Scientific Journal of Electronical & Cyber Defence
Vol. 10, No. 3, Autumn 2022, Serial No. 39

The Study and Analysis of Hardware Impairments Effects with Multiple Eavesdroppers in Internet of Things Network

M. Fatehi*, S. A. Mohajeran, J. Jahanshiri

*Master's student in Information Technology Management, Mashhad Branch, Islamic Azad University, Mashhad, Iran

(Received: 18/12/2021, Accepted: 02/05/2022)

ABSTRACT

Internet of Things is a revolutionary approach for future wireless technology enhancement and hence, network security is vital in protecting client data and information of users. This paper investigates impact of hardware impairments on the probability of non-zero secrecy capacity of internet of things network. In the considered protocol, multiple eavesdroppers attempt to overhear the data that is transferred from a source to a destination. We derive exact expressions of the non-zero secrecy capacity probability in integral forms with different hardware Impairments for source, destination or eavesdroppers over Rayleigh fading channels. Finally, Monte Carlo simulations are performed to verify our derivations.

Keywords: Internet Objects, Physical Layer Security, Hearders, Hardware Failure, Safe Capacity.

* Corresponding Author Email: M.fatehi950@gmail.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۳، پاییز ۱۴۰۱، ص ۱۲۶- ۱۱۹

علمی – پژوهشی

بررسی و شبیه‌سازی تأثیر نارسایی سخت‌افزاری بر امنیت لایه فیزیکی در شبکه‌های اینترنت اشیاء با حضور تعدادی دلخواه شنودگر

محمد فاتحی[1*]، سید علی مهاجران[2]، جواد جهانشیری[3]

۱- دانش‌آموخته کارشناسی ارشد مدیریت فناوری اطلاعات، واحد مشهد، دانشگاه آزاد اسلامی، ۲- دکتری برق مخابرات، دانشگاه فردوسی مشهد، مشهد، ۳- استادیار، مدیریت راهبردی فضای سایبر، گروه فتا، دانشگاه علوم انتظامی امین، تهران، ایران

(دریافت: ۱۴۰۰/۰۹/۲۷، پذیرش: ۱۴۰۱/۰۲/۱۲)

چکیده

امروزه اینترنت اشیاء نوآوری آینده در زمینه تکنولوژی‌های بی‌سیم محسوب می‌گردد. در نتیجه با توجه به گستردگی این فناوری، ایجاد امنیت این شبکه‌ها اهمیت بالایی خواهد داشت. در این مقاله، به بررسی تأثیر نارسایی سخت‌افزاری بر امنیت لایه فیزیکی در شبکه‌های اینترنت اشیاء با حضور تعدادی دلخواه شنودگر می‌پردازیم. به این منظور ظرفیت امن غیرصفر را برای بررسی امنیت لایه فیزیکی مدنظر قرار می‌دهیم. در ادامه عبارت‌های ریاضی برای ظرفیت امن غیرصفر در حالت‌های مختلف با مقدار نارسایی متفاوت در فرستنده، گیرنده و یا شنودگر به دست می‌آوریم. در استراتژی مدنظر ما محدودیتی در تعداد شنودگران نداریم. در انتها، به‌منظور ارزیابی دقت روابط ریاضی، از شبیه‌سازی مونت‌کارلو استفاده می‌کنیم.

کلیدواژه‌ها: اینترنت اشیاء، امنیت لایه فیزیکی، شنودگران، نارسایی سخت‌افزاری، ظرفیت امن غیرصفر

۱- مقدمه

اینترنت اشیاء[1] توصیف جدیدی در دنیای فناوری و اطلاعات است که در آن اشیاء به کمک ابزارهای ارتباطی (اینترنت یا اینترانت)، با سایر اشیاء تعامل دارند و اطلاعات خود را با هم و یا با انسان‌ها به اشتراک می‌گذارند و کلاس جدیدی از قابلیت‌ها، برنامه‌های کاربردی و سرویس‌ها را ارائه می‌دهند. اینترنت اشیاء نوآوری آینده در زمینه تکنولوژی‌های بی‌سیم محسوب می‌گردد و در بسیاری از زمینه‌ها و حوزه‌ها دارای کاربرد است [۱].

این فناوری مدرن پس از طی کردن مراحل تکاملی اولیه با موضوع چالش‌های امنیتی، اهمیت محرمانگی و شکاف اطلاعاتی و ارتباطاتی روبه‌رو شده است که هرکدام از این موضوعات نیازمند بررسی، تحلیل و ارزیابی دقیق است. از طرفی، ماهیت پخشی محیط انتقال بی‌سیم سبب می‌گردد که شنودگران[2] در ارتباطات بی‌سیم پیام‌های انتقال داده شده را شنود کنند و یا اخلال‌گران پیام‌های ارسالی را دچار اختلال کنند و پیامدهای امنیتی شدید را به همراه داشته باشد. جهت ممانعت از شنود، لایه امن فیزیکی[3] برای اجرای تئوری انتقال اطلاعات امن موردمطالعه و بررسی قرار می‌گیرد [۲]. مسئله اخلال‌گری در مخابرات بی‌سیم نیز در بسیاری از سناریوهای عملی وجود دارد و در شبکه‌های تجاری باعث ایجاد کیفیت خدمات نامطلوب می‌شود [۳].

از طرف دیگر، در دنیای واقعیت و در عمل، اکثر فرستنده و گیرنده‌های یک سیستم مخابراتی با اختلالات و نارسایی[4] همچون عدم تطابق شاخه هم‌فاز و شاخه متعامد[5]، نویز فاز[6]، خطای کوانتیزاسیون[7] و قطعات آنالوگ غیرخطی[8] در تقویت‌کننده‌ها همراه است [۴]. هرچند با استفاده از سخت‌افزارهای گران‌تر، دقیق‌تر و الگوریتم‌های پیچیده‌تر همچون جبران‌سازها تا حدودی این نارسایی‌ها برطرف می‌شود اما استفاده از این امکانات به معنای هزینه بیشتر و توان مصرف بالاتر خواهد بود. حتی با استفاده از امکانات و روش‌های ذکرشده لزوماً تمام این نارسایی‌ها برطرف نمی‌شود و همواره مقداری از این نارسایی‌ها در سیستم وجود خواهد داشت. مهم‌ترین دلایل وجود نارسایی سخت‌افزاری در یک سیستم مخابراتی به شرح زیر است [۵ و ۶]:

- مدل‌سازی نادرست که موجب ایجاد خطایی می‌گردد که قابل صرف‌نظر کردن نیست.

* رایانامه نویسنده مسئول: M.fatehi950@gmail.com

[1] Internet of things
[2] Eavesdroppers
[3] Physical layer security
[4] Impairments
[5] Inphase and Quadrature Imbalance
[6] Phase noise
[7] Error in Quantization
[8] Nonlinear amplifiers

ناشر: دانشگاه جامع امام حسین (ع)

- تخمین نادرست پارامترها
- ماهیت متغیر با زمان و تصادفی بودن نویز بنابراین در نظر داشتن این نارسایی‌ها در یک سیستم مخابراتی از اهمیت بسیار بالایی برخوردار است و در طراحی سیستم‌ها باید مدل مناسب این نارسایی‌های سخت‌افزاری مدنظر قرار گیرد.

۱-۱- نوآوری

پژوهش‌های فراوانی در زمینه رمزنگاری در حوزه اینترنت اشیاء تاکنون انجام شده است [۷ و ۸]. در ادامه با پیشرفت اطلاعات و سرعت بالای سیستم‌ها امکان شکست سیستم‌ها و رمزگشایی بالا رفته است و رمزنگاری در لایه‌های داخلی با توجه به محدودیت سرعتی که دارند با چالش روبرو هستند؛ بنابراین محققان جدیداً علاقه‌مند هستند تا امنیت را در لایه فیزیکی در سیستم‌های اینترنت اشیاء بررسی کنند. در [۹] محققان به بررسی احتمال امن و میانگین احتمال قطع با وجود شنودگر در سیستم‌های اینترنت اشیاء پرداخته‌اند. همچنین در [۱۰] محققان احتمال امن را در سیستم‌های چند ورودی –چند خروجی بررسی کرده‌اند. در [۱۱] نویسندگان به بررسی احتمال قطع با وجود رله در حضور شنودگر پرداخته‌اند.

اگرچه بسیاری از پژوهش‌های صورت گرفته تاکنون سیستم‌ها را به لحاظ سخت‌افزاری ایدئال فرض کرده‌اند و مشکلات ناشی از ساخت در بسیاری از این پژوهش‌ها مدنظر قرار نگرفته است. در این مقاله، نویسندگان مقاله به بررسی آثار مخرب تعدادی دلخواه شنودگر در سیستم اینترنت اشیاء با حضور نارسایی سخت‌افزاری پرداخته و مسئله‌ی امنیت لایه‌ی فیزیکی با معیار احتمال امن غیرصفر بررسی شده است.

مهم‌ترین نوآوری مقاله به شرح زیر است:

- به دست آوردن یک رابطه ریاضی صریح برای احتمال امن غیرصفر در یک سیستم اینترنت اشیاء که تعدادی دلخواه شنودگر دارد و هر کدام از این شنودگران به‌تنهایی دارای مشکلات سخت‌افزاری هستند.

۲- مفاهیم اولیه

در این بخش به بررسی مفاهیم اولیه موردنیاز در مقاله می‌پردازیم.

۲-۱- مفهوم امنیت لایه فیزیکی

لایه فیزیکی یک شبکه عبارت است از محیطی که در آن یک بیت از فرستنده به گیرنده منتقل می‌گردد، این محیط می‌تواند یک محیط سیمی یا بی سیم باشد. پروتکل های مختلف اترنت[1]، توکن رینگ[2]، وای فای[3]، بلوتوث[4] و غیره در این لایه وجود دارند اما در امنیت لایه فیزیکی، از ویژگی‌های ذاتی کانال بی‌سیم استفاده می‌کنیم و در حقیقت امنیت لایه فیزیکی مختص شبکه‌های بی‌سیم است. با ایجاد امنیت در لایه فیزیکی به دنبال تأمین امنیت در فاز انتقال اطلاعات هستیم درصورتی‌که در امنیت در لایه‌های بالاتر شبکه به دنبال روش‌هایی مبتنی بر رمزنگاری هستیم [۱۲]. تفاوت دیگری که این روش با روش‌های مبتنی بر رمزنگاری[5] دارد این است که وابسته به قدرت محاسباتی سیستمی نیست، یعنی توانایی محاسباتی سیستم شنودگر، محدودیتی برای ما ایجاد نمی‌کند که یک نکته بسیار مثبت است. این روش‌ها در سال‌های ۱۹۷۰ معرفی شده‌اند ولی امروزه به دلیل گسترده شدن شبکه‌های بی‌سیم و محبوبیت تلفن‌های همراه، توجه ویژه‌ای به این نوع امنیت شده است [۱۳].

۲-۲- نحوه ایجاد امنیت در لایه فیزیکی

در شبکه‌های بی‌سیم، مفهومی به نام «ظرفیت»[6] وجود دارد که مشخص‌کننده‌ی بیشترین تعداد بیت‌هایی است که در این لینک در یک ثانیه و در یک هرتز منتقل می‌شود. به‌عنوان مثال اگر ظرفیت لینکی ۵ بیت بر ثانیه بر هرتز باشد، و پهنای باندی که استفاده می‌کنیم ۱۰ کیلوهرتز باشد، ما یک لینک با حداکثر نرخ ۵۰ کیلوبیت بر ثانیه (۵۰ kbps) ایجاد کردیم. مقدار این ظرفیت وابسته به میزان نویز موجود در این کانال بی‌سیم است به‌طور دقیق‌تر، وابسته به نسبت توان سیگنال ارسالی به توان نویز است که با پارامتر سیگنال به نویز (SNR)[7] آن را نشان می‌دهیم و B پهنای باند در دسترس ما است [۱۳ و ۱۴].

$$C = B\ \log_2(1+SNR). \qquad (۱)$$

در مثال بالا اگر سیگنالی با نرخ ۶۰ کیلوبیت بر ثانیه ارسال کنیم، گیرنده نمی‌تواند سیگنال دریافتی را به‌درستی آشکار کند و سیگنال دریافتی دیگر مفید نیست. اگر از این ویژگی به‌درستی استفاده کنیم و کاری کنیم که نرخ ارسالی برای گیرنده اصلی مناسب باشد درحالی‌که برای شنودگر زیاد باشد، می‌توانیم از شنود دوری کنیم؛ یعنی سیگنال آشکارشده توسط شنودگر، شبیه مثال بالا پر از خطا شده و دیگر مفید نیست. واضح است که اگر ظرفیت شنودگر بیشتر از ظرفیت گیرنده اصلی باشد، نمی‌توانیم از شنود دوری کنیم و روش‌هایی مثل تولید نویز

[1] Ethernet
[2] Token ring
[3] Wifi
[4] Bluetooth
[5] Cryptography
[6] Capacity
[7] Signal to noise ratio

مصنوعی جهت تضعیف کانال شنودگر برای پایین آوردن ظرفیت آن یا تداخل مشارکتی[1] می‌توانند در این حالت مفید واقع شوند [۱۴].

۲-۳- رابطه امنیت لایه فیزیکی و امنیت در دیگر لایه‌ها

در این بخش به این پرسش پاسخ خواهیم داد که در صورت استفاده از امنیت لایه فیزیکی آیا نیازمند استفاده از امنیت در لایه‌های دیگر شبکه همچون رمزنگاری هستیم یا خیر؟ همان‌طور که توضیح داده شد، دو محدودیت به‌صورت کلی وجود دارد: توانایی محاسباتی و کیفیت کانال. محدودیت اول باعث می‌شود که روش‌های رمزنگاری توسط سیستم‌های قوی‌تر شکست بخورد و استفاده از امنیت لایه فیزیکی مکملی برای تأمین امنیت می‌شود. محدودیت دوم باعث می‌شود که فقط بتوانیم این‌گونه امنیت را برای شبکه‌های بی‌سیم استفاده کنیم (زیرا به‌عنوان مثال در فیبر نوری SNR به بی‌نهایت میل می‌کند و کانال گیرنده و شنودگر محدودیتی در ظرفیت ندارد). همچنین اگر ظرفیت شنودگر را به هر دلیلی نتوانیم کمتر از ظرفیت گیرنده اصلی کنیم، دیگر نمی‌توانیم امنیت را در فاز انتقال اطلاعات تأمین کنیم. پس همچنان تکنیک‌های رمزنگاری لازم است. هدف ما در این مقاله این است که از یک ویژگی ذاتی که در محیط وجود دارد (چه بخواهیم، چه نخواهیم در کانال بی‌سیم، ظرفیت حدی دارد) به‌درستی استفاده کنیم.

۳- مدل سیستم

مدل سیستم برای پروتکل مدنظر ما به‌گونه‌ای است که فرستنده A در تلاش هست تا اطلاعات خود را به مقصد B منتقل کند درحالی‌که تعداد k شنودگر دلخواه در سیستم وجود دارند و برای سیستم مزاحمت ایجاد می‌کنند. فرض کنید گیرنده B و همچنین تمامی شنودگرها از یک آنتن در گیرنده خود بهره‌مند هستند. همچنین در مدل سیستم فرض شده، فرستنده و گیرنده اصلی و همچنین گیرنده‌های شنودگران ایدئال نیست و دارای نارسایی سخت‌افزاری هستند.

در این پژوهش، فرض می‌کنیم یک الگوریتم جبران‌ساز مناسب برای نارسایی سخت‌افزاری استفاده شده است و تمرکز ما بر روی بررسی اثر ترکیبی نارسایی‌های سخت‌افزاری باقیمانده ناشی از جبران‌سازی است. برای مدل کردن اثرات باقیمانده نارسایی‌های سخت‌افزاری، معمولاً فرض می‌شود که سیگنال دریافتی در گیرنده اصلی و گیرنده‌های شنودگران توسط یک نویز گوسی جمع شونده دچار اعوجاج می‌شود. این مدل، تجزیه‌وتحلیل تئوری و همچنین تجربی عملی را امکان‌پذیر می‌کند. به‌صورت دقیق‌تر، هنگامی‌که یک اثر ترکیبی از باقیمانده نارسایی‌های سخت‌افزاری در سیستم وجود داشته باشد، سیگنال دریافت شده در گیرنده B یعنی، g، می‌تواند به شرح زیر بیان شود [۱۵]:

$$g = h_s\left(x+\eta_s\right)+\eta_b+n_b \qquad (۲)$$

همچنین سیگنال دریافت شده در گیرنده شنودگر iام یعنی، y_i، به‌صورت زیر است [۱۵]:

$$y_i = h_{ei}\left(x+\eta_s\right)+\eta_i+n_i \qquad (۳)$$

به‌طوری‌که در روابط بالا، h_s بیان‌گر ضریب کانال بین فرستنده A و گیرنده B است و همچنین h_{ei} بیان‌گر ضرایب کانال بین فرستنده A و گیرنده شنودگر iام است. متغیر x بیان‌گر سیگنال ارسالی با قید توان $P = E\left[\left|x\right|^2\right]$ است. η_s بیان‌گر اعوجاج ناشی از سخت‌افزار غیرایدئال در فرستنده A است که به‌صورت یک نویز گوسی جمع شونده با میانگین صفر و واریانس $k_s^2 P$ به‌صورت $\eta_s \sim CN\left(0,k_s^2 P\right)$ مدل می‌شود که k_s میزان نارسایی سخت‌افزار غیرایدئال در فرستنده A است. همچنین، η_b بیان‌گر اعوجاج ناشی از سخت‌افزار غیرایدئال در گیرنده B است که به‌صورت یک نویز گوسی جمع شونده با میانگین صفر و واریانس $k_b^2\left|h_s\right|^2 P$ به‌صورت $\eta_b \sim CN\left(0,k_b^2\left|h_s\right|^2 P\right)$ مدل می‌شود که k_b میزان نارسایی سخت‌افزار غیرایدئال در گیرنده B است. همچنین به‌طور مشابه، η_i بیانگر اعوجاج ناشی از سخت‌افزار غیرایدئال در گیرنده شنودگر iام است که به‌صورت یک نویز گوسی جمع‌شونده با میانگین صفر و واریانس $k_i^2\left|h_{ei}\right|^2 P$ به‌صورت $\eta_i \sim CN\left(0,k_i^2\left|h_{ei}\right|^2 P\right)$ مدل می‌شود که k_i میزان نارسایی سخت‌افزار غیرایدئال در گیرنده شنودگر iام است. ضرایب k_b، k_s و k_i در حقیقت به معیار مربع اندازه بردار خطا مرتبط هستند که این معیار عدم تطابق بین سیگنال واقعی و سیگنال مورد انتظار در فرستنده و گیرنده‌های فرکانس رادیویی را اندازه‌گیری می‌کند. حالت خاص $k_i = k_s = k_b = 0$ نشان‌دهنده‌ی سخت‌افزار ایدئال است در ادامه، n_b و n_i به ترتیب بیان‌گر نویز سیستم مخابراتی در گیرنده B و گیرنده شنودگر iام با میانگین صفر و واریانس N_0 به‌صورت $n_i \text{ and } w_i \sim CN\left(0,N_0\right)$ است.

1. Cooperative jamming

در این مقاله، ضریب کانال بین فرستنده A و گیرنده B یعنی h_s و همچنین ضریب کانال بین فرستنده A و گیرنده شنودگر iام یعنی h_{ei} به‌طوری‌که $i=1,...,k$ را به‌عنوان ضرایب کانال محوشونده رایلی در نظر می‌گیریم. در نتیجه مطابق نتیجه اثبات در [۱۴] بهره کانال یعنی $|h_{ei}|^2$ و $|h_s|^2$ متغیرهای تصادفی نمایی هستند که توابع توزیع تجمعی و همچنین چگالی احتمال آن‌ها به ترتیب به شرح زیر است:

$$\begin{aligned} F_{|h_{ei}|^2}(x) &= 1-\exp(-\alpha_i x) \\ f_{|h_{ei}|^2}(x) &= \frac{d}{dx}F_{|h_{ei}|^2}(x) = \alpha_i \ \exp(-\alpha_i x) \end{aligned} \quad (۴)$$

و

$$\begin{aligned} F_{|h_s|^2}(x) &= 1-\exp(-\alpha_s x) \\ f_{|h_s|^2}(x) &= \frac{d}{dx}F_{|h_s|^2}(x) = \alpha_s \ \exp(-\alpha_s x) \end{aligned} \quad (۵)$$

به‌طوری‌که α_s و α_i بیان‌گر پارامترهای متغیرهای تصادفی $|h_s|^2$ و $|h_{ei}|^2$ است و در عمل با افت مسیر رابطه دارند که طبق [16] به ترتیب به‌صورت $\alpha_i = d_{ei}^{\beta}$ و $\alpha_s = d_s^{\beta}$ بیان می‌گردند. در رابطه فوق، d_S بیان‌گر فاصله بین فرستنده A و گیرنده B است و d_{ei} بیان‌گر فاصله بین فرستنده A و گیرنده شنودگر iام است. همچنین β برابر قدرت افت مسیر است. به‌منظور سادگی مسئله فرض می‌گردد تمام شنودگران مهاجم در نزدیکی یکدیگر قرار دارند و در نتیجه فاصله بین فرستنده A و گیرنده شنودگر iام به‌صورت زیر است:

$$d_{ei} = d_e \ , \forall k \quad (۶)$$

در نتیجه مطابق روابط شماره (۲) و (۳) نسبت سیگنال به نویز و اعوجاج (SNDR)[1] در گیرنده B یعنی g به‌صورت زیر خواهد بود.

$$\begin{aligned} SNDR_g &= \frac{|h_s|^2 P}{|h_s|^2 \ k_s^2 P + |h_s|^2 \ k_b^2 P + N_0} \\ &= \frac{|h_s|^2 P}{|h_s|^2 P\left(k_s^2 + k_b^2\right) + N_0} \\ &= \frac{\gamma_s}{\gamma_s\left(k_s^2 + k_b^2\right)+1}, \end{aligned} \quad (۷)$$

همچنین SNDR در گیرنده شنودگر iام یعنی، y_i برابر خواهد بود با:

$$\begin{aligned} SNDR_{y_i} &= \frac{|h_{ei}|^2 P}{|h_{ei}|^2 \ k_s^2 P + |h_{ei}|^2 \ k_i^2 P + N_0} \\ &= \frac{|h_{ei}|^2 P}{|h_{ei}|^2 P\left(k_s^2 + k_i^2\right) + N_0} \\ &= \frac{\gamma_{ei}}{\gamma_{ei}\left(k_s^2 + k_i^2\right)+1}, \end{aligned} \quad (۸)$$

که در روابط فوق γ_{ei} و γ_s به ترتیب برابر $\gamma_{ei} = \frac{P|h_{ei}|^2}{N_0}$ و $\gamma_s = \frac{P|h_s|^2}{N_0}$ هستند. همچنین تابع توزیع تجمعی برای متغیر تصادفی $\gamma_{ei} = \frac{P|h_{ei}|^2}{N_0}$ به شرح زیر به دست می‌آید:

$$\begin{aligned} F_{\gamma_{ei}}(x) &= F_{\frac{P}{N_0}|h_{ei}|^2}(x) \\ &= \Pr\left(\frac{P}{N_0}|h_{ei}|^2 \le x\right) \\ &= \Pr\left(|h_{ei}|^2 \le \frac{N_0}{P}x\right) \\ &= F_{|h_{ei}|^2}\left(\frac{N_0}{P}x\right) \\ &= 1-\exp\left(-\frac{\alpha_i N_0 x}{P}\right), \end{aligned} \quad (۹)$$

همچنین تابع چگالی احتمال برای متغیر تصادفی $\gamma_{ei} = \frac{P|h_{ei}|^2}{N_0}$ به‌صورت زیر محاسبه می‌گردد:

$$\begin{aligned} f_{\gamma_{ei}}(x) = f_{\frac{P}{N_0}|h_{ei}|^2}(x) &= \frac{d}{dx}F_{\frac{P}{N_0}|h_{ei}|^2}(x) \\ &= \frac{\alpha_i N_0}{P} \ \exp\left(-\frac{\alpha_i N_0 x}{P}\right) \\ &= \frac{d_e^{\beta} N_0}{P} \ \exp\left(-\frac{d_e^{\beta} N_0 x}{P}\right), \end{aligned} \quad (۱۰)$$

به‌طور مشابه تابع توزیع تجمعی برای متغیر تصادفی $\gamma_s = \frac{P|h_s|^2}{N_0}$ به شرح زیر به دست می‌آید:

$$F_{\gamma_s}(x) = 1-\exp\left(-\frac{\alpha_s N_0 x}{P}\right) \quad (۱۱)$$

هم‌چنین به‌طور مشابه تابع چگالی احتمال برای متغیر تصادفی

[1] Signal to noise and distortion ratio

$\gamma_s = \frac{P|h_s|^2}{N_0}$ به‌صورت زیر محاسبه می‌گردد:

$$f_{\gamma_s}(x) = \frac{\alpha_s N_0}{P} \exp\left(-\frac{\alpha_s N_0 x}{P}\right) = \frac{d_s^{\beta} N_0}{P} \exp\left(-\frac{d_s^{\beta} N_0 x}{P}\right), \quad (۱۲)$$

۴- ارزیابی ظرفیت امن سیستم

ظرفیت کانال برای فرستنده و گیرنده اصلی سیستم یا به‌عبارت‌دیگر ظرفیت کانال بین فرستنده A و گیرنده B به‌صورت زیر محاسبه می‌گردد:

$$C_g = \log_2\left(1+SNDR_g\right) = \log_2\left(1+\frac{\gamma_s}{\gamma_s\left(k_s^2+k_b^2\right)+1}\right). \quad (۱۳)$$

همان‌طور که در مقدمه بیان شد به‌منظور ارسال امن اطلاعات در انتقال بی‌سیم در سیستمی با یک گیرنده اصلی و یک گیرنده شنودگر باید توان لحظه‌ای کانال اصلی از توان لحظه‌ای کانال شنودگر بزرگ‌تر باشد. به‌طور مشابه برای انتقال امن اطلاعات در انتقال بی‌سیم در سیستمی با یک گیرنده اصلی و تعدادی دلخواه شنودگر باید توان لحظه‌ای کانال اصلی از تک‌تک توان لحظه‌ای کانال شنودگران بزرگ‌تر باشد یا به‌عبارت‌دیگر توان لحظه‌ای کانال اصلی از بزرگ‌ترین توان لحظه‌ای کانال شنودگر مقداری بزرگ‌تر داشته باشد؛ بنابراین ظرفیت کانال شنودگران به‌صورت زیر محاسبه خواهد شد [۱۷].

$$C_{y_i} = \log_2\left(1+\max_{i=1,..,k} SNDR_{y_i}\right) = \log_2\left(1+\frac{\gamma_{ei}^{\max}}{\gamma_{ei}^{\max}\left(k_s^2+k_i^2\right)+1}\right) \quad (۱۴)$$

به‌طوری‌که $\gamma_{ei}^{\max} = \max_{i=1,..,k} \gamma_{ei}$ و تابع توزیع تجمعی متغیر تصادفی $\gamma_{ei}^{\max}$ به‌صورت زیر محاسبه می‌گردد:

$$F_{\gamma_{ei}^{\max}}(x) = \Pr\left(\gamma_{ei}^{\max} \le x\right) = \left(F_{\gamma_{ei}}\right)^N = \left(1-\exp\left(-\frac{\alpha_i N_0 x}{P}\right)\right)^N \quad (۱۵)$$

همچنین تابع چالی احتمال متغیر تصادفی $\gamma_{ei}^{\max}$ به‌صورت زیر به دست می‌آید:

$$f_{\gamma_{ei}^{\max}}(x) = N\left(1-\exp\left(-\frac{\alpha_i N_0 x}{P}\right)\right)^{N-1} \times \left(\frac{\alpha_i N_0}{P}\right)\left(\exp\left(-\frac{\alpha_i N_0 x}{P}\right)\right) \quad (۱۶)$$

بنابراین ظرفیت امن سیستم مخابراتی بی‌سیم به‌صورت زیر خواهد بود:

$$C_s^{\text{sec}recy} = \max\left[0, C_g - C_{y_i}\right] \quad (۱۷)$$

یا به‌عبارت‌دیگر احتمال ظرفیت امن غیرصفر[1] سیستم مخابراتی به‌صورت زیر محاسبه می‌گردد:

$$P^{NSC} = \Pr\left(C_s^{\text{sec}recy} > 0\right) = \Pr\left(C_g > C_{y_i}\right) = \Pr\left(\frac{\gamma_s}{\gamma_s\left(k_s^2+k_b^2\right)+1} > \frac{\gamma_{ei}^{\max}}{\gamma_{ei}^{\max}\left(k_s^2+k_i^2\right)+1}\right) \quad (۱۸)$$

رابطه فوق را می‌توان با رابطه زیر جایگزین کرد:

$$P^{NSC} = \begin{cases} \Pr\left(\gamma_s > \frac{\gamma_{ei}^{\max}}{1+\gamma_{ei}^{\max}\left(k_i^2-k_b^2\right)}\right) & ;if \quad k_i^2 > k_b^2 \\ \Pr\left(\gamma_{ei}^{\max} > \frac{\gamma_s}{1+\gamma_s\left(k_b^2-k_i^2\right)}\right) & ;if \quad k_i^2 < k_b^2 \\ \Pr\left(\gamma_s > \gamma_{ei}^{\max}\right) & ;if \quad k_i^2 = k_b^2 \end{cases} \quad (۱۹)$$

بنابراین رابطه P^{NSC} را می‌توان با توجه به میزان نارسایی سخت‌افزاری غیرایدئال در گیرنده اصلی و گیرنده‌های شنودگران به سه حالت زیر تقسیم کرد:

الف) $k_i^2 > k_b^2$

ب) $k_i^2 < k_b^2$

ج) $k_i^2 = k_b^2$

حالت اول: الف) $k_i^2 > k_b^2$

در این حالت، با توجه به غیرایدئال بودن سخت‌افزارها فرض می‌گردد مقدار نارسایی سخت‌افزاری در گیرنده‌های شنودگران از مقدار نارسایی سخت‌افزاری در گیرنده اصلی بیشتر است یا به‌عبارت‌دیگر سخت‌افزار گیرنده اصلی از سخت‌افزار گیرنده‌های شنودگران بهتر هست. در این حالت گیرنده اصلی می‌تواند در حکم یک ایستگاه مرکزی عمل کند درحالی‌که شنودگران در

[1] Probability of Non-Zero Secrecy Capacity

حکم کاربر سیار عمل کنند؛ بنابراین با فرض $\gamma_s = Y$ و $\gamma_{ei}^{\max} = X$ احتمال ظرفیت امن غیرصفر به‌صورت زیر خلاصه می‌گردد:

$$\begin{aligned} P^{NSC} &= \int_0^{\infty}\int_{\frac{x}{1+x\left(k_i^2-k_b^2\right)}}^{\infty} f_{XY}\left(x,y\right)dy\ dx \\ &= \int_0^{\infty}\int_{\frac{x}{1+x\left(k_i^2-k_b^2\right)}}^{\infty} f_X\left(x\right)f_Y\left(y\right)dy\ dx \\ &= \int_0^{\infty}\left(\int_{\frac{x}{1+x\left(k_i^2-k_b^2\right)}}^{\infty} f_Y\left(y\right)dy\right)f_X\left(x\right)dx \\ &= \int_0^{\infty}\left[F_Y\left(\infty\right)-F_Y\left(\frac{x}{1+x\left(k_i^2-k_b^2\right)}\right)\right]f_X\left(x\right)dx \\ &= \int_0^{\infty}\left[1-F_Y\left(\frac{x}{1+x\left(k_i^2-k_b^2\right)}\right)\right]f_X\left(x\right)dx \end{aligned} \quad (۲۰)$$

حالت دوم: ب) $k_i^2 < k_b^2$

در این حالت، با توجه به غیرایدئال بودن سخت‌افزارها فرض می‌گردد مقدار نارسایی سخت‌افزاری در گیرنده اصلی (ایستگاه پایه) از مقدار نارسایی سخت‌افزاری در گیرنده‌های شنودگران (کاربران متحرک) بیشتر است یا به‌عبارت‌دیگر سخت‌افزار گیرنده‌های شنودگران از سخت‌افزار گیرنده اصلی بهتر هستند؛ بنابراین با فرض $\gamma_s = Y$ و $\gamma_{ei}^{\max} = X$ احتمال ظرفیت امن غیرصفر به‌صورت زیر خلاصه می‌گردد:

$$\begin{aligned} P^{NSC} &= \int_0^{\infty}\int_0^{\frac{y}{1+y\left(k_b^2-k_i^2\right)}} f_{XY}\left(x,y\right)dx\ dy \\ &= \int_0^{\infty}\int_0^{\frac{y}{1+y\left(k_b^2-k_i^2\right)}} f_X\left(x\right)f_Y\left(y\right)dx\ dy \\ &= \int_0^{\infty}\left(\int_0^{\frac{y}{1+y\left(k_b^2-k_i^2\right)}} f_X\left(x\right)dx\right)f_Y\left(y\right)dy \\ &= \int_0^{\infty}\left[F_X\left(\frac{y}{1+y\left(k_b^2-k_i^2\right)}\right)-F_x\left(0\right)\right]f_Y\left(y\right)dy \\ &= \int_0^{\infty}\left[F_X\left(\frac{y}{1+y\left(k_b^2-k_i^2\right)}\right)\right]f_Y\left(y\right)dy \end{aligned} \quad (۲۱)$$

حالت سوم: ج) $k_i^2 = k_b^2$

در این حالت سخت‌افزار شنودگران و گیرنده اصلی به لحاظ نارسایی سخت‌افزاری در حالت یکسان قرار دارند. با فرض $\gamma_s = Y$ و $\gamma_{ei}^{\max} = X$ احتمال ظرفیت امن غیرصفر به‌صورت زیر خلاصه می‌گردد:

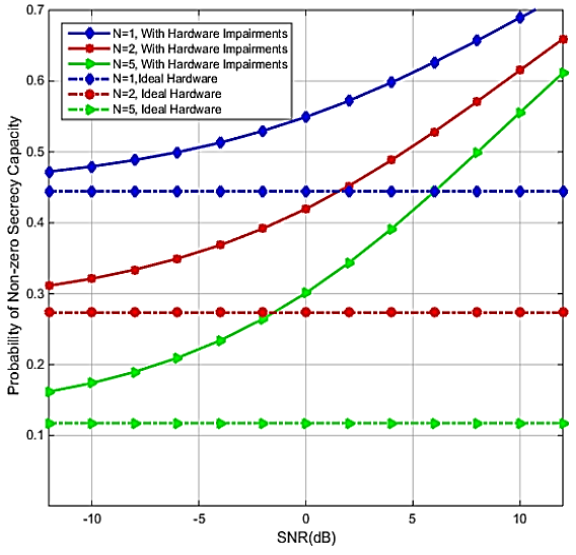
$$\begin{aligned} P^{NSC} &= \int_0^{\infty}\left[F_X\left(y\right)\right]f_Y\left(y\right)dy \\ &= \int_0^{\infty}\left[1-F_Y\left(x\right)\right]f_X\left(x\right)dx \end{aligned} \quad (۲۲)$$

به‌طوری‌که در روابط بالا $F_{\gamma_s}(.)$ و $f_{\gamma_{ei}^{\max}}(.)$ قبلاً معرفی شدند.

۴-شبیه‌سازی

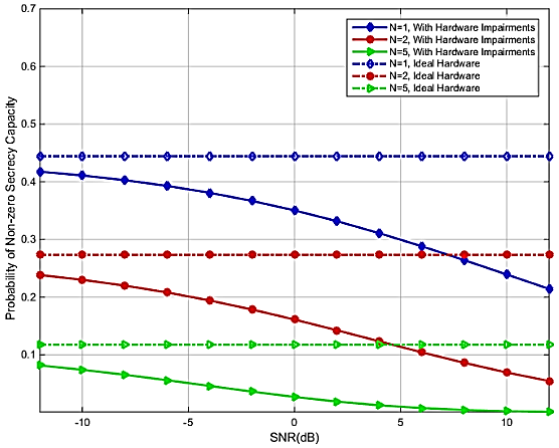
در این بخش، شبیه‌سازی مونت‌کارلو[1] به‌منظور تائید روابط ریاضی مدنظر است. در تمامی شبیه‌سازی‌ها مقدار افت مسیر β برابر با ۳ فرض می‌گردد.

شکل شماره (۱)، احتمال امن غیرصفر برحسب سیگنال به نویز (دسی‌بل) را نشان می‌دهد به‌طوری‌که نارسایی سخت‌افزار موجود در شنودگران بیشتر از نارسایی سخت‌افزاری موجود در فرستنده سیگنال است. مشاهده می‌گردد با افزایش تعداد شنودگران به‌ازای سیگنال به نویزهای بالا، مقدار احتمال امن غیرصفر به سمت یکدیگر میل می‌کنند. همچنین در سیگنال به نویزهای پایین با افزایش تعداد شنودگران احتمال امن غیرصفر کاهش می‌یابد. همچنین مقادیر احتمال امن غیرصفر به ازای تعداد ۱، ۲ و ۵ شنودگر در دو حالت سخت‌افزار ایدئال (نارسایی سخت‌افزاری صفر) و وجود نارسایی سخت‌افزاری مقایسه شده است.



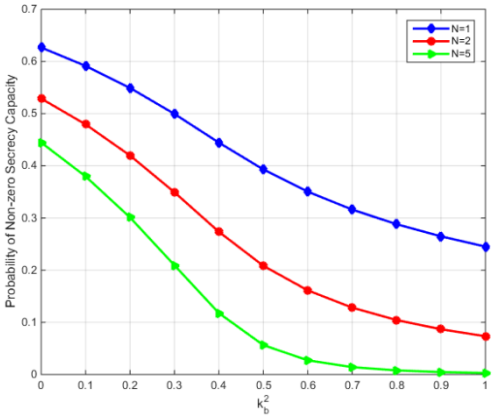
شکل (۱). احتمال امن غیرصفر برحسب سیگنال به نویز (دسی‌بل) به ازای $N = 1,2,5$ شنودگر با $k_b^2 = \mathbf{0.2}, k_i^2 = \mathbf{0.4}, \alpha_s = \mathbf{0.5}, \alpha_i = \mathbf{0.4}$.

[1] Monte-Carlo



شکل (۲). احتمال امن غیرصفر برحسب سیگنال به نویز (دسی‌بل) به ازای $N=1,2,5$ شنودگر با $k_b^2=\mathbf{0.4}, k_i^2=\mathbf{0.2}, \alpha_s=\mathbf{0.5}, \alpha_i=\mathbf{0.4}$.

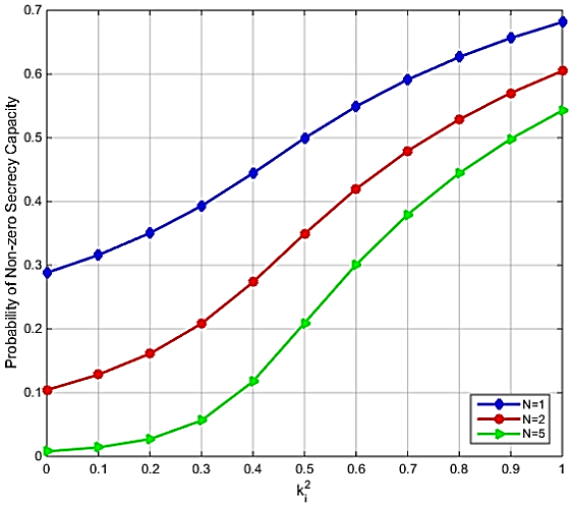
شکل شماره (۲)، بیان‌گر احتمال امن غیرصفر برحسب سیگنال به نویز (دسی‌بل) است. به‌طوری‌که نارسایی سخت‌افزار موجود در شنودگران کمتر از نارسایی سخت‌افزاری موجود در فرستنده سیگنال است. مشاهده می‌گردد با افزایش تعداد شنودگران به ازای سیگنال به نویزهای بالا، مقدار احتمال امن غیرصفر به سمت صفر میل می‌کند. همچنین در سیگنال به نویزهای پایین با افزایش تعداد شنودگران احتمال امن غیرصفر کاهش میابد. همچنین مقادیر احتمال امن غیرصفر به ازای تعداد ۱، ۲ و ۵ شنودگر در دو حالت سخت‌افزار ایدئال (نارسایی سخت‌افزاری صفر) و وجود نارسایی سخت‌افزاری مقایسه شده است.



شکل (۳). احتمال امن غیرصفر برحسب نارسایی سخت‌افزار در فرستنده k_b^2 به ازای $N=1,2,5$ شنودگر با $k_i^2=\mathbf{0.4}, \alpha_i=\mathbf{0.4}, \alpha_s=\mathbf{0.5}, SNR=\mathbf{0}dB$.

شکل شماره (۳)، بیان‌گر احتمال امن غیرصفر برحسب نارسایی سخت‌افزار موجود در فرستنده را نشان می‌دهد. به‌طوری‌که نارسایی سخت‌افزار موجود در شنودگران برابر با ۰/۴ فرض می‌گردد. مشاهده می‌گردد با افزایش تعداد شنودگران به ازای سیگنال به نویزهای بالا، مقدار احتمال امن غیرصفر به سمت صفر میل می‌کند.

شکل شماره (۴)، بیان‌گر احتمال امن غیرصفر برحسب نارسایی سخت‌افزار موجود در شنودگران را نشان می‌دهد. به‌طوری‌که نارسایی سخت‌افزار موجود در شنودگران برابر با ۰/۴ فرض می‌گردد. مشاهده می‌گردد با افزایش تعداد شنودگران به ازای سیگنال به نویزهای بالا، مقدار احتمال امن غیرصفر به سمت یک میل می‌کند.



شکل (۴). احتمال امن غیرصفر برحسب نارسایی سخت‌افزار در شنودگر k_i^2 به ازای $N=1,2,5$ شنودگر با $k_b^2=\mathbf{0.4}, \alpha_i=\mathbf{0.4}, \alpha_s=\mathbf{0.5}, SNR=\mathbf{0}dB$

۵- نتیجه‌گیری

در این مقاله، تأثیر نارسایی سخت‌افزاری بر روی امنیت لایه فیزیکی (ظرفیت امن غیرصفر) در شبکه‌های اینترنت اشیا با حضور تعدادی دلخواه شنودگر را بررسی کردیم. نتایج بررسی به شرح زیر است:

الف) به دست آوردن رابطه ریاضی برای ظرفیت امن غیرصفر در حالت‌های مختلف $k_i^2=k_b^2$ و $k_i^2 => k_b^2$ و $k_i^2 <= k_b^2$.

ب) عملکرد سیستم با مقدار نارسایی سخت‌افزاری کم در فرستنده و مقصد و مقدار نارسایی سخت‌افزاری زیاد در شنودگران به‌شدت کاهش می‌یابد.

ج) اگر مقدار نارسایی سخت‌افزاری در فرستنده و شنودگران با هم برابر باشد مقدار احتمال امن غیرصفر به مقدار سیگنال به نویز و همچنین مقدار نارسایی سخت‌افزاری در فرستنده، گیرنده و شنودگران بستگی ندارد و مقداری ثابت است.

۶- مراجع

[1] H. Ning, F. Farha, Z. N. Mohammad & M. Daneshmand, "A Survey and Tutorial on "Connection Exploding Meets Efficient Communication" in the Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 11, pp. 10733-10744, Nov. 2020.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal & B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019.

[3] C. H. Liao, H. -H. Shuai & L. C. Wang, "Eavesdropping prevention for heterogeneous Internet of Things systems," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1-2, 2018.

[4] S. A. Mohajeran & G. A. Hodtani, "Power Allocation for Wireless Sensor Networks in the Presence of Non-Gaussian Noise and Hardware Impairments Using Distance-Related Bounds," in IEEE Sensors Letters, vol. 5, no. 4, pp. 1-4, April 2021.

[5] G. Ding, X. Gao, Z. Xue, Y. Wu & Q. Shi, "Massive MIMO for Distributed Detection With Transceiver Impairments," in IEEE Transactions on Vehicular Technology, vol. 67, no. 1, pp. 604-617, Jan. 2018.

[6] C. Mollén, U. Gustavsson, T. Eriksson & E. G. Larsson, "Impact of Spatial Filtering on Distortion From Low-Noise Amplifiers in Massive MIMO Base Stations," in IEEE Transactions on Communications, vol. 66, no. 12, pp. 6050-6067, Dec. 2018

[7] P. Williams, P. Rojas & M. Bayoumi, "Security Taxonomy in IoT – A Survey," 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 560-565, 2019.

[8] N. Sklavos & I. D. Zaharakis, "Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations," 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-2, 2016.

[9] J. Zhang, S. Rajendran, Z. Sun, R. Woods & L. Hanzo, "Physical Layer Security for the Internet of Things: Authentication and Key Generation," in IEEE Wireless Communications, vol. 26, no. 5, pp. 92-98, October 2019.

[10] Y. Chen, W. Li & H. Shu, "Wireless physical-layer security with multiple receivers and eavesdroppers: Outage probability and average secrecy capacity," 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 662-667, 2015.

[11] M. Obeed & W. Mesbah, "An efficient physical layer security algorithm for two-way relay systems," 2016 IEEE Wireless Communications and Networking Conference, pp. 1-6, 2016.

[12] A. Sonee & G. A. Hodtani, "On the Secrecy Rate Region of Multiple-Access Wiretap Channel With Noncausal Side Information," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1151-1166, June 2015.

[13] Y. Liang, H. V. Poor & S. Shamai, "Information Theoretic Security, Delft," The Netherlands: Now Publishers, 2009.

[14] T. Cover, & J. Thomas, "Elements of Information Theory," 2nd Edition, Wiley, (2006).

[15] T. T. Duy & V. N. Q. Bao, "Performance analysis of cooperativebased multi-hop transmission protocols in underlay cognitive radio with hardware impairment," VNU Journal of Computer Science and Communication Engineering, vol. 31, no. 2, pp. 15-28, 2015.

[16] J. Mo, M. Tao, & Y. Liu, "Relay placement for physical layer security: A secure connection perspective," IEEE Commun. Lett., vol. 16, no. 6, pp. 878-881, Jun. 2012.

[17] V. N. Q. Bao, N. L. Trung, & M. Debbah, "Relay selection schemes for dual-hop networks under security constraints witb multiple eavesdroppers," IEEE Trans. Wire!' Commun., vol. 12, no. 12, pp. 6076-6085, Otc. 2013.