نشریه علمی پدافند غیرعامل

سال یازدهم، شماره ۲، تابستان ۱۳۹۹، (پیاپی ۴۲): صص ۵۹-۴۵

"علمی-ترویجی"

# فناوری لای‌فای: معرفی، کاربردها، چالش‌ها و ارزیابی امنیتی آن

**سامان کشوری[۱*]، مصطفی عباسی[۲]**

تاریخ دریافت: ۱۳۹۸/۰۴/۳۰

تاریخ پذیرش: ۱۳۹۸/۰۶/۱۹

## چکیده

امروزه با گسترش اینترنت یکی از چالش‌های بزرگ شبکه‌های ارتباطی سرعت دسترسی به آن است. در هنگامی که دستگاه‌های مختلفی به شبکه بی‌سیم متصل می‌شوند سرعت دسترسی به یک چالش تبدیل می‌شود. شبکه‌های وای‌فای با مشکلاتی روبه‌رو هستند از جمله اینکه استفاده از آن‌ها در برخی مکان‌ها دشوار و یا غیر ممکن بوده و سرعت آن برای پاسخگویی به نیازهای امروزی کند است. در این مقاله ضمن معرفی لای‌فای، ویژگی‌ها و محدودیت‌های این شبکه که داده‌ها در آن از طریق نور مرئی به‌صورت بی‌سیم تبادل می‌شوند، بررسی شده است. یکی از مواردی که برای این شبکه نوین اهمیت دارد، طرز کار آن و روابط علمی و مدل‌های ریاضی تعریف شده برای آن است که در این پژوهش به آن و همچنین معماری لای‌فای پرداخته شده است. کاربردها و ایده‌های نوینی برای لای‌فای وجود دارد که در این مقاله بررسی شده‌اند. در پایان عملکرد لای‌فای مورد ارزیابی قرار گرفته شده است. این ارزیابی شامل تحلیل امنیتی و بررسی مزایا و معایب فناوری ارتباطی لای‌فای نسبت به وای‌فای است.

**کلیدواژه‌ها:** لای‌فای، امنیت لای‌فای، وای‌فای، انتقال داده

---

۱- کارشناس ارشد نرم‌افزار، دانشگاه جامع امام حسین(ع)، تهران، ایران (sakeshvari@ihu.ac.ir)- نویسنده مسئول

۲- دانشجوی دکتری جنگ الکترونیک و دفاع سایبری، دانشگاه جامع امام حسین(ع)، تهران، ایران

## ۱. مقدمه

ظهور تلفن‌های هوشمند، تبلت‌ها و وسایل مشابه دیگر، دسترسی به اطلاعات از طریق فناوری تلفن همراه را به یکی از مشخصه‌های اصلی زندگی بدل کرده است. سرعت اینترنت یکی از موضوعات مهم است و هرکسی به جهت کسب‌وکار، سازمان‌ها، کارآفرینان و مؤسسات برای دریافت اطلاعات صحیح در زمان درست و مکان درست وارد آن می‌شود [۱]. در سال ۲۰۱۷ به‌طور میانگین به ازای هر تلفن همراه، ماهانه بیش از یازده گیگابایت ترافیک داده از طریق شبکه‌های تلفن همراهی منتقل شده که این عمل منجر به محدود شدن فناوری‌های بی‌سیم مبتنی بر RF (فرکانس رادیویی) می‌شود [۲].

هنگامی‌که تعداد زیادی از کاربران به یک شبکه بی‌سیم متصل می‌شوند دسترسی نفوذگران به این سامانه‌ها ساده‌تر خواهد شد. امروزه تقاضای کاربران برای اتصال به شبکه اینترنت طیف رادیویی موجود را ناکافی می‌داند که شرکت ارتباطات بی‌سیم با در نظر گرفتن طیف رادیویی فراتر از ۱۰ گیگاهرتز به این نیاز پاسخ داده است. دلایل زیادی وجود دارند که پیوستن فناوری شبکه بی‌سیم x.۸۰۲ به IEEE ضرورت دارد [۳] انتظار می‌رود ارتباطات بی‌سیم، Wi-Fi با چالش‌های بسیاری مانند قابلیت مدیریت، سرویس مقیاس‌پذیری، ظرفیت اتصالات، هزینه بهره‌وری، در دسترس بودن، قابلیت همکاری کارایی و امنیت مواجه باشد.

شبکه‌های وای‌فای با مشکلاتی روبه‌رو هستند از جمله اینکه استفاده از آن‌ها را در برخی مکان‌ها دشوار و یا غیر ممکن است. این شبکه‌ها امنیت مناسبی ندارند، زیرا این فناوری از امواج رادیویی استفاده می‌کند. با توجه به اهمیت انتقال داده در بین سامانه‌های رایانه‌ای و تجهیزات هوشمند همواره نسل جدیدی از فناوری‌های انتقال داده مورد استفاده قرار گرفته است؛ امروزه نقش ارتباط بی‌سیم در تمامی سازمان‌ها، نهادها اعم از انتظامی، نظامی و امنیتی و حتی زندگی روزمره از اهمیت بالایی برخوردار است. نمونه‌ای از این ارتباطات شامل یک ارتباط ساده کنترل از راه دور تلویزیون، ارتباط بی‌سیم یا تلفن همراه از طریق بلوتوث، وای‌فای و انواع دیگر است. سیسکو پیش‌بینی کرده که استفاده از اینترنت تا سال ۲۰۱۹ به ۲۴/۳ اگزابایت (۱۰۱۸ بایت) در ماه برسد. از طرف دیگر تا سال ۲۰۲۰ حدود ۷/۱ میلیارد دستگاه از طریق وای‌فای به یکدیگر متصل می‌شوند. این رشد استفاده از دستگاه‌های بدون سیم تا سال ۲۰۲۵ و به وجود آمدن مفاهیمی همچون اینترنت اشیاء و داده‌های حجیم، منجر خواهد شد که وای‌فای جوابگوی این حجم از ترافیک داده‌ها نباشد.

در مسیر کشف این مسائل، دانشمندان روش جایگزینی برای ارتباطات بی‌سیم با استفاده از فناوری لای‌فای کشف کرده‌اند، جایی که داده‌ها از طریق نور مرئی منتقل می‌شود. انتقال داده‌ها در این روش از طریق روشنایی لامپ‌های LED صورت می‌گیرد. لای‌فای راه‌حلی ارزان‌تر و بسیار جذاب‌تر از وای‌فای است. لای‌فای برای تعیین محل داده به‌جای استفاده از امواج رادیویی از طیف نور قابل مشاهده استفاده می‌کند [۴] مدیر ارتباطات همراه در دانشگاه ادینبورگ (پروفسور هاس)، در کنفرانس TED Global که ۱۲ جولای ۲۰۱۱ در ادینبورگ برگزار شد، لای‌فای را ارائه داد. لای‌فای یک VLC است که شرکت سازنده آن در این مسیر مخترع را یاری کرده است [۴]. اصطلاح "Li-Fi[1]" توسط پروفسور پروفسور هاس هنگامی که یک ویدیو با کیفیت بالا از لامپ استاندارد پخش کرد و مردم را شگفت زده کرد ابداع شد [۵].

در ادامه ضمن معرفی لای‌فای، ویژگی‌ها و محدودیت‌های آن اشاره شده است. پس از آن، طرز کار این فناوری با کاربردها و ایده‌های آن بیان شده است و در پایان ضمن مقایسه لای‌فای با فناوری‌های موجود، به لحاظ امنیتی این فناوری مورد ارزیابی قرار گرفته است.

## ۲. معرفی لای‌فای

در این بخش ضمن برشمردن ویژگی‌ها، ساختار و محدودیت‌های لای‌فای، معماری این فناوری تشریح شده است.

### ۲-۱. ویژگی‌های لای‌فای

فناوری لای‌فای بخشی از طیف الکترومغناطیسی را به‌کار می‌برد که هنوز از بخش قابل مشاهده طیف استفاده زیادی نشده است. علاوه بر در دسترس بودن این نور و مضر نبودن آن فضای قابل دسترسی در این طیف ۱۰،۰۰۰ برابر بیشتر است و فقط با احتساب لامپ‌ها در استفاده، می‌توان گفت که نور ۱۰،۰۰۰ برابر بیشتر از سایر منابع در دسترس است.

لای‌فای در حال حاضر بخشی از ارتباطات نور قابل مشاهده (VLC) استاندارد PAN IEEE 802.15.7 است. فناوری وفاداری نور یک فناوری است که در سال‌های اخیر به دلیل توانایی به‌دست آوردن Multiplexing بالا یا ترکیب هزاران منبع داده به‌عنوان خروجی مورد توجه قرار گرفته است. فناوری لای‌فای یک شبکه رایانه‌ای بی‌سیم محلی است که دستگاه‌های

1- light – Fidelity (به معنی تطابق با نور)

الکترونیکی را به شبکه متصل می‌کند که عمدتاً با باندهای UHF ۲/۵ گیگاهرتز (۱۲ سانتی‌متر) و ۵ گیگاهرتز (۶ سانتی‌متر) نوارهای SHF کار می‌کند. آن‌ها بر اساس استاندارد مؤسسه مهندسان برق و الکترونیک (IEEE) ۸۰۲,۱۱ می‌باشند. رایانه‌ها و گوشی‌هایی که با استفاده از این فناوری فعال شده‌اند از موج رادیویی برای ارسال و دریافت داده در محدوده یک ایستگاه پایه استفاده می‌کنند و انتقال در این کانال‌ها توسط تمام ایستگاه‌های موجود در محدوده دریافت می‌شود. یک نقطه دسترسی بی‌سیم عمومی با استفاده از g۸۰۲,۱۱ یا b۸۰۲,۱۱ با یک آنتن موجود ممکن است محدوده ۳۰ متر در داخل و ۱۱۰ متر خارج از منزل داشته باشد. به‌رغم آن، IEEE n۸۰۲,۱۱ [۶] می‌تواند دارای بیش از دو برابر برد باشد که با باند فرکانس تغییر می‌کند. در آینده به علت کمبود منابع فرکانس رادیو سامانه‌های ارتباطی بی‌سیم، به‌عنوان مثال G ۳، G ۴ با مشکل روبه‌رو خواهند شد. این انسداد در پهنای باند نمی‌تواند رشد تقاضا برای نرخ داده تعداد زیادی از سامانه‌های ارتباطی بالا را پشتیبانی کند. با این وجود، زمانی که از فرکانس بالا برای انتقال داده استفاده شود، تراکم طیف کاهش می‌یابد اما این راه‌حل قابل قبولی نیست، زیرا این بخش از طیف نیازمند تجهیزات پیچیده است و سامانه‌هایی با هزینه‌های بالا را باعث می‌شود. همچنین تخصیص طیف و محدودیت عملیاتی در سراسر جهان سازگار نیست؛ بنابراین، ۸۰۲,۱۱ b و ۸۰۲,۱۱ g از طیف ۲/۴ گیگاهرتز استفاده می‌کند که با سایر دستگاه‌ها سازگار است[۳]. بالاترین سرعتی که فناوری لای‌فای ثبت کرده، میزان ۱۰ گیگابیت بر ثانیه است. این فناوری تجاری در چین وجود دارد که سرعت ۱۵۰ مگابیت بر ثانیه را ارائه داده که ۱۰ برابر سریع‌تر از میانگین سرعت اتصال‌های بدون سیم در کشوری مثل بریتانیا است[۱].

## ۲-۲. محدودیت‌های لای‌فای

یکی از محدودیت‌های لای‌فای، مصرف انرژی است که در آن عمر باتری و حرارت از اهمیت بالایی برخوردار است [۴]. یکی دیگر از این محدودیت‌ها، محدودیت لاین آف سایت[۲] یا محدودیت در دید بودن است، بدین معنی که برای انتقال داده باید گیرنده و فرستنده داده در دید هم قرار داشته باشند. یکی از محدودیت‌های این روش کاهش کارایی آن در محیط‌هایی است که دارای پنجره است بنابراین برای افزایش کارایی باید در محیط‌هایی به‌کار برده شود که کمترین پنجره را داشته یا هیچ پنجره‌ای در آن نباشد. در محیط‌های دارای پنجره نیز محدودیت وجود دارد زیرا اشعه‌های نور خورشید در آن ایجاد اختلال می‌کنند و انتقال داده را مختل می‌سازند. یکی دیگر از محدودیت‌های لای‌فای، عدم استفاده در محیط باز است؛ بنابراین، امکان استفاده از لای‌فای توسط کسی که وارد محیط خارجی می‌شود، وجود ندارد. علاوه بر این نور کم می‌تواند منجر به ایجاد اختلال در انتقال داده شود که در زمان نوسانات جریان برق، امکان بروز چنین اشکالی امکان‌پذیر است. از دیگر موارد محدودیت لای‌فای، نیاز به نور در تمام ساعات روز است.

برای پوشش‌دهی کاربران بیشتر و ترافیک داده بالاتر چندین راه‌حل نویدبخش پیشنهاد شده است که در سه گروه طبقه‌بندی می‌شوند [۷]:

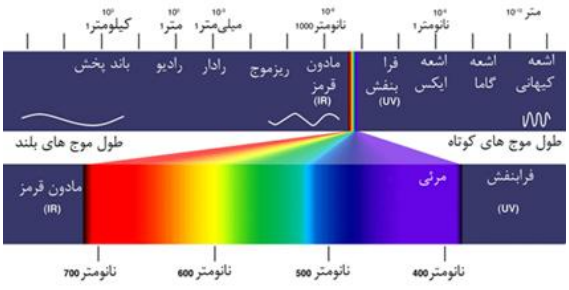
۱) کشف منابع فضایی (مکانی) برای بهبود به‌کارگیری طیف؛

۲) تأسیس شبکه‌های ناهمگن (HetNet) با سلول‌های کوچک برای استفاده مجدد از پهنای باند؛

۳) جست‌وجوی منابع طیفی در دسترس‌تر از قبیل امواج میلی‌متری یا پهنای باند بی‌سیم نوری.

## ۳. طرز کار فناوری لای‌فای

در امواج الکترومغناطیسی، هر چه طول موج کوتاه‌تر باشد، نفوذ کاهش پیدا کرده و در مقابل مقدار داده‌ای که می‌توان منتقل کرد، بیشتر می‌شود. همان‌طور که در شکل (۱) مشاهده می‌شود، امواج رادیویی برد بسیار بالایی دارند اما از نظر سرعت انتقال داده، وضعیت خوبی ندارند.




**شکل (۱):** طیف‌های الکترومغناطیسی[۳]

هاس معتقد است امواج رادیویی که در حال حاضر برای انتقال داده‌ها استفاده می‌شوند کارایی لازم را ندارند و مدعی شده با جایگزین کردن مدل‌های قدیمی تابان با حباب‌های LED،

۱- مجله دانستنی‌ها - ۳۰ آبان ۱۳۹۴ - ص ۸۳

2- Line of Sight

3- Tebyan.net

می‌تواند تمام آن‌ها را به فرستنده‌های اینترنتی تبدیل کند. این ابداع که «دی‌لایت (D-Light)» نام دارد می‌تواند اطلاعات را با تغییر فرکانس نور محیطی در اتاق، سریع‌تر از ۱۰ مگابایت در ثانیه که سرعت معمول اتصال باند پهن است، بفرستد. بدین ترتیب نسل بعدی اینترنت بی‌سیم می‌تواند از لامپ‌های حبابی (LED) به‌جای پهنای باند استفاده و سرعت انتقال داده‌ها را تا ۲۵۰ برابر سریع‌تر کند.

برای انتقال داده نمی‌توان از لامپ‌های LED موجود استفاده کرد و به لامپ‌های جدیدی نیاز است اما انتقال داده با پروتکلی مثل وای‌فای ac۸۰۲,۱۱ امکان‌پذیر است. در حقیقت پالس‌های نور داده را به زبان خاص خود، منتقل می‌کنند و برای ایجاد پالس، به مدارات و کنترل کننده خاص نیاز است. فرستنده و گیرنده مادون قرمز که ممکن است گوشی و تبلت باشد هم به سخت‌افزار خاص و جدیدی نیاز دارد. نام دقیق حسگر مورد نیاز، حسگرنوری[1] یا آشکارساز نوری[2] است. فتودیتکتور حسگری است که نور را اصطلاحاً خوانده و تشخیص می‌دهد. در گوشی‌ها و تبلت‌ها، حسگر نور محیط کاملاً متداول شده است، می‌توان به‌جای این حسگر، فتودیتکتر را تعبیه کرد که پیشرفته‌تر و چند منظوره است.

هزینه ایجاد این فناوری در حال حاضر بالا بوده اما مدیران یک شرکت فرانسوی[3] فعال در این زمینه قول مساعد برای کاهش هزینه‌های آن را داده‌اند. آن‌ها مدعی ارائه این نوع از فناوری شبکه با هزینه‌ای کمتر از ۸۰ یورو در آینده نزدیک هستند. با افزایش تقاضا برای داده‌های بی‌سیم و کمبود طیف رادیویی و مسائل آلودگی الکترومغناطیسی آن، به نظر می‌رسد لای‌فای جایگزین سالم‌تر، ارزان‌تر و کم‌خطرتر نسبت به وای‌فای است.

همان‌طور که گفته شد، این سامانه از ارتباطات نور مرئی میان ۴۰۰ و ۸۰۰ تراهرتز برای انتقال پیام‌ها در کد دودویی استفاده می‌کند که باعث می‌شود سرعت این سامانه آن‌قدر زیاد شود که در هر ثانیه بتوان ۱۸ فیلم سینمایی ۱/۵ گیگاباتی را دانلود کرد.

برای استفاده از این فناوری، باید یک مسیریاب مخصوص لای‌فای در اختیار باشد. انتقال اطلاعات با استفاده از این روش مبتنی بر نور است؛ اما باید توجه داشت که امواج نوری نامرئی هستند و آلودگی نوری ایجاد نمی‌کنند. بهترین مثال درباره نحوه کارکرد لای‌فای، کنترل تلویزیون است. درون کنترل تلویزیون دیود فرستنده نوری وجود دارد و در مدار تلویزیون دیود گیرنده نوری وجود دارد. زمانی که دکمه‌ای از کنترل فشار داده می‌شود، کد مخصوص آن دکمه توسط سیگنال مادون قرمز به سمت تلویزیون ساطع شده و در مدار داخلی تلویزیون، کد مورد نظر رمزگشایی و پردازش می‌شود. در فناوری لای‌فای نیز چنین، فرایندی استفاده می‌شود. مطابق با شکل (۱) لامپ‌های LED مخصوصی طراحی شده که شامل کنترل کننده و تغذیه کننده هستند و اطلاعات از اینترنت، از طریق سیم یا بی‌سیم به این لامپ‌ها فرستاده می‌شوند، این داده‌ها توسط مدار کنترلی پردازش شده و از طریق نور لامپ به ماژول گیرنده نوری ارسال می‌شوند. ماژول نوری ممکن است روی دستگاه نصب شده یا همچون حافظه فلش به‌صورت خارجی به دستگاه متصل شود. اگر ماژول نوری به‌صورت جداگانه استفاده شود، همچون فلشی که دارای گیرنده نوری است به وسیله مبدل ارتباطی به تلفن همراه، لپ‌تاپ یا وسایل دیجیتالی دیگر متصل می‌شود. نور دریافتی حسگر نوری، توسط مدارات داخلی ماژول، تقویت و پردازش شده و به‌صورت داده استفاده می‌شوند. با فناوری ساخت فعلی لامپ‌های LED می‌توان با اضافه کردن امکاناتی، لای‌فای را پیاده‌سازی کرد.

لای‌فای اطلاعات را با خاموش و روشن شدن نور یک لامپ LED که سرعت آن بیشتر از دید بشر است جابه‌جا می‌کند [۸] که دامنه وسیعی از طول موج ۳۸۰ تا ۷۵۰ نانومتر را پوشش می‌دهد. در مقاله نگدو و همکارانش [۹] یک روش انتقال بدون خطا با استفاده از لامپ LED ارائه شده است. تنظیم و استفاده از لای‌فای برای تبادلات می‌تواند به‌عنوان بخشی از موقعیت‌های اساسی، مانند ماشین‌های پرواز یا مراکز درمانی مورد استفاده قرار بگیرد. جایی که برای حفظ قوانین فاصله‌ای استراتژیک و اساسی انتقال‌های مبتنی بر فرکانس (RF) به‌طور کامل رد شده‌اند.

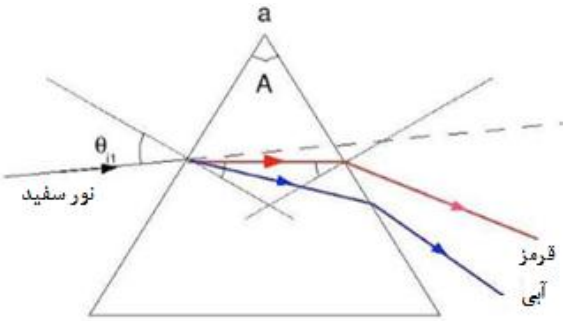
در مقاله تایناماتان و همکارانش [۱۰] پیشنهادی ارائه شده است که در آن اشعه‌های نور، با استفاده از منشور جدا شده است. آن‌ها برای محافظت از اطلاعات در صنعت فقط هفت رنگ مختلف را استفاده کرده‌اند. با توجه به فناوری نور ممکن است تغییرات ایجاد شده در رنگ، فرکانس را مقدار بسیار کوچکی افزایش دهد. برای محاسبه انرژی (E) از معادله ساده‌ای استفاده کرده‌اند، که در آن E برابر انرژی و h یک مقدار ثابت برابر $6.63\times10^{-34}$ J و f فرکانس نور است [۱۰].

$$E = hf \qquad (1)$$

سرعت چراغ‌های رنگی خلأ ثابت است. تغییر سرعت نور با توجه به رنگ به علت انحراف شاخص منشور و مواد آن ناهمسان است. برای تغییر سرعت نور عواملی مانند زاویه نور، اشعه‌های ورودی و انتشار امواج مهم هستند.

1- Photo Sensor
2- Photo Detector
3- OLDCOM

همان‌طور که در شکل (۲) نشان داده شده است می‌توان هنگام انتقال اطلاعات، رنگ‌های مختلف نور را در مرکز داده استفاده کرد. هنگامی که ما از رنگ‌های مختلف استفاده می‌شود به‌طور تصادفی می‌توان راه‌حل‌های امنیتی سایبری، انتقال و ذخیره‌سازی را افزایش داد. در این پژوهش نشان داده شده است که استفاده از منشور برای تجزیه و تحلیل راه‌حل‌های امنیتی سایبری بر اساس فناوری لای‌فای مفید است. الگوریتم جدید تغییر زاویه نور است که بستگی به زاویه منشور دارد [۱۰].




**شکل (۲)**: انتقال داده با فرکانس مختلف [۱۰]

## ۳-۱. روابط علمی و مدل‌های ریاضی لای‌فای

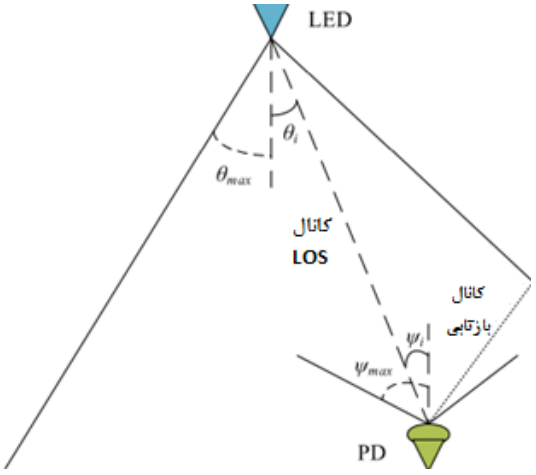
در یک سامانه VLC معمولی، از سقف تعداد لامپ‌های LED برای انتقال داده به گیرنده که روی یک سطح، در فضایی محصور شده قرار دارند، استفاده می‌شود. روشنایی در هر نقطه از سطح دریافت شامل خط دید (LOS) از LED به‌علاوه سهم بازتاب از دیواره‌ها و اشیای درون فضاست. حباب‌های LED معمولی برای ایجاد روشنایی بهینه داخلی، قادر به رسیدن به شدت روشنایی ۴۰۰ لوکس بر واحد سطح هستند. مقادیر این‌چنینی نور، برای انتقال داده با نسبت سیگنال به نور (SNR) بیشتر از ۶۰ دسی‌بل، بر خط دید (LOS) نوری کانال کافی هستند؛ بنابراین حاصل نهایی VLC داخلی کانال متشکل از مقادیر منتشر شده ($H_{DIFF}$) و خط دید (HLOS) LOS است. پاسخ فراکنشی کانال به‌صورت معادله (۲) محاسبه می‌شود [۳۳]:

$$H(f) = \sum_i \eta_{LOS,i} EXP(-j2\pi f \Delta\tau LOS,i) + \eta_{DIFF} \frac{EXP(-j2\pi f \Delta\tau LOS,i)}{1+if/f_0} \quad (۲)$$

در این معادله، $i$ برابر است با مسیرهای خط دید (LOS)، $\eta_{LOS}$ و $\eta_{DIFF}$ بیانگر بهره کانال برای LOS و مسیر انتشار هستند. LOS $\Delta\tau$ و $\Delta\tau_{DIFF}$ به ترتیب نشانگر تأخیر مربوطه هستند و $f_0$ برابر است با بسامد قطع کانال متراکم شده. میزان بهره‌های خط دید LOS و کانال منتشر شده از معادله (۳) به‌دست می‌آید [۳۳].

$$\eta_{LOS,i} = \begin{cases} A_R(m+1)COS^m\theta_i COS\psi_i/(2\pi r_i^2) & \psi_i \le \psi_{max} \\ 0 & otherwise \end{cases}$$
$$and,$$
$$\eta_{DIFF} = \frac{A_R}{A_{Room}} \frac{\rho}{1-\rho} \quad (۳)$$

که در آن، $A_R$ و $A_{Room}$ به ترتیب مساحت گیرنده نوری و مکان هستند. $\theta_i$ بیان‌گر زاویه پرتابش بر حسب محور فرستنده است. $\psi_i$ نشان دهنده زاویه بروز نسبت به زاویه گیرنده است. $\psi_{max}$ برابر است با نیم زاویه میدان دید گیرنده ((FOV. $r_i$ عبارت است از فاصله بین n امین فرستنده و n امین گیرنده. M شاخص Lamber است که به $\theta_{max}$ نیم زاویه تابشی منبع بستگی دارد زیرا: $\rho(\cos.m= -l/\log_2 \theta_{max})$ بیانگر میانگین انعکاس است، در واقع کمیتی است که برای فضای درونی مفروض می‌شود. نمای شماتیک کانال بی‌سیم نوری داخلی در شکل (۳) نشان داده شده است. اگر موقعیت ایده آلی را با فرض وجود بازتابنده‌های لامبرتین[1] و $\rho = 1$ در نظر بگیرید، قدرت نوری اولین مرتبه بازتاب‌ها تقریباً بیش از ۱۰۰ دسی‌بل از مقدار افت مسیر انتقال خط دید (LOS) کوچک‌تر است. به این دلیل که افت مسیر در بازتاب‌های مربوط به مرتبه‌های بالاتر از این مقادیر هم بیشتر است، می‌توان از اثرات مسیرهای پراکنده چشم‌پوشی کرد؛ بنابراین اگر آشکارسازهای نوری مربوط به فرستنده LED متقارن باشند، کانال‌های VLC به قوت خود همبسته باقی می‌مانند. در هر حال، این بدترین سناریو برای ایجاد شبکه بی‌سیم است و یک مشخصه کاملاً متمایز نسبت به کانال RF به‌حساب می‌آید.




**شکل (۳)**: طرح شماتیک از مدل بی‌سیم نوری [۳۳]

## ۳-۲. کاربردها و ایده‌های تعریف شده برای لای‌فای

فناوری لای‌فای می‌تواند کاربرد گسترده‌ای پیدا کند. لای‌فای برای انواع زمینه‌ها به ویژه برای برنامه‌های مصرف محتوای

1- Lambertin

اینترنتی محبوب مانند دانلود فیلم و صدا، جریان مستقیم بسیاری مناسب است. این برنامه‌ها تقاضای زیاد برای پهنای باند downlink دارند اما به حداقل ظرفیت uplink [۱۱ و ۱۲] نیاز دارند. یک بحث مفصل از برنامه‌های مختلف آن در زیر آمده است:

- روشنایی هوشمند: نورپردازی خصوصی یا عمومی از جمله چراغ‌های خیابانی، برای به ارمغان آوردن نقاط دسترسی لای‌فای و همان ارتباطات و زیرساخت حسگر و همچنین می‌تواند برای نظارت و کنترل روشنایی و داده‌ها استفاده شود.
- اتصال تلفن همراه: با استفاده از لای‌فای. تلفن‌های هوشمند، لپ‌تاپ‌ها و دیگر دستگاه‌های تلفن همراه می‌توانند به‌طور مستقیم اتصال داشته باشند. لای‌فای استفاده از لینک‌های کوتاه برد با نرخ داده بسیار بالا و همچنین امنیت را فراهم می‌کند.
- اجتناب از فرکانس‌های رادیویی: حساسیت به فرکانس‌های رادیویی موجب شده تا محققان به دنبال جایگزینی همچون لای‌فای برای RF باشند.
- خدمات مبتنی بر مکان (LBS): اطلاعات فوق‌العاده دقیق مکان خاص خدمات اطلاعاتی مانند تبلیغات و ناوبری که گیرنده را قادر می‌سازد تا اطلاعات را به موقع و در محل درست دریافت کند [۱۳].
- امداد طیف رادیویی: نیازهای اضافی ظرفیت از شبکه‌های تلفن همراه می‌تواند در جایی که شبکه‌های لای‌فای در دسترس است تخلیه شود. این عملاً در downlink که در آن تنگناهایی بروز پیدا کرده مؤثر است.
- آموزش از طریق لای‌فای: این فناوری یک فناوری پیشرو است که سرعت دسترسی به اینترنت را بهتر می‌کند و پهنای باند بالایی دارد، درنتیجه، مؤسسات آموزشی و سازمان‌ها می‌توانند از این فناوری برای دسترسی به اینترنت با سرعت بالا برای کنفرانس ویدئویی، دریافت آموزش دیجیتال و یادگیری آنلاین استفاده کنند.
- مدیریت بحران: به کمک لای‌فای می‌توان در زمان فاجعه طبیعی مانند زمین‌لرزه، سونامی یا طوفان ارتباطات را برقرار کرد.
- لامپ‌های لای‌فای می‌توانند در خیابان‌ها برای فراهم آوردن نور ثابت شوند و دسترسی به اینترنت با سرعت بالا در هر یک گوشه‌ای از خیابان را فراهم کنند.
- محیط‌های خطرناک لای‌فای: امن است و جایگزینی برای تداخل الکترومغناطیسی از رادیو است. نیروگاه‌ها نیازمند سامانه انتقال داده با سرعت بالا هستند. تجهیزات مربوط به وای‌فای برای تجهیزات حساس به دلیل تشعشاتی که دارند مضر هستند از این رو فناوری لای‌فای می‌تواند برای تجهیزات حساس مانند نیروگاه‌های تولید برق و نیروگاه‌های هسته‌ای مفید باشند. همچنین اماکنی مانند کارخانه‌های تولید مواد شیمیایی و نفتی و پتروشیمی بهترین مکان‌هایی هستند که امکان به‌کارگیری لای‌فای برای آن‌ها وجود دارد.
- بیمارستان و بهداشت و درمان: لای‌فای هیچ تداخلی چه از نوع الکترومغناطیسی و غیره با ابزار پزشکی و اسکنرهای MRI ندارد. استفاده از وای‌فای به دلیل تداخلات رادیویی در اتاق عمل بیمارستان ممنوع است. وای‌فای در کار تجهیزات مانیتورینگ دستگاه‌ها و تجهیزات پزشکی داخل اتاق عمل اختلال ایجاد می‌کند و بنابراین خطرناک است. برای غلبه بر این مشکل برای دسترسی به اینترنت در اطلاق عملی و کنترل تجهیزات پزشکی می‌توان از لای‌فای استفاده کرد. همچنین برای جراحی‌های از راه دور و جراحی به وسیله ربات و سایر فرایندهای جراحی خودکار می‌توان از این فناوری استفاده کرد.
- حمل‌ونقل هوایی: از لای‌فای می‌توان برای کاهش وزن، کابل‌کشی و اضافه کردن قابلیت تغذیه در طرح‌بندی کابین‌های هواپیما [۱۴] که در آن‌ها چراغ‌های LED از پیش مستقر هستند استفاده کرد. به کمک لای‌فای می‌توان با دستگاه‌های تلفن همراه خود مسافر سرگرمی پرواز (IFE) را پشتیبانی و یکپارچه نمود.
- کنسول‌های بازی: قرار دادن حسگرها بر روی یک تلویزیون برای دریافت اطلاعات از کنسول‌های بازی یک ایده مدرن است [۱۳]. به این صورت که اجازه می‌دهد یک واحد در داخل اتاق تا زمانی که خط مستقیمی برای دید حسگر وجود دارد جابه‌جا شود.
- ارتباطات زیر آب: با توجه به آنکه جذب سیگنال در آب قوی است، مصرف RF نامناسب است. امواج صوتی پهنای باند کمتری دارند و لای‌فای یک راه‌حل برای نابود ساختن ارتباطات کوتاه مدت زندگی دریایی است [۱۵ و ۱۶].

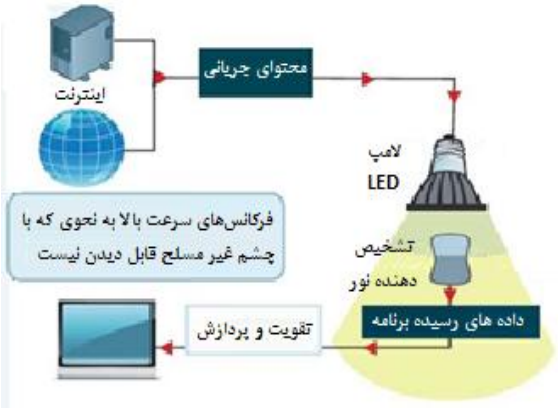
تجهیزات موجود در زیر دریا در مورد استفاده از وای‌فای با قطعی مکرر روبه‌رو هستند. استفاده از فناوری لای‌فای این قطعی را از بین ببرد. این تجهیزات با استفاده از لامپ‌های تحت عنوان هد لامپ قادر به برقراری ارتباط با تجهیزات بالای آب هستند. در این حالت تجهیزات زیردریایی قادر خواهند مکرراً یافته‌های خود را از زیر دریا به ایستگاه‌های بیرونی ارسال کنند.

- مکان‌های آموزشی: فناوری لای‌فای به دلیل بالا بودن سرعت آن می‌تواند در مدارس، دانشگاه‌ها و سایر مراکز آموزشی به‌کار گرفته شود.
- فرودگاه: در فرودگاه‌ها بیشتر مسافران با مشکل سرعت بسیار پایین اینترنت مواجه هستند از سویی دیگر استفاده از فناوری وای‌فای برای ارائه خدمات اینترنت باعث ایجاد اختلال در سامانه ناوبری فرودگاه‌ها می‌شود. از این رو لای‌فای در فرودگاه‌ها می‌تواند برای انتقال داده‌ها استفاده شود. با به‌کارگیری منابع تولید نور مرئی در لامپ‌های LED در داخل هواپیما امکان استفاده از اینترنت با سرعت بالا فراهم خواهد شد.
- در مدیریت ترافیک: با به‌کارگیری فناوری لای‌فای در تجهیزات ترافیکی می‌توان با انتقال داده‌ها بین این تجهیزات و لامپ‌های ماشین‌ها که مجهز به این فناوری هستند امکان تبادل داده بین این‌ها را فراهم نموده و تصادفات را به حداقل کاهش داد.
- سایر مکان‌ها: لای‌فای می‌تواند در هر مکان دیگری که استفاده از وای‌فای، بلوتوث و سایر فناوری‌ها ممنوع شده است به‌کار گرفته شود.

## ۳-۳. معماری لای‌فای

لای‌فای به‌عنوان یک فناوری بی‌سیم این امکان را می‌دهد که اطلاعات را از طریق لامپ‌های LED تبادل کند. لای‌فای یک توانایی منحصر به‌فرد مبتنی بر سامانه روشنایی حالت جامد است که برای تولید کدهای باینری صفر و یک از LED چشمک‌زن استفاده می‌کند. در فضاهایی که نور چراغ در آن وجود دارد اطلاعات می‌تواند توسط دستگاه‌های الکترونیکی که مجهز به دیود حساس به نور هستند دریافت شود. این به این معنی است که هر جا که از لامپ LED استفاده شود می‌تواند در یک زمان هم روشنایی را فراهم و هم ارتباطات بی‌سیم را برقرار کند. با افزایش تقاضا برای داده‌های بی‌سیم و کمبود طیف رادیویی و مسائل آلودگی الکترومغناطیسی آن، به نظر می‌رسد لای‌فای جایگزین سالم‌تر، ارزان‌تر و کم‌خطرتر نسبت به وای‌فای است [۱۷].

در کنار سرعت بالای LED، امکان رمزنگاری اطلاعات با دریافت سری‌های مختلف نیز وجود دارد. نیروی LED خیلی سریع تنظیم شده که با چشم قابل دیدن نیست بنابراین به نظر می‌رسد عملکرد پایداری داشته باشد [۱۷]. هدف این فناوری در شبکه‌های صنعتی، ذخیره‌سازی داده‌های سبز و انتقال آن با سرعت بالا است [۱۸]. دلیل استفاده از داده سبز در لای‌فای امکان گرفتن انرژی خورشیدی جهت روشن کردن LED و استفاده از طیف الکترومغناطیسی که بر خلاف وای‌فای برای بدن ضرر ندارد است. شکل (۴) نمای کلی یک سامانه لای‌فای و لامپ LED درون آن را نشان می‌دهد و همچنین تصویری از اجزای اصلی را شامل می‌شود.



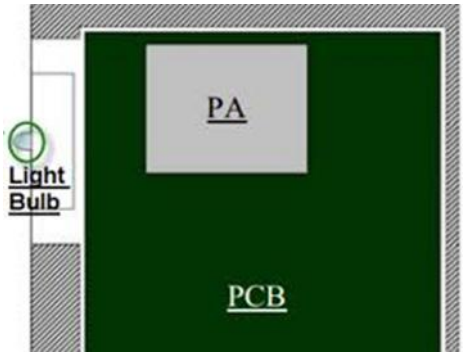

**شکل (۴)**: نمای کلی یک سامانه لای‌فای و لامپ LED درون آن [۱۰]

لای‌فای از نور مرئی برای انجام فرایند انتقال داده استفاده می‌کند. همان‌طور که در شکل (۵) نشان داده شده، سامانه لای‌فای از چهار بخش زیر تشکیل شده است:

۱. لامپ
۲. مدار تقویت کننده قدرت RF (PA)
۳. بورد مدار چاپی (PCB)
۴. محفظه

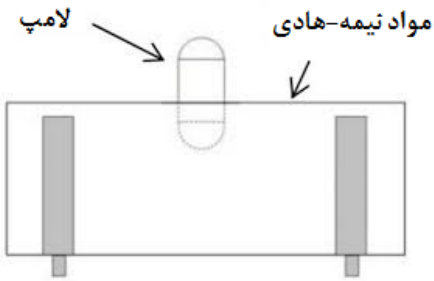
PCB ورودی الکتریسیته و خروجی لامپ را کنترل می‌کند و میکروکنترلرهای مورد استفاده در مدیریت لامپ‌ها را در خود جای می‌دهد. سیگنال RF به وسیله PA تولید می‌شود و به سمت یک فیلد الکتریکی همچون لامپ هدایت می‌شود. تمرکز بالای انرژی در فیلد الکتریکی محتوای موجود در لامپ را در مرکز آن به شکل پلاسما تبدیل کرده و این پلاسمای کنترل شده منبع قوی ایجاد نور می‌شود. تمام این فرایندها در یک محفظه آلومینیومی[1] صورت می‌گیرد.

1- ENCLOSURE




**شکل (۵):** اجزای لای‌فای [۳۳]

در سامانه لای‌فای یک زیرسامانه لامپی وجود دارد که در شکل (۶) مشاهده می‌شود. در این زیرسامانه لامپی درون یک پوش از جنس نارسانا قرار گرفته است. این طرح بسیار قابل اطمینان‌تر از منابع تولید نور معمولی است که در آن الکترودهای تضعیف شده وارد لامپ می‌شوند. در به‌کارگیری ماده نارسانا، دو هدف اصلی مورد نظر است: نخست اینکه ماده نارسانا برای طول موج فرکانس‌های رادیویی انتقال یافته به وسیله PA به‌عنوان هادی عمل کرده و دوم اینکه به‌عنوان یک فیلد الکتریکی استفاده شده که انرژی را در لامپ متمرکز می‌کند استفاده می‌شود. انرژی فیلد الکتریکی به سرعت باعث گرم شدن ماده موجود در لامپ شده و آن را به پلاسما تبدیل می‌کند. این ماده پلاسما نور با شدت بالا و پهنای باند کامل تولید می‌کند. این پهنای باند کامل به‌صورت دیجیتالی قابل کنترل بوده و به راحتی قابل کاربرد است.




**شکل (۶):** ساختار لامپ لای‌فای [۳۳]

انرژی یک فوتون متناسب با فرکانس نور است [۱۹] فوتون یک ذره است که یک کوانتوم نور را نشان می‌دهد بنابراین، از لحاظ خواص با کوانتوم یکسان هستند، اما برخی از مسائل امنیتی سایبری بدون آن قابل دست‌یابی است این مفهوم به ما اجازه می‌دهد که ذخیره‌سازی اطلاعات سبز در مراکز داده سبز از طریق خدمات محاسبات ابری حفظ شود. وقتی که از بلوک‌های بزرگ استفاده می‌شود پیچیدگی در طول زمان افزایش می‌یابد اما می‌توان مراحل پردازش را به‌صورت پویا با استفاده از الگوریتم گروور و خواص نور به حداقل رساند [۱۰].

از طریق خواص نور، ارتباط بین کاربران امن است و سرور با تأیید هویت در مرکز داده می‌تواند ایجاد شود. همچنین می‌توان پیچیدگی و مراحل پردازش را کاهش داد در حالی که بهتر است کلیدهای صحیح برای حفظ امنیت سایبری در داخل مرکز داده‌ها و ابر محاسبات ایجاد نمود. بر این اساس لای‌فای راه‌حل‌های امنیتی سایبری را با کمترین هزینه ارائه می‌دهد. لای‌فای به دلیل حجم و سرعت بالا در انتقال داده، پیچیدگی ظرفیت ذخیره‌سازی را افزایش می‌دهد، با استفاده از آن می‌توان ذخیره‌سازی اطلاعات سبز برای انواع داده‌ها از جمله داده‌ای بزرگ که مشکل بزرگی در شبکه‌های صنعتی است را انجام داد. با توجه به شبکه‌های صنعتی فعلی، بسیاری از برنامه‌های کاربردی از معماری‌های مختلف استفاده می‌کنند که نه‌تنها به اندازه داده هستند بلکه به ترافیک داده بستگی دارند. برای مدیریت امنیت سایبری در برنامه‌های مختلف مدیریت کلید KM روش مناسبی است [۱۰].

### ۳-۳-۱. LEDها

دیود نوری (LED) یک دستگاه نیمه هادی است که نور را هنگام عبور یک جریان الکتریکی، منتشر می‌کند. از طریق LED هنگامی‌که جریان توسط ذرات حمل می‌شوند و با هم ترکیب می‌شوند، نور تولید می‌شود. در مواد نیمه هادی نور به صراحت روشن نیست، اما در بیشتر LEDها که در آن یک طول موج اتفاق می‌افتد اینگونه نیست [۲۰] این نور در ماده نیمه هادی جامد تولید می‌شود چراغ‌های LED به‌عنوان دستگاه‌های حالت جامد ذکر شده‌اند. کلمه روشنایی حالت جامد که شامل LEDهای آلی است متمایز می‌شود این فناوری روشنایی از دیگر منابع مورد استفاده مانند رشته‌های داغ (رشته‌های رشته‌ای و لامپ هالوژن تنگستن) یا تخلیه گاز (فلورسنت چراغ‌های LED مقدماتی) که فقط نور قرمز تولید می‌کنند متمایز می‌شوند. همان‌طور که در شکل (۷ - الف) نشان داده شده است LED های مدرن می‌توانند انواع رنگ‌های مختلف را از جمله قرمز، سبز و آبی (RGB) نور تولید کنند. امروزه پیشرفت در فناوری LED امکان‌پذیر شده است LED ها برای ساخت نور سفید نیز قابل استفاده هستند.

### ۳-۳-۲. دیودهای نوری

دیود نوری که در قسمت شکل (۷ – ب) نشان داده شده دستگاهی است که در تبدیل نور به جریان برق کمک می‌کند. دیود نوری از مواد نیمه هادی و حاوی اتصال p-n ساخته و طراحی شده است تا در بایاس معکوس عمل کند. در دیود نوری زمانی که فوتون‌ها جذب شدند جریان پخش می‌شود و مقدار

بسیار کمی از جریان نیز در زمانی که هیچ نوری موجود نیست پخش می‌شود. همراه با افزایش سطح زمین، مدت زمان پاسخ‌دهی دیود نوری‌ها همراه با تأخیر می‌شود [۲۰] فناوری دیود نوری موفقیت‌آمیز بوده و به دلیل ساختار معمولی و کم هزینه‌اش به‌طور گسترده‌ای استفاده می‌شود. دیودهای نوری دو حالت عملیاتی مجزا دارند، اولاً حالت فتوولتاییک نامی و ثانیاً حالت هادی نور، در حالت فتوولتاییک تغییر نور غیر خطی است و دامنه پویای به‌دست آمده به درستی کوچک است و بالاترین سرعت نیز در حالت فتوولتاییک حاصل نمی‌شود.

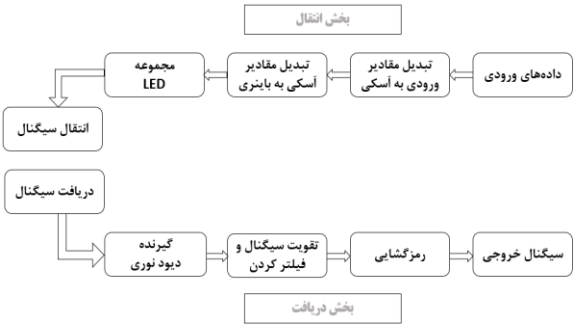
(ب) (الف)

**شکل (۷)**: دیودها [۱]

در حالت فوتوولتاییک، هدایت نور بسیار خطی است و ولتاژ مخالف تأثیر قابل توجهی بر نور ندارد اما تأثیر ضعیفی بر روی جریان تاریک (جریان بدون نور) دارد. دیودهای نوری به‌طور جامع در صنعت الکترونیک، به ویژه در آشکارسازها و سامانه‌های مخابراتی نوری با پهنای باند گسترده استفاده می‌شود.

نسل دیگری از دیودهای نوری پایه و اساس منطقی‌ای دارند: در این دیودها وقتی LED روشن است ۱ منتقل شده و وقتی خاموش است ۰ منتقل می‌شود [۱۷] این LEDهای درخشان به سرعت خاموش و روشن می‌شوند و مسیرهایی برای انتقال اطلاعات از طریق نور اختصاص می‌دهند. کار با لای‌فای بسیار ساده است. لای‌فای نور را به یک سمت منتقل می‌کند. به‌عنوان مثال: یک LED و یک حسگر نوری در سمت دیگر وجود دارند. حسگر دارای دو حالت خاموش و روشن است.

برای ایجاد یک پیام بسته به شرایط LEDهای مختلفی استفاده می‌شوند. ممکن است از LEDهایی با دو رنگ مختلف برای دریافت اطلاعات در بازه چندین مگابایت در هر ثانیه استفاده شود. در نور با نرخ[1] نوسان در روشن و خاموش شدن LED برای تولید سری‌هایی از ۰ و ۱ اطلاعات رمزگشایی می‌شوند. نیروی LED به‌گونه‌ای است که چشم انسان نمی‌تواند ببیند و این‌طور به نظر می‌آید که نور آن همیشه ثابت است. دیودهای روشنایی (LEDها، چراغ ترمز خودکار، واحد کنترل از راه دور و برنامه‌های مختلف بسیار) می‌توانند خیلی سریع‌تر از چشم انسان قابل شناسایی باشند و یک منبع نوری به نظر برسند. با این وجود، در واقع یک تابش واقعی است. عمل خاموش شدن اگر که به هر دلیلی انجام گیرد به‌طور نامحسوس انتقال اطلاعات را با استفاده از کدهای باینری تقویت می‌کند. با استفاده از ترکیبی از صفرها و با تغییر نرخ خاموش و روشن با فلاش در LEDها، داده‌ها می‌توانند کدگذاری شوند. این روش برای استفاده سریع از نور برای انتقال داده از راه دور، در واقع ارتباط دیداری نور (VLC) نامیده می‌شود، اما به‌طور رایج‌تر آن را لای‌فای نامند، که آن می‌تواند با رقیب مبتنی بر رادیوی خود، وای‌فای رقابت کند (فرآیند شکل (۸)).




**شکل (۸)**: نحوه انتقال داده در لای‌فای [۱۷]

### ۳-۳-۳. حسگر تصویر

حسگر تصویر یک دستگاه الکترونیکی و حساس به نور است که یک تصویر نوری را به یک سیگنال الکترونیک تبدیل می‌کند. آن‌ها از میلیون‌ها دیود نوری تشکیل شده‌اند و در تجهیزات تصویربرداری دیجیتال به‌عنوان یک گیرنده تصویر استفاده می‌شود. حسگر تصویر جزئی است که به تأثیر فوتون‌ها واکنش نشان می‌دهد، همان‌طور که در شکل (۹) نشان داده شده است، ابتدا آن‌ها را به یک جریان الکتریکی تبدیل می‌کند سپس به یک مبدل آنالوگ - دیجیتال منتقل می‌شود. رایج‌ترین گونه‌های حسگرهای تصویر، حسگرهای CCD و CMOS هستند. حسگرهای تصویر معمولاً در ماژول‌های دوربین و سایر دستگاه‌های تصویربرداری استفاده می‌شوند. در این زمان، رایج‌ترین حسگرهای تصویری دستگاه شارژ دیجیتال جفت شده (CCD) یا حسگرهای پیکسل فعال نیمه هادی اکسید فلز مکمل (CMOS) هستند.

1- Rate

**شکل (۹)**: حسگر تصویر [۱]

در یک دوربین، یک حسگر تصویر نوری الکترونیکی نور عبوری از عدسی را به شارهای دیود نوری با اندازه‌های مختلف تبدیل می‌کند.

## ۳-۴. پروتکل‌های اولیه تعریف شده برای لای‌فای

پروتکل‌های لای‌فای به وسیله استاندارد بین‌المللی IEEE 802.15 تعریف شده‌اند. این استانداردها از سال ۲۰۱۱ میلادی توسط کمیته IEEE به تصویب رسیده‌اند. این کمیته همان کمیته‌ای است که استانداردهای وای‌فای ۸۰۲٫۱۱ و اترنت ۸۰۲٫۳ را تعریف کرده‌اند. IEEE802.15 کارگروهی از مؤسسه مهندسان الکترونیک و برق (IEEE) است که به‌صورت تخصصی استانداردهای شبکه‌های بی‌سیم خصوصی (WPAN) را تنظیم می‌کنند. این کمیته خود شامل ۷ گروه مختلف است که گروه کاری شماره ۷ این کمیته وظایف بررسی و تنظیم استانداردهای ارتباطات نوری قابل رؤیت (VLC) را بر عهده دارد. گروه استاندارد IEEE 802.15.7 در دسامبر ۲۰۱۱ پیش‌نویس 5C از استاندارد PHY و استاندارد MAC را آماده کردند. برای ارتباطات مرئی که لای‌فای در این دسته قرار می‌گیرد دو لایه فیزیکی و مک توسط کارگروه IEEE 802.15.7 تعریف شده است. در ادامه به معرفی معروف‌ترین پروتکل‌های لای‌فای پرداخته می‌شود.

### ۳-۴-۱. پروتکل SECVLC

فناوری که به‌عنوان VANET ساخته شده است هماهنگ با ITS است و همچنین ITF VANET پیشنهاد شده است تا مشکلاتی که در ITS وجود داشت (از جمله کنترل ترافیک و بهینه‌سازی) را حل کند. VANET ITS یک نوع از شبکه‌های Ad Hoc است که زیرساخت ارتباطی وسایل نقلیه (V2V)، همچنین وسیله نقلیه به زیرساخت (V2I) یا هر دو [۲۱] بر اساس ( IEEE802.11p DSRC) - که فرم استاندارد دسترسی بی‌سیم برای محیط‌های وسیله نقلیه است - عمل می‌کند. یکی از کاربردهای VANET استفاده آن در محیط‌های نظامی است.

در شبکه‌های Ad Hoc نظامی، وسایل نقلیه عضو یک گروه می‌شوند که با یکدیگر بسته‌ها را تبادل می‌کنند. در طول حمل‌ونقل، فرمان تاکتیکی وسیله نقلیه که اولین یا آخرین وسیله نقلیه در تیم است، انتقال داده‌ها را جایی که داده‌ها حاوی دستور یا برنامه است و نیاز به تحویل موقتی و قابل اطمینان را فراهم می‌کنند[۲۲]. علاوه بر این، شبکه Ad Hoc نظامی باید اطمینان حاصل کند که داده‌های منتشر شده را نمی‌توان با سایر وسایل نقلیه رمزگشایی کرد محدوده ارتباطات زمانی که بسته‌های اطلاعاتی مورد هجوم قرار گرفتند. ارتباطات شبکه آسیب‌پذیر ارتش در جاده‌ها مقررات سخت‌گیرانه‌ای را برای امنیت کانال‌های ارتباطی مورد استفاده در وسایل نقلیه قرار می‌دهد و از این رو به پروتکل‌های امنیتی نیاز دارد.

در حال حاضر، راه‌حل‌های امنیتی VANET عمدتاً بر روی فناوری ارتباطات خودرویی عمل می‌کنند. هر دستگاه می‌تواند برای جلوگیری از برقراری ارتباط بین وسایل نقلیه دشمن در محدوده انتقال سیگنال مخرب ارسال کند. از سوی دیگر، در حمله‌ای دروغین، دشمن، کانال DSRC را بیش از حد مورد حمله قرار داده تا دستوراتی که می‌خواهد اجرا کند؛ اگر چه فناوری VANET مبتنی بر DSRC در طول زمان تکامل یافته است [۱۲]، اما دارای آسیب‌پذیری‌های امنیتی است که هنوز حل نشده‌اند؛ به‌عنوان مثال یکی از راه‌کارها در ارتباطات نظامی استفاده دستگاه از کلیدهای اختصاصی است که روزانه برای ارتباطات تولید می‌شوند. با این حال، حوادثی وجود دارد که هکرها در دستیابی به کلید مخفی [۱۳] با حمله به DSRC کانال موفق می‌شوند. از سوی دیگر کمبود طیف RF منجر شده است محققان برای بررسی فناوری‌های جایگزین که یکی از آن‌ها VLC است. VLC فناوری ارتباطی نسبتاً جدید است که با استفاده از تابش نوری مدولاسیون در طیف نور مرئی اطلاعات دیجیتال حمل می‌کند به تازگی، بسیاری از محققان از VLC برای اهداف مختلف استفاده می‌کنند که هر کدام دارای ویژگی‌ها [۱۴ و ۱۵]، الزامات [۱۶، ۲۳ و ۲۴] و امکانات خاصی در معماری ترکیبی با DSRC [۲۰] پیشنهاد شده که این طرح‌های VLC به‌صورت آزمایشی [۱۶، ۲۳ و ۲۴] یا از طریق شبیه‌سازی رایانه‌ای [۱۴] مورد بررسی قرار گرفتند.

یک سامانه VLC معمولی برای ارائه هم‌زمان روشنایی و ارتباط در سناریوهای داخلی و خارجی با استفاده از نوردهی سریع سوئیچینگ از دیودها (LEDها) به‌عنوان فرستنده استفاده می‌کند. VLC شبکه با اکثر اجزای ارتباطی موجود در داخل وسایل نقلیه یک فناوری امیدوار کننده برای کارهای نظامی است. وسایل نقلیه مدرن در حال حاضر با توجه به طول عمر طولانی، مقاومت بالا در برابر ارتعاش و عملکرد ایمنی بهتر LEDها، شروع

به استفاده از LED نمودند. LEDها در چراغ‌های توقف، چراغ‌های ترمز، سیگنال‌های چرخشی استفاده می‌شوند. از سوی دیگر گیرنده‌های VLC عمدتاً یا دیودهای عکس (PD) یا CMOS در چراغ‌های جلو بسیاری از وسایل نقلیه [۲۵] و دوربین جلو یا عقب برای ردیابی خطوط و پارکینگ کاربرد دارند [۲۶].

### ۳-۴-۲. پروتکل SECVLC

ویژگی‌های پروتکل امنیتی پیشنهاد شده SecVLC به شرح زیر است [۳۴]:

۱. از ویژگی VLC جهت اطمینان استفاده می‌کند و تنها وسایل مورد هدف در ارتباطات شرکت می‌کنند.

۲. از ارتباط کامل دو طرفه که IR است استفاده می‌کند. لینک خروجی برای به اشتراک گذاشتن کلید مخفی و VLC است و لینک ورودی برای دریافت داده‌های وسیله نقلیه رمز شده مورد استفاده قرار می‌گیرد.

۳. جایی که بسته‌های داده را نمی‌توان بدون کلیدهای تولید رمزگشایی کرد این پروتکل با تولید کلید و سازوکار به اشتراک‌گذاری عمل می‌کند که برای رمزنگاری داده‌ها و رمزگشایی استفاده می‌شود.

SecVLC متشکل از پنج بخش است؛ سامانه راه‌اندازی، تولید کلید، IR انتقال کلید، رمزگذاری / رمزگشایی داده‌ها و انتشار داده‌های رمزگذاری شده توسط VLC با مقداردهی اولیه سامانه شروع می‌شود. سامانه اجزای سخت‌افزاری خود را چک می‌کند و مقصد را که در انتظار کلید است قابل مشاهده می‌شود. در مقصد از طریق پرتو نور حادثه‌ای کلیدی ایجاد می‌شود که از منبع بیرون می‌آید و هنگامی که مقصد آن را دریافت کرد، پرتوهای نور پس از آن یک کلید مخفی برای رمزگذاری داده تولید می‌کند.

کلید مخفی تولید شده از طریق فرستنده آیفون ارسال می‌شود. انتقال فقط با ویژگی زاویه باریک IR امکان‌پذیر است. در مورد DSRC در محدوده ارتباطی وسیله نقلیه برای دریافت کلید مخفی، به‌عنوان مخالف تمام وسایل نقلیه در نظر گرفته می‌شود. کلیدهای مخفی بر اساس استاندارد رمزگذاری پیشرفته (AES) هستند که به‌طور گسترده‌ای به دلیل ویژگی‌هایی چون سرعت به‌کار گرفته شده‌اند.

پس از دریافت کلید مخفی از مقصد، منبع رمزگذاری، داده‌ها را رمزگذاری می‌کند و بسته رمزگذاری شده از طریق پرتوهای نور در VLC را انتقال می‌دهد. اگر وسیله نقلیه‌ای وجود داشته باشد پوشش نور از منبع، نمی‌تواند بسته داده را بدون کلید مخفی رمزگشایی کند. این در واقع حل مشکل کانال Overraring از ارتباطات نظامی مبتنی بر DSRC است. پس از به اشتراک گذاشتن کلید مخفی، مقصد بسته‌های داده رمز شده را از منبع دریافت می‌کند در حالی که از طریق فرستنده IP برای دور بعدی انتقال داده‌ها کلید رمز جدید ایجاد شده است. IR کامل دوبلکس و ارتباطات VLC را بدون افزایش تأخیر امنیت داده‌ها فعال می‌کند. پس از دریافت بسته‌های داده، مقصد با استفاده از کلید مخفی آن‌ها را رمزگشایی می‌کند. برای هر پیام، مقصد برای رمزگذاری یک کلید مخفی با منبع دارد.

## ۴. ارزیابی عملکرد

نویسندگان Purelifi[1] پروتکل SecVLC را توسط جاوا در سمت مقصد پیاده‌سازی کرده‌اند. Li-1st[2] ابزاری از نسل Keyczar Li-1 است که اولین محصول تجاری است. VLC که توسط pureLifi Ltd تولید شده، از زیرساخت‌های تجاری استفاده می‌کنند که به سرعت در حال توسعه و آزمایش است. Li-1 واحد فرستنده Tx و واحد دریافت کننده بر اساس Rx را شامل می‌شود. واحد Tx به دو چراغ مهتابی LED متقاطع وصل شده است [۲۷] چرا که چراغ‌های مهیج خودرو به دلیل گسترده بودن و الگوی روشنایی مسطح برای به حداقل رساندن انعکاس توسط مه، ترجیح داده می‌شوند. از سوی دیگر، Keyczar یک مجموعه ابزار منبع باز است که توسط گوگل برای تولید کلید تولید شده است.

بین منبع و مقصد برای فرستادن IR و گیرنده IR از کلید مخفی استفاده می‌شود. Tx و Rx هر دو برای ارزیابی کارایی ارتباطات به رایانه متصل می‌شوند. به‌منظور مقایسه آسیب‌پذیری‌های امنیتی رسانه‌های ارتباطی، سناریوهایی که وسایل نقلیه استفاده می‌کنند، DSRC و انتقال اطلاعات قابل مشاهده نور، یعنی VLC، ارزیابی شدند. سناریو ارتباط DSRC با رانندگی شبیه‌ساز Vehicular NeTwork و با شبیه‌ساز (VENTOS) شبیه‌سازی و اجرا شده است [۲۸]. از سوی دیگر، VLC و SecVLC در یک آزمایش که در محیط بیرونی انجام می‌شود، بازتاب‌هایی از وسایل نقلیه و جاده را در نظر می‌گیرند. اندازه‌گیری‌های ساعتی و منبع تغذیه روزانه در فضای باز برای جبران نویز شات انجام می‌شود. آزمایش‌های انجام شده همانند سناریوهایی است که پیش از انتشار وسیله نقلیه انجام می‌شوند.

1- http://purelifi.com/li-fire/li-1st/
2- https://goo.gl/LMuY1l

در این آزمایش‌ها با چراغ مه چراغ عقب خودروی پیشرو در مسیر منحنی حرکت می‌کند.

ارزیابی عملکرد SecVLC در دو بخش انجام می‌شود. قسمت اول تمرکز بر تحلیل امنیتی SecVLC است جایی که سامانه با یک ویروس مخرب مورد بررسی قرار گرفته است. در جاده با تحرک ثابت برای هر آزمایش، ۱۰۰ بسته داده بر روی شبکه Ad Hoc نظامی ارسال می‌شوند و شخص مخرب سوم تلاش می‌کند تا محتوای داده را استخراج کند. در بخش دوم از ارزیابی عملکرد، عملکرد معیارهای شبکه با مقایسه نسبت ارسال بسته‌های داده (DPDR) و تأخیر بین وسایل نقلیه تفسیر می‌شوند. در هر یک از آزمایش‌ها، ۱۰۰ بایت بسته داده سفارشی ارسال شده است. داده‌ها از ۲۰۰ بایت به ۵۰۰ بایت متغیر هستند و برای حجم متفاوت اثر اندازه داده‌ها در نظر گرفته شده است.

## ۴-۱. تحلیل امنیتی

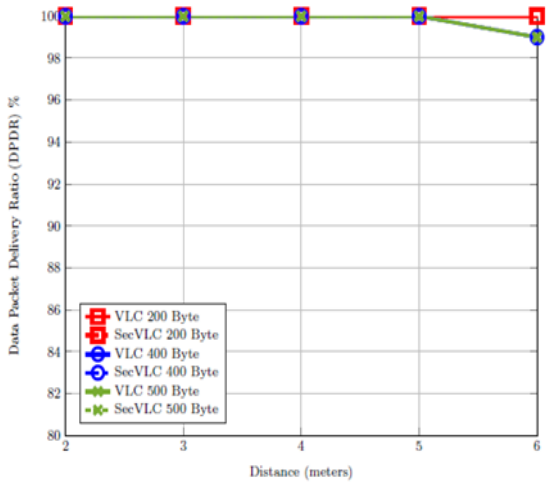
در تجزیه و تحلیل امنیتی پروتکل SecVLC، نسبت رمزگشایی داده‌های مخرب خودرو مورد ارزیابی قرار می‌گیرد. نسبت داده رمزگشایی نسبت به تعداد متن ساده با موفقیت به تعداد کل خودروها ارسال شده‌ها است. در این سناریو، خودرو مخرب بسته‌های داده‌ها را دریافت می‌کند و پس از آن برای رمزگشایی داده‌ها یا پروسه‌هایی مانند سرقت اطلاعات هویت خودرو تلاش می‌کند [۳۴].

وسیله نقلیه دشمن می‌تواند بسته اطلاعاتی را در هر دو سناریو DSRC و VLC با حداقل ۷۰٪ نسبت رمزگشایی داده‌های داده دریافت کند. در DSRC، وسیله نقلیه دشمن در صورتی که در آن واقع شده باشد، کانال را در محدوده انتقال (۳۰۰ متر) وسایل نقلیه نظامی خاموش می‌کند. از سوی دیگر، VLC به دلیل دریافت داده‌های دشمن، محدودیت انتقال و هدایت را دارد. با این حال، خودروی دشمن همچنان اطلاعات را در صورت لزوم در نور قرار می‌دهد. پوشش SecVLC در مقایسه با DSRC و VLC بسته داده‌ها را رمزگذاری می‌کند و داده‌ها فقط با کلید مخفی می‌تواند رمزگشایی شود. حتی اگر وسیله نقلیه دشمن از کانال فرار کند، فقط می‌تواند بسته‌های کنترل متن ساده را دریافت و در مرحله اولیه پروتکل انتقال دهد.

در این بخش از ارزیابی عملکرد، تجزیه و تحلیل عملکرد شبکه، عملکرد پروتکل شبکه SecVLC با تجزیه و تحلیل داده‌ها و معیارها از جمله DPDR و تأخیر، مورد بررسی قرار می‌گیرد. DPDR به‌عنوان نسبت تعداد بسته‌های داده با موفقیت دریافت شده به تعداد کل بسته‌های داده منتقل شده تعریف شده است.

این میانگین تأخیر متریک به‌عنوان میانگین زمان تأخیر تعریف شده است. بسته‌های داده‌ای که شامل انتقال کلید رمزهای IR، رمزگذاری / رمزگشایی داده‌ها و انتشار VLC هستند از منبع به مقصد منتقل می‌شوند.

شکل (۱۰) مقایسه DPDR در فاصله‌های مختلف برای اندازه بسته‌های داده متفاوت SecVLC و VLC را نشان می‌دهد. همان‌طور که مشاهده می‌شود الگوهای تخریب ارزش DPDR را با فاصله زمانی افزایش می‌دهد. علاوه بر این، با افزایش فاصله، SecVLC و VLC هر دو افت می‌کنند. در ارائه بسته‌های داده با توضیح قدرت سیگنال دریافتی (RSS) این را می‌توان دریافت که هر چه فاصله بزرگ‌تر می‌شود RSS در واحد گیرنده کاهش می‌یابد. در نتیجه با کاهش RSS، بسته‌های داده را نمی‌توان با موفقیت دریافت کرد. از این دیدگاه می‌توان گفت که در فواصل بزرگ کاهش RSS عامل اصلی است که بر روی آن تأثیر می‌گذارد.

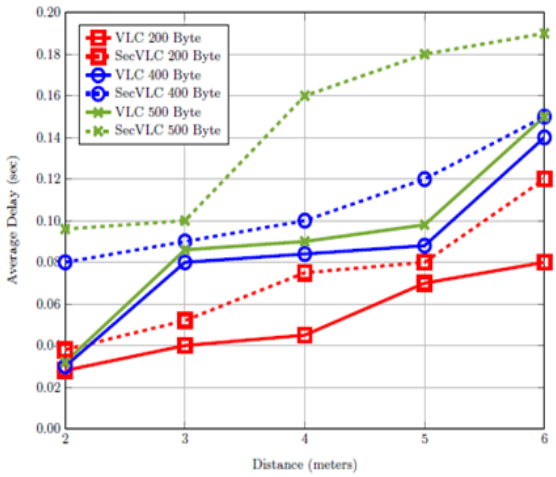



**شکل( ۱۰):** نمودار مقایسه نسبت بارگذاری بسته‌های داده [۳۴]

### ۴-۱-۱. DPDR در SecVLC

شکل (۱۱) عملکرد متوسط تأخیر پروتکل SecVLC را در مقایسه با VLC به‌عنوان تابع فاصله با متغیر اندازه داده‌ها نشان را می‌دهد. برای SecVLC که شامل کلید انتقال IR، رمزگذاری داده‌ها، رمزگشایی اطلاعات و انتشار داده VLC بوده و همچنین مقدار تأخیر اندازه‌گیری شده است. علاوه بر این، با تغییر حجم داده‌ها اثر اندازه داده‌ها به‌طور متوسط بر تأخیر تجزیه و تحلیل می‌شود. همان‌طور که در شکل (۱۱) دیده می‌شود، وقتی حجم داده‌ها بیشتر باشد SecVLC زمان بیشتری را برای رمزگذاری و رمزگشایی نیاز دارد. در صورتی که انتقال اطلاعات ایمن فعال باشد به این معنا که تنها وسیله هدف بتواند محتوای داده را

استخراج کند، وجود تأخیر متوسط بالاتر برای SecVLC نسبت به VLC، قابل قبول است. از این دیدگاه می‌توان گفت که بین امنیت و تأخیر برای VLC و پروتکل SecVLC، VLC تأخیر کمتری را نسبت به SecVLC فراهم می‌کند در حالی که SecVLC با استفاده از ارتباطات رمزنگاری، امنیت داده‌ها را می‌گیرد.




**شکل (۱۱):** متوسط ضریب تأخیر [۳۴]

## ۴-۲. بررسی مزایا و معایب لای‌فای نسبت به فناوری ارتباطی وای‌فای

لای‌فای دارای مزایایی نسبت به روش‌های قدیمی‌تر است که در ادامه به برخی از آن‌ها اشاره می‌شود.

### ۴-۲-۱. توسعه هزینه کم

از جمله این مزایای لای‌فای می‌توان به هزینه کمتر این فناوری نسبت به برخی از فناوری‌های شبکه‌های رایانه‌ای اشاره کرد. همان‌طور که در بخش قبلی اشاره شد، با استفاده از LED و اضافه کردن امکاناتی که اکنون در دسترس است، می‌توان ابزارهای توسعه آن را فراهم نمود.

### ۴-۲-۲. سرعت بالا

با توجه به اینکه سرعت طیف نور قابل رؤیت ۱۰ هزار بار بزرگ‌تر از امواج رادیویی است. سرعت انتقال داده در این فناوری بالاتر از فناوری‌های دیگر است. آزمایش‌ها نشان داده‌اند که لای‌فای قادر است تا ۲۲۴ گیگابایت اطلاعات را تنها در یک ثانیه را انتقال دهد؛ یعنی با استفاده از این فناوری می‌توان ۱۸ فیلم سینمایی، هر کدام با حجم ۱/۵ گیگابایت را تنها در یک ثانیه دانلود کرد. البته دستیابی به چنین سرعتی در فضای غیر آزمایشگاهی با وجود محدودیت‌ها و موانع مختلف تاکنون ممکن نشده است. دانشمندان توانسته‌اند در شرایط واقعی در آزمایش‌های خود به سرعت انتقال اطلاعات ۱ گیگابایت در ثانیه دست یابند. اگر چه ۱ گیگابایت در ثانیه در برابر ۲۲۴ گیگابایت در ثانیه، کوچک به نظر می‌رسد، ولی نسبت به اعداد و ارقام مطرح شده در سرعت ارسال داده با فناوری وای‌فای بسیار بزرگ است.

### ۴-۲-۳. دسترسی پذیری بالا

فناوری لای‌فای نسبت به برخی دیگر از فناوری‌ها به ویژه وای‌فای بیشتر در دسترس است، زیرا در لای‌فای نور مرئی وسیله انتقال داده است که لامپ‌های LED به‌عنوان تولید کننده این نور محسوب می‌شوند و این وسیله در دسترس است. این فناوری در برخی از مکان‌ها قابل استفاده است که امکان استفاده از سایر فناوری‌ها در این مکان‌ها میسر نیست از جمله این مکان‌ها هواپیما است که در ارتفاعات بالا استفاده از این فناوری امکان‌پذیر است.

### ۴-۲-۴. کاربرد چندمنظوره

دیگر مزیت این فناوری این است که نورهای LED می‌توانند در حین انتقال داده، به فعالیت اصلی خود یعنی روشنایی ادامه دهند. در مقابل، زمانی که نوری مورد نیاز نیست، لامپ می‌تواند نور خود را کاهش داده و به انتقال داده ادامه دهد.

### ۴-۲-۵. امنیت بیشتر

از آنجا که وای‌فای توانایی عبور از دیوار، سقف و اجسام سخت و حرکت در تمام جهات[1] را دارد، امکان هک توسط افراد دیگر را دارد؛ اما لای‌فای تنها در محدوده‌ای که توسط لامپ‌ها روشن شده است عمل می‌کند و امکان هک کردن توسط دیگران میسر نخواهد بود. این مسئله می‌تواند برای مراکز نظامی، تأسیساتی و بانکی مورد توجه قرار گیرد.

### ۴-۲-۶. مصرف انرژی کم و بازدهی بالا

لامپ‌های LED بسیار کم مصرف بوده و با پیشرفت فناوری و مطالعات دقیق‌تر مصرف انرژی آن‌ها کمتر خواهد شد. ضمن اینکه امواج وای‌فای، باتری بیشتری از دستگاه گیرنده مصرف می‌کنند.

### ۴-۲-۷. عدم ضرر برای بدن

با توجه به مطالعات انجام شده امواج وای‌فای برای بدن مضر بوده

1- Omnidirectional

در حالی که طیف نور مرئی برای بدن هیچ ضرری ندارد، حتی طیف مشخصی از نور مرئی برای بدن مفید هستند. به همین دلیل، لای‌فای جایگزین مناسبی برای مدارس، دانشگاه‌ها، بیمارستان‌ها و سایر اماکن عمومی است.

### ۴-۲-۸. تراکم بیشتر اطلاعات

با توجه به اینکه در مکان‌های مختلف بسته به نیاز از چندین لامپ استفاده می‌شود و در فناوری لای‌فای لامپ‌ها می‌توانند حاوی اطلاعات باشند در مجموع تراکم داده بیشتر از حالتی است که تنها یک مودم وای‌فای در آن فضا قرار دارد. باید توجه داشت که از آنجا که طیف‌های نوری با یکدیگر متفاوت هستند، تداخل در آن‌ها رخ نمی‌دهد، به همین دلیل در لای‌فای برخلاف وای‌فای امکان تداخل الکترومغناطیسی وجود ندارد.

در جدول (۱) خلاصه بررسی و مقایسه فناوری‌های وای‌فای و لای‌فای ارایه شده است.

**جدول (۱):** مقایسه فناوری‌های وای‌فای و لای‌فای بر اساس معیارهای مختلف

| نام فناوری | وای‌فای | لای‌فای |
|---|---|---|
| تعریف | وفاداری بی‌سیم | وفاداری نوری |
| اتصال | امواج رادیویی | نور |
| امنیت | متوسط | بالا |
| امکان تداخل | دارد | ندارد |
| هزینه | متوسط | کم |
| امکان دسترسی | در فاصله ۳۲ متری | دسترسی مستقیم به نور |
| پهنای باند | 150 Mbps | بیش از 1 Gbps |
| سرعت | کم | بالا |
| تراکم داده | کم | بالا |
| کاربرد | استفاده در محل‌هایی که امکان تداخل امواج رادیویی نیست. | استفاده در هواپیما، اکتشافات زیرزمینی، بیمارستان‌ها، ادارات و خانه‌ها به‌منظور انتقال داده و استفاده از اینترنت |
| بلوغ | بالغ | نوپا |
| فناوری | WLAN 802.11a/b/g/n/ac /ad | دستگاه‌های سازگار با IrDA[۱] |

۱- Infrared Data Association این یک استاندارد برای انتقال داده‌ها از طریق پورت اشعه مادون قرمز است.

## ۴-۳. چالش‌های لای‌فای

پشتیبانی دستگاه‌های موجود از سامانه لای‌فای نیازمند نگاه ارتباطی است که یکی از چالش‌های این موضوع تداخل آن با دیگر نورهای خارجی از جمله نور خورشید است [۵]. هزینه‌های تأسیسات این سامانه بیشتر تجاری است. اینترنت بدون یک منبع نوری قابل استفاده نیست. مکان‌های محدودی برای استفاده از لای‌فای وجود دارد [۲۹] با توجه به این واقعیت که از نور مرئی استفاده می‌کند و نور نمی‌تواند به دیوار نفوذ کند، محدوده سیگنال توسط موانع فیزیکی محدود می‌شود. از طرفی سایر منابع نور ممکن است با سیگنالی خارجی مواجه شوند. یکی از بزرگ‌ترین چالش‌ها تداخل سیگنال در خارج از منزل با نور خورشید است. زیرساخت‌های لای‌فای کاملاً جدید هستند و باید بررسی شوند. این سیگنال‌ها قدرت کمتری دارند و به‌منظور استفاده از اینترنت لای‌فای چراغ‌ها باید در طول روز و شب روشن نگه داشته شوند [۴، ۳۰ و ۳۱]. در هنگام تاریکی نمی‌توان از لای‌فای بهره برد که این یک مشکل جدی است [۳۲].

## ۵. نتیجه‌گیری

با گسترش روزافزون استفاده از شبکه‌های ارتباطی داده‌ای یکی از چالش‌های این شبکه‌ها سرعت دستیابی به داده است. این در حالی است که سرعت وای‌فای که از فرکانس‌های رادیویی برای انتقال داده استفاده می‌کند علاوه بر ضررهایی که برای بدن داشته و عدم امکان استفاده از آن در برخی از محیط‌ها از سرعت قابل قبولی برخوردار نیست. لای‌فای یک فناوری بی‌سیم جدید است که امکان تبادل داده‌ها را از طریق لامپ‌های LED می‌دهد. این فناوری دارای مزیت‌های فراوانی است از جمله اینکه نور ۱۰،۰۰۰ برابر بیشتر از سایر منابع در دسترس بوده و قادر است سرعت انتقال داده‌ها را تا ۲۵۰ برابر سریع‌تر کند. کاربردها و ایده‌هایی برای لای‌فای تعریف شده که در این مقاله به آن پرداخته شد. این فناوری دارای معماری خاصی است که برای توسعه آن و استفاده از آن به ویژه در مباحث امنیتی نیاز به شناخت دقیق آن وجود دارد که در این مقاله ضمن معرفی معماری داخلی آن پروتکل‌های ارتباطی که برای آن تعریف شده در جهت برقراری امنیتی و شناخت آن ارائه شده است. در پایان نیز عملکرد لای‌فای مورد ارزیابی قرار گرفته و با مقایسه آن با فناوری وای‌فای نقاط قوت و ضعف آن نشان داده شد. در تحقیق‌های آینده پیشنهاد می‌شود که به راه‌حل‌های امنیتی بیشتری برای برقراری امنیت و جلوگیری از سرقت اطلاعات تبادل شده در این شبکه پرداخته شود.

## ۶. منابع


1. Y. Perwej "The Next Generation of Wireless Communication Using Li-Fi (Light Fidelity) Technology," J. of Computer Networks," vol. 4, pp. 20-29, 2017.
2. Global Mobile Data Traffic Forecast Update, "Cisco Visual Networking Index," 2012–2017.
3. "802.15.7-2011- IEEE Standard for Local and Metropolitan Area Networks--Part 15.7: Short-Range Wireless Optical Communication Using Visible Light," Ed: IEEE.
4. S. Dimitrov and H. Haas, "Principles of LED Light Communications: Towards Networked Li-Fi," Cambridge University Press, pp. 978-110, 2015.
5. H. Haas, "Wireless Data from Every Light Bulb," Ed: TED Website [Online], 2011.
6. D. O'Brien, H. Le Minh, L. Zeng, G. Faulkner, K. Lee, and D. Jung, "Indoor visible light communications: challenges and prospects," in Free-Space Laser Communications VIII, p. 709106, 2008.
7. "National Telecommunications and Information Admission (NTIA),"Available: http://www.Ntia.doc.gov/osmhome/allochrt.
8. R. Sharma, R. Raunak, and A. Sanganal, "Li-Fi Technology: Transmission of Data through Light," Int. J. of Computer Technology & Applications, vol. 5, pp. 113-124.
9. B. Nemmaniwar, M. Bhalerao, and S. Tirmanwar "Data Transmission by Using Light Fidelity," Nt. Res. J. of Science & Engineering, vol. 3, pp. 84-92, 2015.
10. V. Thayananthan, K. Jambi, O. A. Abdulkader, and A. M. Bamahdi, "Analysis of Cybersecurity Based on Li-Fi in Green Data Storage Environments," Presented at the IEEE 4th Int. Conf. on Cyber Security and Cloud Computing, 2017.
11. I. Rubin, A. Baiocchi, F. Cuomo, and P. Salvo, "Vehicular Backbone Network Approach to Vehicular Military Ad Hoc Networks," In MILCOM 2013- 2013 IEEE Military Communications Conf., San Diego, CA, USA, 2013.
12. R. GillesEngoulou, M. Bellaïche, S. Pierre, and A. Quintero "VANET Security Surveys," Computer Communications, vol. 44, pp. 1-13, 2014.
13. J. Leskovec and K. Krevl, "Quotes 2008-08: Stanford Large Network Dataset Collection," Available: http://snap.stanford.edu, 2014.
14. P. Luo, Z. Ghassemlooy, H. L. Minh, E. Bentley, and A. Burton, and X. Tang , "Performance Analysis of a Car-to-car Visible Light Communication System," Applied Optics, vol. 54, pp. 1696-1706, 2015.
15. W. Viriyasitavat, S.-H. Yu, and H.-M. Tsai, "Short Paper: Channel Model for Visible Light Communications Using Off-the-shelf Scooter Taillight," Presented at the IEEE Vehicular Networkin, Boston, MA, USA, 2013.
16. H.-Y. Tseng, Y.-L. Wei, A.-L. Chen, H.-P. Wu, H. Hsu, and H.-M. Tsai "Characterizing Link Asymmetry in Vehicle-to-vehicle Visible Light Communications," Presented at the Vehicular Networking Conference (VNC), 2015.
17. R. Sonawane, A. Kusmude, S. Gelot3, and A. Vaidya, "A Potential Solution to Global Wireless Spectrum Shortage and Wireless Data Transmission Using Light Fidelity (Li-Fi)," Int. Research J. of Engineering and Technology (IRJET), vol. 4, Jan 2017.
18. K. Gaia, M. Qiua, H. Zhaob, L. Taoa, and Z. Zong "Dynamic Energy-Aware Cloudlet-Based Mobile Cloud Computing Model for Green Computing," J. of Network and Computer Applications, vol. 59, pp. 46-54, 2016.
19. B. Crowell, "Quantum Physics (Chapter 13)," In Simple Nature an Introduction to Physics for Engineering and Physical Science Students, Fullerton ed, 2008.
20. S. Ishihara, R. V. Rabsatt, and M. Gerla "Improving Reliability of Platooning Control Messages Using Radio and Visible Light Hybrid Communication," Presented at the 2015 IEEE Vehicular Networking Conference (VNC), Kyoto, Japan, 2015.
21. A. Gomez, K. Shi, C. Quintana, M. Sato, G. Faulkner, and B. C. Thomsen, "Beyond 100-Gb/s Indoor Wide Field-of-View Optical Wireless Communications," IEEE Photonics Technology Letters, vol. 27, pp. 367 - 370, 2015.
22. D. Tsonev, S. Videv, and H. Haas, "Towards a 100 Gb/s Visible Light Wireless Access Network," Optics Express, vol. 23, pp. 1627-1637, 2015.
23. B. Turan, S. Ucar, S. C. Ergen, and O. Ozkasap, "Dual Channel Visible Light Communications for Enhanced Vehicular Connectivity," Presented at the Vehicular Networking Conference (VNC), Kyoto, Japan, 2015.
24. S. Ucar, B. Turan, S. C. Ergen, O. Ozkasap, and M. Ergen "Dimming Support for Visible Light Communication in Intelligent Transportation and Traffic System," Presented at the NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 2016.
25. S.-H. Yu, O. Shih, H.-M. Tsai, N. Wisitpongphan, and R. D. Roberts "Smart Automotive Lighting for Vehicle Safety," IEEE Communications Magazine, vol. 51, pp. 50 - 59, 19 December 2013.
26. T. Yamazato, I. Takai, H. Okada, T. Fujii, T. Yendo, and S. Arai, "Image-sensor-based Visible Light Communication for Automotive Applications," IEEE Communications Magazine, vol. 52, pp. 88 - 97, 2014.
27. LEDFog101 OSRAM. Available: http://goo.gl/ty5zEC
28. VEhicular NeTwork Open Simulator (VENTOS). Available: http://goo.gl/OueFkO
29. Z. Wang, D. Tsonev, S. Videv, and H. Haas, "On the Design of a Solar-Panel Receiver for Optical Wireless Communications with Simultaneous Energy Harvesting," IEEE J. on Selected Areas in Communications, vol. 33, pp. 1612-1623, 2015.
30. D. Tsonev, S. Videv, and H. Haas, "Light fidelity (Li-Fi): Towards All-Optical Networking," In Proc in Broadband Access Communication Technologies VIII, 2013.
31. D. Tsonev, S. Videv, and H. Haas, "Unlocking Spectral Efficiency in Intensity Modulation and Direct Detection Systems," IEEE J. Sel. Areas Commun, vol. 33, pp. 1758-1770, 2015.
32. H.-H. Lu, C.-Y. Li, T.-C. Lu, C.-J. Wu, C.-A. Chu, A. Shiva, and T. Mochii, "Bidirectional Fiber-wireless and Fiber-VLLC Transmission System Based on an OEO-based BLS and a RSOA," Optics Letters, vol. 41, pp. 476-479, 2016.
33. X. BaoEmail, G. YuJisheng, and D. X. Zhu, "Li-Fi: Light Fidelity-a survey," vol. 21, Issue 6, pp. 1879–1889, August 2015.
34. S. Ucar, S. Coleri Ergen, O. Ozkasap, D. Tsonev, and H. Burchardt, "SecVLC: Secure Visible Light Communication for Military Vehicular Networks," In Proc. of the 14th ACM Int. Symposium on Mobility Management and Wireless Access (MobiWac '16), ACM, New York, NY, USA, pp. 123-129, 2016.

# Lifi Technology: Introduction, Applications, Challenges and Security Evaluation

S. Keshvari*, M. Abbasi

## Abstract

Nowadays, with the widespread use of the Internet, one of the great challenges of communication networks is the access speed. The speed of access becomes a challenge when different devices connect to a wireless network. Wi-Fi networks are facing some problems, such as difficult or impossible connectivity in some places and a speed far below today's needs. In this research, while introducing Li-Fi technology, where the data is exchanged wirelessly through visible light, its features and limitations are studied. The architecture and scientific relations and mathematical models of this new technology are also presented. There are new ideas and applications for the Li-Fi that are explored in this paper and finally, Li-Fi technology is compared to Wi-Fi technology based on various parameters.

**Key Words:** *Lifi, Lifi Security, Wifi, Data Transfer.*

❊ Imam Hossein Comprehensive University (sakeshvari@ihu.ac.ir)- Writer-in-Charge