بیشتر می‌شود. در این شرایط روش ارسال در جهت‌های مختلف پیشنهاد می‌شود و نشان می‌دهیم که این روش می‌تواند نرخ کلید امن را افزایش دهد. هم‌چنین در ادامه می‌توان مسئله‌ای که در آن چند شنودگر وجود دارند که می‌توانند با یکدیگر همکاری کنند را در نظر گرفت.

سپاس‌گزاری

این مقاله توسط صندوق حمایت از پژوهشگران کشور (INSF) با شماره قرارداد ۹۶/۵۳۹۷۹ حمایت شده است.

۷- مراجع

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, “Safeguarding 5g Wireless Communication Networks Using Physical Layer Security,” IEEE Communications Magazine, vol. 53, no. 4, pp. 20–27, 2015.

[2] C. E. Shannon, “A Mathematical Theory of Communication, Part i, Part ii,” Bell Syst. Tech. J., vol. 27, pp. 623–656, 1948.

[3] C. E. Shannon, “Communication Theory of Secrecy Systems,” Bell Labs Technical Journal, vol. 28, no. 4, pp. 656–715, 1949.

[4] A. D. Wyner, “The Wire-tap Channel,” Bell Labs Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] I. Csiszár and J. Korner, “Broadcast Channels with Confidential Messages,” IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, 1978.

[6] W. Diffie and M. Hellman, “New Directions in Cryptography,” IEEE Trans. Inf. Theory, vol. 22, pp. 644–654, Nov. 1976.

[7] A. Bidokhti, S. M. Pournaghei, and A. H. Khalili Tirandaz, “A Generalized Scheme for Extracting Biometric Keys from Keystroke Dynamics,” Journal of Electronical & Cyber Defence, vol. 5, no. 1, Serial no. 17, 2017. (In Persian)

[8] R. Ahlswede and I. Csiszár, “Common Randomness in Information Theory and Cryptography. Part i: Secret Sharing,” IEEE Trans. Inf. Theory, vol. 39, pp. 1121–1132, Jul. 1993.

[9] U. M. Maurer and S. Wolf, “Unconditionally Secure Key Agreement and the Intrinsic Conditional Information,” IEEE Trans. Inf. Theory, vol. 45, no. 2, pp. 499–514, 1999.

[10] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, “Wireless Information-Theoretic Security,” IEEE Trans. Inf. Theory, vol. 54, pp. 2515–2534, Jun. 2008.

[11] R. Wilson, D. Tse, and R. A. Scholtz, “Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels,” IEEE Trans. Inf. Forens. Security, vol. 2, pp. 364–375, Sep. 2007.

[12] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radiotelepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel,” In Proc. 14th ACM Int. Conf. Mobile Computing and Networking (MobiCom’08), pp. 128–139, Sep. 2008.

[13] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, “On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments,” in ACM MobiCom, 2009.

[14] T. Shimizu, H. Iwai, and H. Sasaoka, “Physical-Layer Secret Key Agreement in Two-Way Wireless Relaying Systems,” IEEE Trans. Inf. Forens. Security, vol. 6, pp. 650–660, Sep. 2011.

[15] J. M. Rüeger, Electronic Distance Measurement: An Introduction. Springer Science & Business Media, 2012.

[16] J. J. Caffery Jr, Wireless Location in CDMA Cellular Radio Systems, vol. 535. Springer Science & Business edia, 2006.

[17] C. Neuberg, P. Papadimitratos, C. Fragouli, and R. Urbanke, “A Mobile World of Security- the Model,” in Information Sciences and Systems (CISS), 2011 45th Annual Conference on, pp. 1–6, IEEE, 2011.

[18] O. Gungor, F. Chen, and C. E. Koksal, “Secret Key Generation via Localization and Mobility,” IEEE

Trans. on Veh. Technol., vol. 64, pp. 2214–2230, Jun. 2015.

[19] N. Kazempour, M.Mirmohseni, and MR.Aref. "New Techniques for Localization Based Information Theoretic Secret Key Agreement," In 2017 14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), pp. 70-76. IEEE, 2017.

[20] S. Salimi and P. Papadimitratos, "Pairwise Secret Key Agreement Based on Location-Derived Common Randomness," arXiv preprint arXiv:1512.08652, 2015.

[21] C. R. Rao, Linear Statistical Inference and Its Applications. New York:Wiley, 2nd ed., 1973.

[22] Y. Qi and H. Kobayashi, "Cramer-Rao Lower Bound for Geolocation in Non-Line-of-Sight Environment," in Proc. IEEE Conf. Acoustics, Speech, Signal Process., pp. 2473–2476, May 2002.

[23] D. Bharadia, E. McMilin, and S. Katti, "Full Duplex Radios," ACM SIGCOM.

[24] S. Gezici, M. R. Gholami, S. Bayram, and M. Jansson, "Jamming of Wireless Localization Systems," IEEE Trans. on Commun., vol. 64, pp. 2660–2676, Jun. 2016.

[25] L. Gerdes, M. Riemensberger, and W. Utschick, "On the Equivalence of Degraded Gaussian MIMO Broadcast Channels," Smart Antennas (WSA 2015); Proceedings of the 19th International ITG Workshop on, pp. 1–5, VDE, 2015.

Journal of Electronical & Cyber Defence
Vol. 8, No. 2, 2020, Serial No. 30

Information Theoretic Secret Key Agreement Based on Localization

N. Kazempour, M. Mirmohseni*, M. R. Aref

*Sharif University of Technology

(Received: 50/09/2018, Accepted: 26/05/2019)

ABSTRACT

Sharing secret key is an essential prerequisite of symmetric key cryptography and one way to share the key, is to agree on a secret key. In this research, we consider a source model for information theoretic secret key agreement based on the distance among the nodes. Secret key agreement based on information theory, unlike computational models, guarantees full information secrecy so that eavesdroppers receive no efficient information. The model is a basic system consisting of two legitimate users and an eavesdropper. The legitimate nodes try to agree on a reliable and secure key based on their (noisy) observation of the distance between them. The eavesdropper observes the distance, too. Since the distance between the nodes is under control of none of them, the model for secret key agreement is a source model. First, we model the distance estimation by the nodes to study the performance of the system (secret key capacity bounds). Error of distance estimation is modeled by a gaussian process with zero mean and a variance equal to the Cramer-Rao bound. Then we propose two methods to enhance system utility: artificial noise forwarding (ANF) and multi-antenna transmission (transmission in different beam directions). In the first method artificial noise is used to worsen eavesdropper's distance estimation and in the second method beacon signals are sent in different directions and the virtual distances, that is equal to total distances the beacon signal has traveled, in different beam directions are used as the randomness sources. We show that if the eavesdropper is not equipped with a multi-directional antenna, then artificial noise forwarding is a useful method while in the case of users equipped with multi-directional antenna, artificial noise forwarding leaks more information to the eavesdropper and transmitting in different directions is a suitable way to increase the secret key rate, since the eavesdropper gains little information about virtual distances and most of the observations of the legitimate nodes and the eavesdropper are independent.

Keywords: Secret key Agreement, Localization, Information Theoretic Secrecy, Artificial Noise forwarding, Secret key Capacity.

* Corresponding Author Email: mirmohseni@sharif.edu