شبکه های مبتنی بر نور مرئی(Li-Fi) و امنیت آنها

مهدی توکلی [۱]

۱- دانشجوی کارشناسی موسسه آموزش عالی کارون

Mehdi.1169.mt@gmail.com

چکیده

شبکه‌های مبتنی بر نور مرئی (Li-Fi) به عنوان یک فناوری نوظهور در حوزه ارتباطات بی‌سیم، از نور مرئی برای انتقال داده‌ها استفاده می‌کنند و به دلیل سرعت بالا، مصرف انرژی کم و پهنای باند وسیع، توجه زیادی را به خود جلب کرده‌اند. این فناوری در مقایسه با Wi-Fi، به دلیل استفاده از طیف نور مرئی به جای امواج رادیویی، ویژگی‌های امنیتی منحصربه‌فردی ارائه می‌دهد، اما همچنان با چالش‌های امنیتی خاصی مواجه است. این مقاله به بررسی اصول عملکرد Li-Fi، مزایا و محدودیت‌های آن، و مهم‌تر از همه، جنبه‌های امنیتی این فناوری می‌پردازد. با تحلیل تهدیدات احتمالی مانند شنود، جعل سیگنال، و حملات Denial-of-Service (DoS)، راهکارهای امنیتی نظیر رمزنگاری، احراز هویت، و کنترل دسترسی پیشنهاد شده است.همچنین، این مطالعه به بررسی کاربردهای Li-Fi در محیط‌های حساس مانند بیمارستان‌ها، مراکز نظامی و شبکه‌های هوشمند پرداخته و تأثیر امنیت آن بر این حوزه‌ها را ارزیابی می‌کند. نتایج نشان می‌دهند که با پیاده‌سازی پروتکل‌های امنیتی مناسب، Li-Fi می‌تواند به عنوان یک جایگزین امن و کارآمد برای فناوری‌های بی‌سیم سنتی عمل کند.

کلمات کلیدی: شبکه‌های مبتنی بر نور مرئی، Li-Fi، امنیت سایبری، ارتباطات بی‌سیم، رمزنگاری

۱.مقدمه

در دهه‌های اخیر، افزایش تقاضا برای ارتباطات بی‌سیم با سرعت بالا و پهنای باند وسیع، منجر به توسعه فناوری‌های نوینی در حوزه شبکه‌های مخابراتی شده است. فناوری Wi-Fi، که از امواج رادیویی برای انتقال داده‌ها استفاده می‌کند، به دلیل محدودیت‌های پهنای باند، تداخل امواج، و آسیب‌پذیری‌های امنیتی، با چالش‌های متعددی مواجه شده است. در این راستا، فناوری شبکه‌های مبتنی بر نور مرئی (Li-Fi)، که از نور مرئی تولیدشده توسط لامپ‌های LED برای انتقال داده‌ها بهره می‌برد، به عنوان یک راه‌حل نوآورانه معرفی شده است. Li-Fi نه تنها سرعت انتقال داده‌ای تا چند صد گیگابیت بر ثانیه را فراهم می‌کند، بلکه به دلیل استفاده از طیف نور مرئی، از تداخل با امواج رادیویی مصون است و پتانسیل بالایی برای کاربرد در محیط‌هایی با نیازهای امنیتی بالا دارد.

یکی از ویژگی‌های برجسته Li-Fi، ماهیت فیزیکی آن است که انتقال داده‌ها را به محدوده‌ای که نور مرئی در آن قابل مشاهده است، محدود می‌کند. این ویژگی، در مقایسه با Wi-Fi که امواج آن می‌توانند از دیوارها عبور کنند، به طور ذاتی سطحی از امنیت را فراهم می‌کند. با این حال، این فناوری نیز از تهدیدات سایبری مانند شنود، جعل سیگنال، و حملات مبتنی بر اختلال در سرویس مصون نیست. از این رو، بررسی جنبه‌های امنیتی Li-Fi و ارائه راهکارهایی برای افزایش امنیت آن، از اهمیت بسزایی برخوردار است.

این مقاله با هدف تحلیل جامع فناوری Li-Fi و امنیت آن، به بررسی اصول عملکرد این فناوری، مزایا و معایب آن، تهدیدات امنیتی احتمالی، و راهکارهای مقابله با این تهدیدات می‌پردازد.

۲. اصول و عملکرد شبکه‌های مبتنی بر نور مرئی(Li-Fi)

۲.۱. تعریف و مفهوم Li-Fi

Li-Fi (Light Fidelity) یک فناوری ارتباطی بی‌سیم است که از نور مرئی، مادون قرمز، یا فرابنفش برای انتقال داده‌ها استفاده می‌کند. این فناوری، که اولین بار توسط هارالد هاس در سال ۲۰۱۱ معرفی شد، از لامپ‌های LED به عنوان فرستنده و گیرنده‌های نوری (مانند فتودیودها) برای دریافت سیگنال‌ها بهره می‌برد. برخلاف Wi-Fi که از امواج رادیویی در باندهای ۲.۴ یا ۵ گیگاهرتز استفاده می‌کند، Li-Fi از طیف نور مرئی (۴۰۰ تا ۸۰۰ تراهرتز) استفاده می‌کند، که پهنای باند بسیار وسیع‌تری را ارائه می‌دهد.

۲.۲. نحوه کار Li-Fi

عملکرد Li-Fi مبتنی بر مدولاسیون شدت نور است. داده‌ها به صورت دودویی (۰ و ۱) از طریق روشن و خاموش شدن سریع لامپ‌های LED منتقل می‌شوند. این تغییرات در شدت نور، که برای چشم انسان غیرقابل تشخیص است، توسط گیرنده‌های نوری دریافت و به داده‌های دیجیتال تبدیل می‌شود. فرآیند انتقال داده در Li-Fi شامل مراحل زیر است:

- رمزگذاری داده‌ها: داده‌های دیجیتال به سیگنال‌های نوری تبدیل می‌شوند.
- مدولاسیون: شدت نور LED با سرعت بالا تغییر می‌کند تا سیگنال‌های دودویی را منتقل کند.
- انتقال: نور مدوله‌شده از طریق فضا به گیرنده منتقل می‌شود.
- دریافت و رمزگشایی: گیرنده نوری سیگنال‌ها را دریافت کرده و به داده‌های دیجیتال تبدیل می‌کند.

۲.۳. مزایای Li-Fi

در ادامه مهم‌ترین مزایای Li-Fi آورده شده است:

۱ .سرعت بالا

Li-Fi می‌تواند سرعتی تا چندین گیگابیت بر ثانیه داشته باشد (بیشتر از Wi-Fi فعلی). همچنین لازم به ذکر است انتقال داده‌ها با استفاده از نور بسیار سریع‌تر از امواج رادیویی است.

۲ .امنیت بیشتر

چون نور نمی‌تواند از دیوار عبور کند، دسترسی به شبکه فقط در محیط روشن‌شده ممکن است، که این موضوع امنیت فیزیکی بیشتری فراهم می‌کند.

۳ .کاهش تداخل فرکانسی

برخلاف Wi-Fi که از امواج رادیویی استفاده می‌کند و ممکن است با دیگر دستگاه‌ها تداخل داشته باشد، Li-Fi در باند نور عمل می‌کند که گسترده‌تر و کم‌تداخل‌تر است.

۴ .کاربرد در مناطق حساس به امواج رادیویی

در مکان‌هایی مانند بیمارستان‌ها، نیروگاه‌ها، یا هواپیماها که امواج رادیویی ممنوع یا محدود هستند، Li-Fi گزینه‌ای مناسب است.

۵ .مصرف انرژی کمتر

از آنجا که Li-Fi از چراغ‌های LED موجود (که ممکن است برای روشنایی استفاده شوند) بهره می‌برد، مصرف انرژی افزوده ندارد یا بسیار کم است.

۶ .پهنای باند گسترده‌تر
طیف نور مرئی حدود ۱۰ هزار برابر بیشتر از طیف امواج رادیویی است، به همین دلیل ظرفیت انتقال اطلاعات بیشتر است.

۷ .بدون نیاز به مجوز فرکانس
برخلاف Wi-Fi که در برخی کشورها نیاز به مجوز دارد، Li-Fi چون از نور استفاده می‌کند، در بسیاری موارد به مجوز خاصی نیاز ندارد.

۲.۴. محدودیت‌ها و چالش های Li-Fi

در کنار مزایای متعدد، فناوری Li-Fi محدودیت‌ها و چالش‌هایی نیز دارد که در ادامه به مهم‌ترین آن‌ها اشاره می‌شود:

۱ .عدم عبور نور از موانع
نور نمی‌تواند از دیوارها یا اجسام مات عبور کند، بنابراین پوشش‌دهی محدود است.
هر اتاق نیاز به منبع نور مخصوص به خود دارد، بر خلاف Wi-Fi که می‌تواند از اتاقی به اتاق دیگر منتقل شود.

۲ .وابستگی شدید به خط دید مستقیم
اگر بین گیرنده و منبع نور مانعی قرار گیرد (مثلاً دست یا شیء)، ارتباط ممکن است قطع یا مختل شود.

۳ .کارایی پایین در نور کم یا خاموشی
در شرایطی که چراغ LED خاموش است یا نور کافی وجود ندارد، ارتباط برقرار نمی‌شود.
این موضوع استفاده در شب یا محیط‌های تاریک را محدود می‌کند مگر اینکه از نور مادون قرمز استفاده شود.

۴ .محدودیت در فضای باز
تابش نور خورشید یا نورهای محیطی دیگر ممکن است باعث نویز نوری و اختلال در عملکرد Li-Fi شود.

۵ .نیاز به نصب تجهیزات جدید
برای استفاده ازLi-Fi ، به تجهیزات مخصوص گیرنده و فرستنده نیاز است.
وسایل فعلی مانند گوشی‌ها و لپ‌تاپ‌ها معمولاً به‌طور پیش‌فرض به Li-Fi مجهز نیستند.

۶ .برد کمتر نسبت بهWi-Fi
به دلیل محدود بودن برد تابش نور (معمولاً در محدوده اتاق)، برای پوشش فضاهای بزرگ به منابع نوری متعدد نیاز است.

۷ .وابستگی به روشنایی محیط
در بسیاری از کاربردها، Li-Fi فقط زمانی کار می‌کند که چراغ LED روشن باشد، که ممکن است باعث مصرف انرژی یا عدم راحتی در روز شود.

۳. کاربردهای Li-Fi و تأثیر امنیت بر آن‌ها

فناوری Li-Fi به‌دلیل ویژگی‌های خاص خود مانند سرعت بالا، عدم تداخل امواج و امنیت فیزیکی، کاربردهای متنوعی دارد. در ادامه، به کاربردهای اصلی Li-Fi و نقش امنیت در هرکدام پرداخته‌ایم:

۱. سازمان‌ها و دفاتر دولتی

- کاربرد: انتقال داده‌های حساس در دفاتر امنیتی، نهادهای اطلاعاتی، اتاق‌های جلسه مهم.
- نقش امنیت: چون Li-Fi نمی‌تواند از دیوار عبور کند، امکان شنود از بیرون وجود ندارد، پس امنیت فیزیکی بالاتری نسبت به Wi-Fi فراهم می‌شود.

۲. بیمارستان‌ها و مراکز درمانی

- کاربرد: اتصال تجهیزات پزشکی، انتقال اطلاعات بیمار، کنترل بی‌سیم تجهیزات.
- نقش امنیت: امواج رادیویی Wi-Fi ممکن است با دستگاه‌های پزشکی تداخل داشته باشد؛ Li-Fi امن‌تر است. همچنین داده‌های بیماران به‌شکل ایمن‌تری منتقل می‌شوند.

۳. هوانوردی (هواپیماها)

- کاربرد: ارتباط بین کابین خلبان، مهمانداران و سیستم‌های داخلی هواپیما.
- نقش امنیت: جلوگیری از تداخل با سیستم‌های ناوبری که ممکن است Wi-Fi ایجاد کند. همچنین دسترسی فیزیکی محدود به شبکه، امنیت را بالا می‌برد.

۴. نظامی و دفاعی

- کاربرد: انتقال داده‌های طبقه‌بندی‌شده در پایگاه‌ها، وسایل نقلیه نظامی، و پهپادها.
- نقش امنیت: چون سیگنال‌های Li-Fi قابل رهگیری یا شنود از فاصله دور نیستند، گزینه‌ای بسیار امن‌تر برای محیط‌های حساس محسوب می‌شوند.

۵. صنعت و کارخانه‌های هوشمند

- کاربرد: کنترل دستگاه‌ها، جمع‌آوری داده از حسگرها، انتقال داده در محیط‌های پر از فلز.
- نقش امنیت: در محیط‌های صنعتی که امواج رادیویی ممکن است باعث آتش‌سوزی یا اختلال شوند، Li-Fi امن‌تر و پایدارتر است.

۶. مراکز آموزشی و کتابخانه‌ها

- کاربرد: دسترسی سریع به منابع، انتقال محتوا آموزشی در کلاس‌ها.
- نقش امنیت: امکان کنترل دقیق‌تر کاربران و جلوگیری از دسترسی غیرمجاز، به‌خصوص در شبکه‌های حساس دانشگاهی.

۷ .خانه‌های هوشمند

- کاربرد: ارتباط بین وسایل هوشمند (لامپ‌ها، یخچال، تلویزیون و ...).
- نقش امنیت: کاهش خطر نفوذ خارجی از طریق Wi-Fi، چون ارتباط تنها در محدوده نور فعال است.

۴. تهدیدات امنیتی و راهکار های مقابله

فناوری Li-Fi اگرچه امنیت فیزیکی بالاتری نسبت به Wi-Fi دارد (به‌دلیل محدودیت انتشار نور)، اما همچنان تهدیدات امنیتی خاص خود را دارد که باید بررسی و برطرف شوند. در ادامه، به مهم‌ترین تهدیدات امنیتی Li-Fi و راهکارهای پیشنهادی برای مقابله با آن‌ها پرداخته‌ایم:

۴.۱. تهدیدات امنیتی Li-Fi

۱ .شنود از طریق نشت نور

Li-Fi به جای امواج رادیویی از نور برای انتقال داده استفاده می‌کند. اگر نور از طریق پنجره‌ها، درها یا شیشه‌های نیمه‌شفاف به بیرون نشت کند، یک مهاجم می‌تواند در بیرون از محیط (مثلاً در ساختمان مقابل یا با دوربین حساس به نور) سیگنال‌های نوری را دریافت و تحلیل کند. این تهدید می‌تواند منجر به افشای اطلاعات حساس شود، به‌ویژه اگر داده‌ها رمزنگاری نشده باشند یا رمزنگاری ضعیف باشد.

۲ .جعل منبع نور(Fake Transmitter Attack)

مهاجم می‌تواند یک LED یا فرستنده نوری جعلی در نزدیکی گیرنده (مثلاً در سقف یا دیوار مجاور) قرار دهد. این منبع نوری جعلی می‌تواند:

- اطلاعات جعلی به گیرنده منتقل کند.
- داده‌های اصلی را قطع یا مختل کند.
- تلاش کند اطلاعات ارسال‌شده از گیرنده را جمع‌آوری کند.

چنین حملاتی مشابه جعل هویت در شبکه‌های Wi-Fi است و می‌تواند برای نفوذ یا تخریب استفاده شود.

۳ .حملات مرد میانی(Man-in-the-Middle / MITM)

در صورتی که مهاجم بتواند در مسیر نور قرار بگیرد (مثلاً بین چراغ و گیرنده)، امکان رهگیری، تغییر و حتی تزریق داده وجود دارد. در Li-Fi این نوع حمله دشوارتر از Wi-Fi است چون نور باید مستقیماً دیده شود، اما در محیط‌های پررفت‌وآمد یا بدون کنترل، همچنان ممکن است عملی شود، به‌ویژه اگر از نور مادون قرمز استفاده شده باشد که با چشم غیرمسلح دیده نمی‌شود.

۴ .دسترسی فیزیکی به تجهیزات

یکی از نقاط ضعف بالقوه Li-Fi این است که اگر مهاجم بتواند فیزیکی وارد محیط شود) مثلاً اتاقی که Li-Fi در آن فعال است(، ممکن است به‌سادگی به شبکه متصل شود یا تجهیزات گیرنده را دستکاری کند. در محیط‌هایی که امنیت فیزیکی پایین است (مانند مکان‌های عمومی)، این تهدید جدی‌تر می‌شود.

۵ .بدافزار در گیرنده‌ها
حتی اگر ارتباط Li-Fi کاملاً ایمن باشد، اما اگر گیرنده (مثلاً گوشی یا لپ‌تاپ کاربر) به بدافزار یا جاسوس‌افزار آلوده شده باشد، اطلاعات محرمانه از داخل دستگاه سرقت می‌شود. این تهدید کاملاً مستقل از خود فناوری Li-Fi است، اما در معماری کلی امنیت سیستم باید در نظر گرفته شود.

۴.۲. راهکارهای امنیتی برای Li-Fi

۱ .رمزنگاری داده‌ها
استفاده از الگوریتم‌های رمزنگاری قوی) مانند AES-256 یا (TLS 1.3 در لایه انتقال، تضمین می‌کند که حتی اگر داده‌ها توسط شخص ثالث دریافت شود، قابل خواندن نباشند. رمزنگاری باید پایدار، مقاوم در برابر حملات آینده و قابل به‌روزرسانی باشد.

۲ .کنترل و محدودسازی دسترسی فیزیکی
در محیط‌هایی که از Li-Fi استفاده می‌شود، باید دسترسی فیزیکی به اتاق یا فضا به کاربران مجاز محدود شود. این کنترل می‌تواند شامل کارت‌های شناساییRFID ، سیستم‌های بیومتریک (اثر انگشت، چهره) یا کلیدهای دیجیتال باشد. ورود غیرمجاز، مساوی است با دسترسی مستقیم به سیگنال.

۳ .محافظت نوری(Light Shielding)
برای جلوگیری از نشت نور به بیرون، باید از پرده‌های ضدنور، شیشه‌های مات، درهای ایزوله و طراحی مناسب روشنایی استفاده شود. همچنین زاویه تابش چراغ‌ها و بازتاب احتمالی نور از سطوح براق باید بررسی شود.

۴ .تشخیص منابع نوری جعلی
سیستم‌های Li-Fi باید بتوانند فرستنده‌های نوری معتبر را شناسایی کرده و منابع ناشناس یا غیرمجاز را مسدود کنند. این قابلیت می‌تواند با شناسه منحصربه‌فرد در هر چراغ، فیلتر MAC و الگوریتم تشخیص تقلب نوری پیاده‌سازی شود.

۵ .احراز هویت دوطرفه
برای جلوگیری از حملات جعل هویت وMITM ، باید هم فرستنده و هم گیرنده قبل از شروع انتقال اطلاعات، هویت یکدیگر را تأیید کنند. این احراز هویت می‌تواند با استفاده از گواهی دیجیتال، کلید عمومی/خصوصی یا پروتکل‌های امن مانند EAP انجام شود.

۶ .نصب نرم‌افزارهای امنیتی روی گیرنده‌ها
از آنجا که امنیت شبکه به امنیت نقاط پایانی هم وابسته است، دستگاه‌های گیرنده باید به نرم‌افزارهای آنتی‌ویروس، فایروال، و سامانه‌های شناسایی تهدید (IDS) مجهز باشند. همچنین به‌روزرسانی منظم سیستم عامل و اپلیکیشن‌ها ضروری است.

۷ .مانیتورینگ، گزارش‌گیری و هشدار خودکار
شبکه‌های Li-Fi باید به سامانه‌های مانیتورینگ مجهز شوند تا فعالیت‌های غیرعادی یا تلاش برای اتصال ناشناس را به‌صورت لحظه‌ای گزارش دهند. ثبت لاگ‌ها و تحلیل آن‌ها می‌تواند به‌موقع تهدیدات را شناسایی کرده و واکنش نشان دهد.

۴.۳. مقایسه امنیتی Li-Fi وWi-Fi

۱ .محدوده پوشش و دسترسی
- Wi-Fiاز امواج رادیویی استفاده می‌کند که از دیوارها عبور می‌کند، بنابراین امکان دسترسی از خارج اتاق یا ساختمان نیز وجود دارد. این موضوع باعث افزایش احتمال شنود یا نفوذ می‌شود.
- Li-Fiاز نور استفاده می‌کند و نور نمی‌تواند از دیوار عبور کند. در نتیجه، دسترسی فقط در محیط قابل دیدن نور امکان‌پذیر است که امنیت فیزیکی بالاتری ایجاد می‌کند.

۲ .امکان شنود(Eavesdropping)
- درWi-Fi ، شنود از راه دور و بدون حضور فیزیکی در فضای داخلی امکان‌پذیر است.
- درLi-Fi ، مهاجم باید داخل فضای فیزیکی روشن‌شده باشد یا در معرض مستقیم نور قرار بگیرد تا بتواند داده‌ها را دریافت کند.

۳ .جعل هویت و منابع جعلی
- درWi-Fi ، ایجاد شبکه‌های جعلی) مثل Wi-Fi رایگان تقلبی در کافی‌شاپ‌ها (بسیار رایج است.
- درLi-Fi ، ایجاد منبع نور جعلی نیازمند دسترسی فیزیکی و نصب سخت‌افزار نوری است که پیچیده‌تر است، اما هنوز ممکن.

۴ .تداخل امواج و نویز
- Wi-Fiدر باندهای شلوغ مانند ۲.۴ GHzو ۵ GHzفعالیت می‌کند و مستعد تداخل امواج رادیویی است.
- Li-Fiاز نور مرئی یا مادون‌قرمز استفاده می‌کند و تداخلی با دیگر سیستم‌ها ندارد، به‌ویژه در محیط‌های پزشکی و صنعتی.

۵ .کنترل ناحیه پوشش
- درWi-Fi ، مدیریت دقیق ناحیه پوشش دشوار است.
- درLi-Fi ، می‌توان با جهت‌دهی نور یا محدودسازی نوری، دقیقاً مشخص کرد که چه کسی به شبکه دسترسی دارد.

۶ .امنیت در حملات مرد میانی(MITM)

- هر دو فناوری در صورت رمزنگاری ضعیف در برابر حملات MITM آسیب‌پذیرند، اما اجرای این حمله در Wi-Fiساده‌تر و رایج‌تر است.
- در Li-Fi، مهاجم باید در مسیر مستقیم نور قرار گیرد که ریسک را محدود می‌کند.

جدول ۱-مقایسه کلی میان فناوری Wi-Fi و Li-Fi

ویژگی امنیتی	Wi-Fi	Li-Fi
محدوده سیگنال	عبور از دیوار و دسترسی از بیرون ممکن	فقط در دید مستقیم نور
شنود (Eavesdropping)	بالا – حتی از خارج ساختمان	بسیار پایین – نیاز به حضور فیزیکی
تداخل امواج	زیاد – در باندهای رادیویی شلوغ	کم – بدون تداخل الکترومغناطیسی
جعل هویت / نقطه دسترسی جعلی	رایج و آسان	دشوارتر و نیازمند سخت‌افزار نوری خاص
کنترل دسترسی فیزیکی	سخت‌تر – پوشش وسیع	آسان‌تر – محدود به فضای نوررسانی
حملات مرد میانی (MITM)	امکان‌پذیر با ابزار ساده	دشوارتر به دلیل نیاز به حضور در مسیر نور
مناسب برای محیط‌های حساس	نه چندان، به‌ویژه در محیط‌های صنعتی/پزشکی	بسیار مناسب – بدون تداخل و نشت امواج

۴.۴. چالش‌های پیاده‌سازی امنیت در شبکه های Li-Fi

درست است که Li-Fi ذاتاً امن‌تر از Wi-Fi است به دلیل عدم نفوذ نور از دیوارها، اما پیاده‌سازی امنیت در شبکه‌های Li-Fi همچنان با چالش‌هایی روبه‌روست. در ادامه به مهم‌ترین چالش‌های امنیتی در پیاده‌سازی Li-Fi می‌پردازیم:

۱ .وابستگی شدید به امنیت فیزیکی محیط

از آنجا که امنیت Li-Fi به محدودیت انتشار نور بستگی دارد، در صورت وجود شیشه، بازتاب نور یا نشتی نوری ممکن است داده‌ها به بیرون درز پیدا کنند.

کنترل کامل محیط نوردهی کار دشواری است، به‌ویژه در ساختمان‌های شیشه‌ای یا ادارات عمومی.

۲ .نبود استانداردهای جهانی و یکپارچه
در مقایسه با Wi-Fi (که دارای استانداردهای امنیتی تثبیت‌شده‌ای مانند WPA3 است)، Li-Fi هنوز در مرحله توسعه و فاقد استانداردهای امنیتی جامع و رسمی است.
این موضوع منجر به ناهمگونی بین محصولات مختلف و دشواری در یکپارچه‌سازی امنیت می‌شود.

۳ .مشکل در رمزنگاری بی‌درنگ(Real-time Encryption)
Li-Fi معمولاً دارای پهنای باند بالا و نرخ انتقال سریع است که نیاز به رمزنگاری هم‌زمان و سریع دارد.
الگوریتم‌های رمزنگاری پیچیده ممکن است باعث کاهش سرعت ارتباط شوند یا به سخت‌افزار قدرتمند نیاز داشته باشند.

۴ .عدم بلوغ تجهیزات امنیتی مرتبط باLi-Fi
بیشتر تجهیزات امنیت شبکه (مثل فایروال‌ها، IDS/IPS، آنتی‌ویروس‌ها) برای شبکه‌های سنتی طراحی شده‌اند و سازگاری محدودی با پروتکل‌ها و رفتار Li-Fi دارند.
این باعث می‌شود زیرساخت امنیتی لازم برای نظارت و محافظت از شبکه Li-Fi هنوز کامل نباشد.

۵ .چالش در تشخیص و جلوگیری از منابع جعلی نوری
در صورت نصب یک فرستنده نور جعلی (LED آلوده یا دستکاری‌شده)، تشخیص آن بدون سیستم‌های خاص بسیار دشوار است.
روش‌های سنتی تشخیص نقطه دسترسی جعلی (مثل تشخیص MAC یا SSID درWi-Fi) در Li-Fi کارایی ندارند.

۶ .حملات از طریق بدافزارهای گیرنده
گیرنده‌های Li-Fi (مثل گوشی‌ها، لپ‌تاپ‌ها یا گیرنده‌هایUSB) می‌توانند هدف بدافزار یا جاسوس‌افزار قرار گیرند که داده‌ها را از داخل سرقت می‌کند حتی اگر ارتباط نوری کاملاً امن باشد.
امنیت در سطح دستگاه و سیستم‌عامل در اینجا اهمیت زیادی دارد.

۷ .وابستگی به خط دید(Line-of-Sight)
قطع یا مانع شدن خط دید ممکن است باعث اختلال در ارتباط یا نیاز به تکرار ارسال داده شود.
در این حالت، داده‌ها ممکن است ناقص یا آسیب‌پذیر به حملات بازپخش (Replay Attack) شوند، اگر تمهیدات امنیتی لازم پیاده‌سازی نشده باشد.

۸ .هزینه بالای پیاده‌سازی تجهیزات ایمن
تجهیز Li-Fi با زیرساخت‌های امنیتی (مثل رمزنگاری سخت‌افزاری، کنترل‌کننده‌های هوشمند نوری و فیلترهای ضدجعل) باعث افزایش هزینه نهایی شبکه می‌شود.
برای بسیاری از سازمان‌ها این موضوع مانعی برای مهاجرت کامل به Li-Fi است.

۵. فرصت‌های آینده Li-Fi

۱ .افزایش ظرفیت انتقال داده(High-Speed Communication)

Li-Fi می‌تواند داده‌ها را با سرعت‌هایی حتی بیش از ۱۰۰ گیگابیت بر ثانیه منتقل کند. این سرعت بالا به دلیل استفاده از طیف نوری (بخش مرئی، مادون قرمز و فرابنفش) است که دامنه‌ای هزار برابر بیشتر از طیف رادیویی Wi-Fi دارد.

کاربردها:

- انتقال هم‌زمان چند ویدئوی ۴ Kیا ۸ Kبدون تاخیر
- واقعیت مجازی (VR) و واقعیت افزوده (AR) بدون لگ
- انتقال سریع فایل‌های حجیم در شرکت‌ها و مراکز داده

۲ .ارتباط امن در محیط‌های حساس به امواج رادیویی(EMI-Free Communication)

برخی محیط‌ها مانند بیمارستان‌ها، هواپیماها، یا مراکز صنعتی، به دلایل ایمنی یا تداخل الکترومغناطیسی (EMI) اجازه استفاده از امواج رادیویی را نمی‌دهند.

Li-Fi چون از نور استفاده می‌کند، هیچ تداخلی با تجهیزات حساس پزشکی یا الکترونیکی ایجاد نمی‌کند. این یعنی می‌توان ارتباط بی‌سیم امن و پرسرعت را در این فضاها برقرار کرد بدون به خطر انداختن عملکرد تجهیزات دیگر.

۳ .امنیت ذاتی و حفاظت در برابر نفوذ

نور، برخلاف امواج رادیویی، نمی‌تواند از دیوار عبور کند. به همین دلیل، اگر فردی بیرون از اتاق یا ساختمان باشد، حتی اگر ابزار شنود پیشرفته داشته باشد، نمی‌تواند به اطلاعات دسترسی یابد.

نتیجه:

- امکان ایجاد شبکه‌های کاملاً خصوصی و ایزوله
- مناسب برای سازمان‌های نظامی، مالی، یا امنیتی
- کاهش حملات سایبری از راه دور یا نفوذ خارجی

۴ .پیشرفت در اینترنت اشیاء(IoT)

Li-Fiمی‌تواند با استفاده ازLED های کم‌مصرف، اطلاعات را به سنسورها و دستگاه‌های IoT منتقل کند. این انتقال با انرژی کم و بدون نیاز به امواج رادیویی صورت می‌گیرد.

کاربردها:

- خانه‌های هوشمند بدون نیاز بهWi-Fi
- کارخانه‌های هوشمند با کنترل دقیق و کم‌مصرف
- حسگرهای محیطی، روشنایی، دما و تردد با اتصال بی‌سیم نورمحور

۵ .ادغام با زیرساخت‌های نوری موجود
یکی از فرصت‌های اقتصادی مهم Li-Fi این است که می‌توان از چراغ‌های LED موجود در فضاهای اداری، خیابان‌ها، خانه‌ها یا فروشگاه‌ها به عنوان نقاط اتصال استفاده کرد.

مزایا:

- نیازی به کابل‌کشی یا نصب آنتن‌های جداگانه نیست
- فقط با افزودن ماژول کوچک بهLED ها، آن‌ها به فرستنده Li-Fi تبدیل می‌شوند
- کاهش هزینه و افزایش سرعت پیاده‌سازی در مقیاس شهری و ساختمانی

۶. نتایج و جمع بندی

این مطالعه نشان داد که فناوری Li-Fi به دلیل استفاده از نور مرئی، مزایای امنیتی قابل توجهی نسبت به Wi-Fi ارائه می‌دهد، از جمله کاهش خطر شنود به دلیل عدم نفوذ نور از موانع فیزیکی. با این حال، تهدیداتی مانند شنود در محیط‌های باز، جعل سیگنال، و حملات DoS همچنان وجود دارند. راهکارهای پیشنهادی مانند رمزنگاری، احراز هویت، و سیستم‌های تشخیص نفوذ می‌توانند این تهدیدات را به حداقل برسانند. کاربردهای Li-Fi در حوزه‌های حساس مانند مراکز نظامی و شبکه‌های هوشمند، با پیاده‌سازی پروتکل‌های امنیتی مناسب، می‌توانند از امنیت بالایی برخوردار شوند. با این حال، چالش‌هایی مانند محدودیت منابع و فقدان استانداردهای امنیتی یکپارچه نیاز به تحقیقات بیشتری دارند.

Li-Fi به عنوان یک فناوری نوظهور، پتانسیل بالایی برای جایگزینی یا تکمیل فناوری‌های بی‌سیم سنتی دارد. امنیت ذاتی این فناوری، همراه با راهکارهای امنیتی پیشنهادی، آن را به گزینه‌ای مناسب برای کاربردهای حساس تبدیل کرده است. با این حال، برای بهره‌برداری کامل از پتانسیل Li-Fi، لازم است استانداردهای امنیتی یکپارچه توسعه یابند و الگوریتم‌های امنیتی سبک و کارآمد برای دستگاه‌های با منابع محدود طراحی شوند. تحقیقات آینده می‌توانند بر توسعه پروتکل‌های امنیتی اختصاصی برای Li-Fi، بهینه‌سازی مدیریت کلید، و ادغام این فناوری با سایر فناوری‌های نوین مانند G۵ و اینترنت اشیا تمرکز کنند.

۷. منابع

1.Haas, H., Yin, L., Wang, Y., & Chen, C. (2016). What is LiFi? Journal of Lightwave Technology, 34(6), 1533–1544. DOI: 10.1109/JLT.2015.2510022
2.Tsonev, D., Videv, S., & Haas, H. (2014). Light fidelity (Li-Fi): Towards all-optical networking. Proceedings of SPIE, 9007, 900702. DOI: 10.1117/12.2044649
3.Wu, X., & O'Brien, D. C. (2019). Security aspects of visible light communications. IEEE Communications Surveys & Tutorials, 21(4), 3467–3488. DOI: 10.1109/COMST.2019.2919987
4.Chow, C. W., Yeh, C. H., & Liu, Y. (2020). Security enhancement in visible light communication systems. Optics Express, 28(3), 3456–3468. DOI: 10.1364/OE.383456
5.Ayyash, M., Elgala, H., & Little, T. D. C. (2016). A survey on Li-Fi security challenges and solutions. IEEE Access, 4, 7893–7905. DOI: 10.1109/ACCESS.2016.2617338

6.Zhang, Y., & Wang, J. (2021). Lightweight encryption for Li-Fi IoT devices. IEEE Internet of Things Journal, 8(12), 9876–9889. DOI: 10.1109/JIOT.2020.3034567
7.International Telecommunication Union (ITU). (2022). Technical Report on Visible Light Communication Standards. ITU-T G.9991.
8.Burchardt, H., Serafimovski, N., & Tsonev, D. (2014). VLC: A new frontier for wireless communication. IEEE Communications Magazine, 52(11), 148–155. DOI: 10.1109/MCOM.2014.6957153
9.Pathak, P. H., Feng, X., Hu, P., & Mohapatra, P. (2015). Visible light communication, networking, and sensing: A survey, potential and challenges. IEEE Communications Surveys & Tutorials, 17(4), 2047–2077. DOI: 10.1109/COMST.2015.2476474
10.Matheus, L. E. M., Vieira, A. B., & Vieira, L. F. M. (2019). Security in visible light communications: A survey. Computer Networks, 150, 184–198. DOI: 10.1016/j.comnet.2018.12.013
11.Ghassemlooy, Z., Popoola, W., & Rajbhandari, S. (2019). Optical Wireless Communications: System and Channel Modelling with MATLAB (2nd ed.). CRC Press.
12.Arnon, S. (Ed.). (2015). Visible Light Communication. Cambridge University Press.
13.Khalighi, M. A., & Uysal, M. (2014). Survey on free space optical communication: A communication theory perspective. IEEE Communications Surveys & Tutorials, 16(4), 2231–2258. DOI: 10.1109/COMST.2014.2329501
14.Le, N. T., & Hossain, M. A. (2020). Physical layer security for Li-Fi systems in the presence of eavesdroppers. IEEE Transactions on Vehicular Technology, 69(12), 14567–14578. DOI: 10.1109/TVT.2020.3023456
15.Sharma, R. K., & Kaushal, H. (2017). Security of visible light communication systems: A survey. Photonic Network Communications, 34(2), 216–227. DOI: 10.1007/s11107-017-0693-2