مجله محاسبات نرم، جلد ۱۱، شماره ۲ (پاییز و زمستان ۱۴۰۱)، صفحه ۳۶ـ۵۳
https://doi.org/10.22052/scj.2023.242846.0

مجله محاسبات نرم
SOFT COMPUTING JOURNAL
تارنمای مجله: scj.kashanu.ac.ir

دانشگاه کاشان
University of Kashan

# مروری بر ویژگی‌های فناوری‌های ارتباطی در خانه‌های هوشمند و چالش‌های پیش‌رو✧

الهام توکلی[۱]، کارشناسی ارشد، علیرضا کشاورز حداد[۲*]، دانشیار

[۱] دانشکده آموزش‌های الکترونیکی، دانشگاه شیراز، شیراز، ایران.

[۲] دانشکده مهندسی برق و کامپیوتر، دانشگاه شیراز، شیراز، ایران.

**اطلاعات مقاله**

**تاریخچه مقاله:**

دریافت ۲۱ فروردین ماه ۱۴۰۰

پذیرش ۱۸ تیر ماه ۱۴۰۲

**کلمات کلیدی:**

اینترنت اشیا

خانه هوشمند

ساختمان هوشمند

فناوری ارتباطی سیمی

فناوری ارتباطی بی‌سیمی

امنیت

**چکیده**

**هوشمندسازی خانه‌ها یکی از موضوعات کاربردی و پررونق در دنیای امروز است که به افراد امکان تنظیم و کنترل از راه دور تجهیزات الکترونیکی و همچنین امکان برنامه‌ریزی آنها جهت صرفه‌جویی در مصرف انرژی را می‌دهد. در سال‌های اخیر شرکت‌های مطرح سیستم‌های مختلف سخت‌افزاری و نرم‌افزاری برای تجهیزات خانگی هوشمند و همچنین فناوری‌های ارتباطی آنها عرضه کرده‌اند. این فناوری‌ها از جهات مختلفی نظیر شرایط پیاده‌سازی، هزینه، مقیاس‌پذیری، تکامل‌پذیری، امنیت و غیره با یکدیگر متفاوتند و به دلیل تنوع زیاد آنها، انتخاب یک فناوری درخور با توجه به نیازمندی و امکانات موجود دشوار به نظر می‌رسد. پرواضح است که لازمه طراحی و پیاده‌سازی صحیح و اصولی یک خانه هوشمند، شناخت ویژگی‌ها و محدودیت‌های این فناوری‌ها در شرایط مختلف است. این مقاله مروری به فناوری‌های متداول ارتباطی در خانه‌های هوشمند مبتنی بر سیم‌کشی مجزا، خطوط برق ساختمان و ارتباطات بی‌سیم می‌پردازند و ویژگی‌ها و محدودیت‌های هر فناوری را بیان می‌کند، علاوه بر این به پژوهش‌های مرتبط و چالش‌های پیش‌رو جهت بهبود این فناوری‌ها می‌پردازد. نکات مطرح شده در مقاله به طراحان سیستم‌های هوشمند خانگی کمک می‌کند تا فناوری ارتباطی مناسبی را با توجه به شرایط موجود در خانه هوشمند انتخاب و استفاده نمایند.**



## ۱. مقدمه

بکارگیری امکاناتی که خانه را در اصطلاح هوشمند کند، همواره یکی از موضوعات مورد توجه زندگی مدرن بوده و در طول دوره‌های مختلف با توسعه فناوری راه‌حل‌های متعددی برای این منظور خلق شده است. طبق تعریف انجمن خانه‌های هوشمند، یک خانه هوشمند مجموعه‌ای از فناوری‌ها و سرویس‌ها در شبکه‌ای خانگی برای بهبود کیفیت زندگی است [۱]، [۲]. در واقع، خانه هوشمند به خانه‌هایی گفته می‌شود که ساکنان آن امکان تنظیم و کنترل تجهیزات الکترونیکی منزل خود را در فاصله نزدیک (داخل خانه) و یا از راه دور (خارج از خانه) داشته و قادر باشند برای کاربردهای مختلف نظیر کنترل عملکرد و صرفه‌جویی مصرف انرژی، برنامه‌های کاری مختلفی را روی تجهیزات خانگی استفاده کنند [۳].

در سال‌های اخیر در فناوری‌های خانه‌های هوشمند مفهوم ایجاد

✧ نوع مقاله: مروری

* نویسنده مسئول

پست(های) الکترونیک: etavakoli92@gmail.com (توکلی)

keshavarz@shirazu.ac.ir (کشاورز حداد)

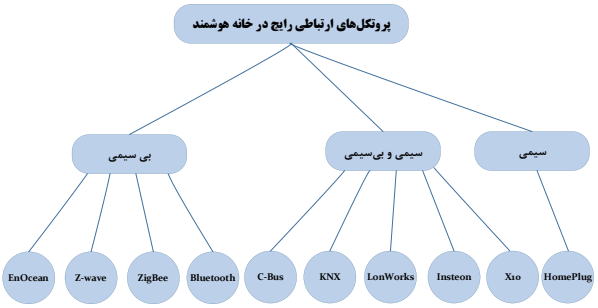
**نحوه ارجاع به مقاله: الهام توکلی، علیرضا کشاورز حداد، «مروری بر ویژگی‌های فناوری‌های ارتباطی در خانه‌های هوشمند و چالش‌های پیش‌رو»، مجله محاسبات نرم، جلد ۱۱، شماره ۲، صفحات ۳۶ـ۵۳، پاییز و زمستان ۱۴۰۱.**

شبکه ارتباطی میان تجهیزات خانگی مطرح و به طور گسترده از سیستم‌ها و ابزارهای کامپیوتری جهت هوشمندسازی خانه‌ها استفاده شده است. خانه‌های هوشمند شامل امکانات ارتباطی، سرگرمی، امنیتی، آسایشی و اطلاعاتی و همچنین خدماتی برای افراد معلول و سالمند می‌باشد که تحت یک ساختار شبکه‌ای به یکدیگر متصل شده‌اند. خانه هوشمند تنها به معنای مکانی با تعدادی وسیله که وظایف و کارهای خاصی را انجام می‌دهند نیست، بلکه سیستم توزیع شده‌ای است شامل موجودیت‌هایی که در کنار یکدیگر کار می‌کنند و با هم همکاری دارند. برای این منظور، وسایل و سیستم‌ها نه تنها باید به یکدیگر وصل باشند، بلکه باید توانایی انجام اجرای کارهای مشترک را داشته باشند که به این توانایی «قابلیت همکاری» می‌گویند. به عبارت دیگر، شبکه خانه هوشمند شامل زیرسیستم‌های ناهمگونی است که نیازمند برقراری ارتباط و تبادل داده با یکدیگر هستند تا بتوانند وظایف مشترکی را به درستی اجرا کنند. برای انجام این کار باید به دو مساله پرداخته شود: اول برقراری ارتباط بین تجهیزات خانگی و دوم همکاری و انجام وظایف مشترک میان آنها است [۴].

فناوری‌های ارتباطی که تاکنون برای خانه‌های هوشمند توسعه یافته‌اند به دو دسته کلی قابل تقسیم هستند: (۱) فناوری‌هایی که در آنها نیازی به کابل‌کشی مجزا جهت ارتباطات تجهیزات خانگی مختلف وجود ندارند و اطلاعات آنها از طریق خطوط برق داخل ساختمان و یا با کمک امواج رادیویی منتقل می‌شود که فناوری بی‌سیم نامیده می‌شود و (۲) فناوری‌هایی که در آنها برای تبادل اطلاعات و کنترل وسایل و ادوات مختلف نیاز به یک شبکه کابلی اختصاصی است که فناوری سیمی گفته می‌شود [۵]، [۶].

در یک دسته‌بندی دیگر فناوری‌های ارتباطی خانه هوشمند را می‌توان به سه دسته سیمی، بی‌سیم و ترکیب سیمی و بی‌سیم تقسیم کرد. در شکل (۱)، بر اساس مطالعات انجام شده، پروتکل‌های ارتباطی در خانه‌های هوشمند دسته‌بندی و نمایش داده شده است.

در سال‌های اخیر برخی مقالات مروری در زمینه فناوری‌های خانه هوشمند منتشر شده که روی موضوعات متفاوتی تمرکز داشته‌اند. برای مثال، در مراجع [۷] و [۸]، با توجه به نیازمندی‌های فنی و علایق مشتریان، اهداف، سیاست‌های توسعه‌ای، مخاطرات پیش‌رو برای شرکت‌های سازنده تجهیزات مورد بحث قرار گرفته است. در مرجع [۸] به روش‌های کاهش مصرف انرژی با اجرای رویکرد زمانبندی برای فناوری‌های ارتباطی خانه هوشمند پرداخته شده است. در مراجع [۹] و [۱۰] مروری روی موضوع امنیت و حفظ حریم شخصی در این فناوری‌ها صورت گرفته است. همچنین در مراجع [۱۱] و [۱۲] با رویکردی مشابه، بحث امنیت و حفظ حریم شخصی در شبکه‌های توزیع برق و ساختار بلاک–چین بررسی شده است.




**شکل (۱): دسته‌بندی فناوری‌های رایج در خانه هوشمند**

در این مقاله سعی شده با تمرکز روی فناوری‌های ارتباطی رایج در خانه‌های هوشمند، ضمن معرفی هر فناوری به ویژگی‌های فنی، معایب و محدودیت‌های هر یک پرداخته شود. به علاوه، به نکات کاربردی در پیاده‌سازی هر فناوری بیان شده و چالش‌های پیش‌رو و موضوعات پژوهشی قابل طرح برای توسعه فناوری مطرح گردیده است. همچنین به مهم‌ترین تحلیل‌های موجود در مقالات در زمینه تاخیر، نرخ تلفات بسته‌ها و بروندهی شبکه برای برخی از این فناوری‌ها اشاره می‌شود. البته به دلیل آن که اغلب فناوری‌های ارتباطی خانه‌های هوشمند خاص منظوره و انحصاری هستند، تا کنون تحلیلی برای عملکرد آنها در مقالات علمی ارائه نشده است. در آخر، با تعریف برخی معیارهای کاربردی شامل محدودیت‌های ساختاری شبکه، هزینه تمام شده، سادگی در نصب و اجرا، سازگاری با فناوری‌های دیگر، مقیاس‌پذیری در تعداد تجهیزات هوشمند، تکامل‌پذیری در ارتقا سیستم‌های موجود و امنیت ارتباطات، این فناوری‌های ارتباطی

خانه هوشمند با یکدیگر مقایسه شده‌اند. نتایج مقایسه به طراحان خانه‌های هوشمند کمک می‌کند تا با توجه به نیازمندی و شرایط موجود در هر خانه، از فناوری‌های مناسب ارتباطی جهت رسیدن به اهداف خود بهره ببرند.

ادامه مطالب این مقاله در سه بخش ارائه می‌گردد. در بخش دوم مقاله به فناوری‌های ارتباطی سیمی پرداخته می‌شود. در بخش سوم فناوری‌های بی‌سیم در خانه‌های هوشمند تشریح می‌شود. همچنین توضیحات هر فناوری در یک زیربخش جداگانه ارائه می‌شود. در بخش آخر به اختصار فناوری‌های مختلف با یکدیگر مقایسه شده و نتیجه‌گیری‌های نهایی ارائه می‌گردد.

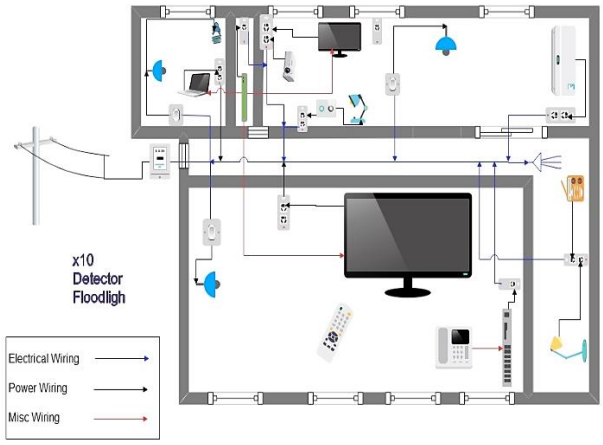
قبل از پرداختن به فناوری‌های مختلف چند واژه فنی مرتبط با موضوع را بیان می‌کنیم. متن باز بودن یک استاندارد به این معنا است که جزئیات فنی استاندارد منتشر شده و در اختیار همگان است. همچنین افراد مجازند که راهکارهای خود را نیز به آن بیافزایند. برای ارسال سیگنال روی هر بستر مخابراتی نیاز است از شکل موج‌های خاصی استفاده شود که به این کار در مدولاسیون سیگنال گفته می‌شود. همچنین برای کنترل خطا در هنگام ارسال، از روش‌های کدگذاری کانال استفاده می‌شود.

## ۲. فناوری‌های ارتباطات سیمی

در این بخش به بررسی فناوری‌های ارتباطی در خانه هوشمند مبتنی بر سیم‌کشی‌های خطوط برق ساختمان یا کابل‌کشی‌های اختصاصی جهت انتقال داده پرداخته می‌شود.

### ۱.۲. فناوری X10

یکی از فناوری‌های معروف و قدیمی برای انتقال داده روی بستر سیم‌کشی برق ساختمان، X10 می‌باشد. این فناوری به دلیل سهولت استفاده و قابلیت اطمینان بالا، به سرعت در اروپا فراگیر شده است و اخیرا نیز در حال گسترش در آسیا است. فناوری X10 یک زبان ساده جهت ارتباط تجهیزات اتوماسیون خانگی با یکدیگر تعریف کرده و اطلاعات را با مدولاسیون و کدگذاری مناسب روی خطوط برق ارسال می‌کند. این فناوری همه منظوره یک استاندارد باز برای تمامی بخش‌های اتوماسیون خانگی شامل تجهیزات امنیتی، کنترل وسایل و کنترل روشنایی محسوب می‌شود [۱۳]. در شکل (۲) هوشمندسازی خانه بر مبنای پروتکل X10 نمایش داده شده است.




**شکل (۲): هوشمندسازی خانه بر مبنای پروتکل X10**

ساختار شبکه ارتباطی X10 شامل دو نوع سخت‌افزار است:

- واحدهای X10: این واحدها برای کنترل وسایل به آنها افزوده می‌شوند و به طور معمول روی سوکت‌های برق نصب می‌شوند.
- کنترل‌کننده X10: این تجهیز پیام‌های کنترلی را برای واحدهای X10 می‌فرستند و بر روی بستر ارتباطی پاسخ‌ها را دریافت می‌کند. برای کنترل وسایل خانه می‌توان از چند کنترل‌کننده X10 نیز استفاده نمود.

کنترل‌کننده‌های X10 در سه دسته با قابلیت‌های متفاوت عرضه شده است:

- کنترل‌کننده‌های کوچک که به خطوط برق وصل شده و برای فرمان گرفتن از کاربران ساخته شده‌اند و اغلب آنها برای نمایش وضعیت وسایل دارای صفحه نمایش‌اند.
- کنترل‌کننده‌های بی‌سیم که بر روی خطوط برق نصب شده و دارای ارتباط رادیویی هستند و کاربران از طریق یک کنترل از راه دور به آنها فرمان می‌دهند.
- کنترل‌کننده کامپیوتری که به طور معمول از واسطهای خطوط برق و کابل سریال RS232 به کاربران اجازه می‌دهند که از طریق یک برنامه کاربردی نصب شده روی

کامپیوتر تنظیمات و دستورات را به آنها بدهند.

آدرس‌دهی در X10 بر اساس کد خانه و کد واحد انجام می‌شود. به عنوان مثال اگر کلیدی روی ریموت کنترل شما برای آدرس D8 تنظیم شده باشد، کلیه ماژول‌هایی که با این آدرس تعریف شده باشد، توسط این کلید روشن و خاموش می‌شود. تلفیق کد خانه و کد واحد امکان استفاده از ۲۵۶ تجهیز را در یک منزل فراهم می‌کند. از مزایای X10 می‌توان به موارد زیر اشاره کرد:

۱. عدم نیاز به سیم‌کشی اضافی در خانه
۲. هزینه پایین برای پیاده‌سازی
۳. سادگی نصب و راه‌اندازی
۴. سازگاری با بسیاری محصولات تجاری.

البته X10 معایبی هم دارد، برای مثال:

۱. محدودیت ۲۵۶ تایی برای آدرسی‌دهی تجهیزات
۲. نرخ ارسال داده بسیار پایین ارتباطات
۳. مشخص نبودن نوع تجهیز خانگی در پروتکل ارتباطی
۴. عدم مدیریت تصادم[1] پیام‌ها: اگر دو پیام X10 به صورت تقریبی همزمان ارسال شوند، به دلیل بروز تصادم، گیرنده‌ها قادر به دریافت پیام نخواهد بود. تصادم به شرایطی اطلاق می‌شود که در آن دو یا چند تجهیز در زمان تقریبا یکسانی بر روی یک رسانه مشترک داده ارسال کنند و تداخل سیگنال‌های آنها باعث از دست رفتن داده‌ها شود. پس از تصادم، هر تجهیز پس از یک وقفه کوتاه مجدد تلاش می‌کند تا داده خود را ارسال کند.
۵. عدم وجود رویکرد اطمینان از رسیدن و اجرای فرمان
۶. مشکل تداخل پیام: زمانی که فردی در خانه خود پیامی ارسال کند و سیگنال داده او به خانه دیگری وارد شود، ممکن است این فرمان به اشتباه در آنجا نیز به طریقی دیگر اجرا گردد. برای حل این مشکل لازم است فیلترهای الکترونیکی در ورودی خانه‌ها نصب شود.
۷. نویزی بودن خطوط برق که باعث پایین آمدن سطح اطمینان در این فناوری می‌شود.
۸. وجود ترانسفورماتور در میان مسیر ارتباطی یا داخل وسایل خانه، باعث تضعیف شدید سیگنال X10 می‌شود و در برخی وسایل برقی نظیر بخاری‌ها و خشک‌کن‌ها ممکن است باعث خاموش و روشن شدن ناخواسته آنها گردد. به علاوه، روی وسایل مدرن امروزی نظیر تلویزیون و کامپیوتر فیلترهای نویزگیری و منابع تغذیه خاصی وجود دارد که ممکن است به دلیل عدم سازگاری با X10، سیگنال آن را از بین ببرند [۱۴]، [۱۵].

با توجه به موارد فوق، برای توسعه X10 لازم است توسعه فناوری جهت کاهش تداخل در پیام‌ها در زیرلایه مک[2] و بهبود نرخ ارسال و مقابله با نویز با ارتقا مدولاسیون و کدگذاری در لایه فیزیکی اتفاق بیفتد. همچنین، باید در ساختار پیام‌ها تغییراتی اساسی در جهت بزرگتر کردن فضای آدرس و تعریف کردن نوع تجهیزات خانگی ایجاد شود.

### ۲.۲. فناوری Insteon

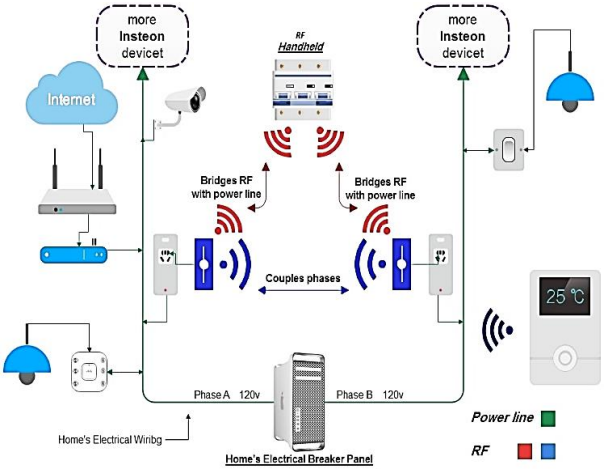
فناوری Insteon با هدف رفع ایرادات پروتکل X10 و کوتاه کردن زمان پاسخ و قابلیت اطمینان و پایداری بالا در انتقال داده ایجاد شد. برای رسیدن این هدف Insteon از ترکیب سیم‌کشی برق و ارتباطات رادیویی استفاده می‌کند [۱۳]، [۱۵]، [۱۶].

تجهیزات این فناوری اولین بار در سال ۲۰۰۵ توسط شرکت اسمارت لب[3] ارائه شده و با علامت تجاری Insteon ثبت گردید. این فناوری امکان ایجاد یک شبکه نقطه-به-نقطه برای اتوماسیون خانگی با هزینه و پیچیدگی کم و قابلیت اطمینان بالا را فراهم می‌کند. در شبکه ارتباطی Insteon همه گره‌ها قابلیت ارتباط با یکدیگر را دارند و نیازی به یک کنترل‌کننده اصلی، نرم‌افزار مسیریاب پیچیده، گیرنده یا فرستنده یا تکرارکننده پیام‌ها نمی‌باشد. نکته جالب اینجاست که اضافه کردن وسایل به شبکه ارتباطی Insteon آن را بهبود می‌دهد، چرا که وسایل پیام‌های یکدیگر را تکرار می‌کنند و بنابراین وسایل بیشتر، سیگنال‌های قوی‌تر و همچنین مسیرهای انتقال بیشتری را فراهم می‌کنند. البته

[1] Collision

[2] MAC
[3] Smartlabs

Insteon با محدود کردن تعداد تکرارهای پیام از کپی‌های بی‌رویه جلوگیری می‌کند [۱۳]، [۱۷]. به علاوه، در Insteon قابلیت اتصال به شبکه‌های ارتباطی دیگری نظیر اینترنت، وای‌فای[1]، تلفن و همچنین سایر فناوری‌ها HomePlug، Z-Wave، ZigBee و بلوتوث[2] وجود دارد. همچنین فناوری Insteon با X10 سازگاری کامل دارد. البته وسایل مجهز به Insteon سیگنال‌های وسایل X10 را دریافت و ارسال می‌کنند ولی آنها را تقویت نمی‌کنند. در شکل (۳)، ارتباطات دستگاه‌های Insteon نمایش داده شده است.




**شکل(۳): ساختار شبکه Insteon**

ویژگی‌های فنی فناوری Insteon عبارتند از:

۱. پاسخ‌دهی سریع: وسایل Insteon بدون تاخیر به فرمان‌ها پاسخ می‌دهند،
۲. نصب آسان و بدون نیاز به سیم‌کشی اضافی،
۳. قابلیت اطمینان بالا به دلیل تکرار پیام‌ها توسط وسایل مختلف،
۴. هزینه‌ی پایین پیاده‌سازی به دلیل نبود کنترل‌کننده‌های خاص یا الگوریتم‌های مسیریابی پیچیده،
۵. سازگاری با سایر فناوری‌ها همچون HomePlug، Z-Wave، ZigBee و بلوتوث،
۶. نرخ ارسال انتقال نسبتا خوب (۲۸۸۰ بیت بر ثانیه)،
۷. استفاده از هر دو بستر مخابراتی خطوط برق و امواج رادیویی [۱۳]، [۱۷].

موارد فوق نشان‌دهنده بلوغ کافی در طراحی Insteon می‌باشد. البته هنوز نیاز است که نرخ ارسال اطلاعات در Insteon بهبود یابد و با توجه به تکرار پیام‌ها توسط تمام گره‌های شبکه، عملکرد شبکه Insteon روی تعداد بالای وسایل و پیام‌ها مورد تحلیل و بررسی قرار گیرد. همچنین نیاز است رویکردهای اصلاحی برای محدود کردن تکرارها با توجه به جایگاه گره‌های شبکه ارائه شود.

### ۳.۲. فناوری LonWorks

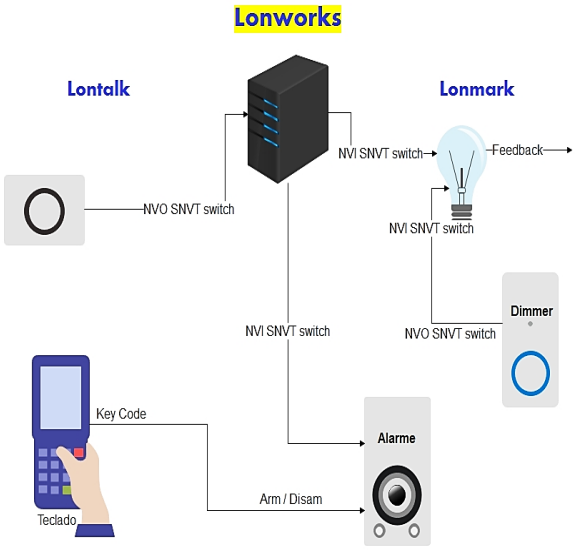
فناوری LonWorks انتخابی ارزان برای اتصال و شبکه‌سازی میان تجهیزات خانه‌های هوشمند می‌باشد. این فناوری می‌تواند یک شبکه نقطه-به-نقطه و همه منظوره از وسایل هوشمند ایجاد کرده و از واسط‌های ارتباطی مختلف نظیر کابل‌های هم‌محور، زوج سیم بهم تابیده، فیبر، خطوط برق و ارتباطات رادیویی و مادون قرمز استفاده کند. فناوری LonWorks مبتنی بر طراحی سیگنال، مسیریاب‌ها، نرم‌افزار مدیریت شبکه، روی تراشه شرکت Echelon می‌باشد. همچنین Altera تراشه‌های خاصی با نام Nios برای قابلیت همکاری میان سیستم‌ها طراحی و تولید نموده است. از طرف دیگر شرکت موتورولا[3] سهامدار عمده شرکت Echelon شده و موافقت‌نامه‌هایی را با سایر سازندگان تراشه برای اعطای مجوز تولید دارد. به علاوه، شرکت توشیبا[4] نیز در تولید تراشه‌ها وارد همکاری شده است.

در فناوری LonWorks همه لایه‌های مدل مرجع OSI طراحی شده و پروتکل ارتباطی آن که به صورت نرم‌افزاری دائمی در تراشه‌های نورون[5] و فرستنده گیرنده‌های هوشمند پیاده‌سازی شده است. هر تراشه نورون سه کنترلر کوچک را در خود جای داده است که هر یک از این کنترلرها مسئول توابعی مطابق لایه‌های خاص مدل مرجع OSI است. کنترلر اول کنترل و

[1] WiFi
[2] Bluetooth
[3] Motorola
[4] Toshiba
[5] Neuron

پردازش در لایه فیزیکی را پیاده‌سازی می‌کند. کنترلر دوم مسیریابی و آدرس‌دهی شبکه (معادل لایه ۳ تا ۶) را مدیریت می‌کند. کنترلر سوم جهت اجرای سرویس‌های سیستم‌عامل و برنامه‌های کاربر استفاده می‌شود. هر گره شبکه شامل یک حسگر/ محرک، تراشه نورون با یک کد شناسایی ۴۸ بیتی یکتا بوده و همچنین یک فرستنده و گیرنده که به واسط فیزیکی متصل هستند [۱۸].

نصب شبکه کنترل LonWorks بسیار ساده است زیرا از یک پروتکل استاندارد و واسط شبکه با قابلیت همکاری استفاده می‌کند. فرآیند نصب شامل اتصال وسایل به یک واسط فیزیکی و توصیف وسایل و ابزارهای مرتبط به یکدیگر می‌باشد. ممکن است بسته به ابعاد شبکه و حجم ترافیک مسیریاب‌هایی برای اتصال وسایل افزوده شود. برای تسهیل مسیریابی پیام‌ها، در پروتکل LonTalk آدرس‌دهی سلسله مراتبی با استفاده از آدرس‌های دامنه، زیرسیستم و گره تعریف شده است. هر گره به طور فیزیکی به یک کانال روی یکی بسترهای خطوط برق، فیبر نوری، ارتباط رادیویی و غیره متصل است. در شکل (۴)، شبکه LonWorks نمایش داده شده است.




**شکل (۴): شبکه LonWorks**

ویژگی‌های فنی LonWorks عبارتند از:

۱. درجه بالایی از قابلیت همکاری: یک گره LonWorks از اجزا استاندارد LonMarks استفاده می‌کند که درجه بالایی از قابلیت همکاری را تضمین می‌کنند.

۲. کاهش هزینه‌های نصب: در بسیاری از کاربردها، یک شبکه جدید می‌تواند بر روی بستر سیم‌کشی موجود افزوده شود. البته در مقایسه با X10 گران‌تر است.

۳. سادگی توسعه نرم‌افزارها: از آنجا که برنامه‌ها توزیع شده هستند، وظایف نرم‌افزارها می‌توانند به قسمت‌های کوچک‌تر و برنامه‌های قابل مدیریت شکسته شوند.

۴. توسعه سریع سیستم‌های جدید: فناوری LonWorks ارتباطات را مدیریت می‌کند و کافیست طراحان سیستم بر روی کارکرد مناسب برنامه‌ها تمرکز کنند.

۵. آزادی عمل در انتخاب بسترهای ارتباطی: در LonWorks از ارتباطات مختلف همچون سیم، رادیویی و غیره می‌توان بهره برد.

از معایب LonWorks می‌توان به موارد زیر اشاره کرد:

۱. پروتکل این فناوری باز نبوده و اختصاصی است.

۲. نیازمند سخت‌افزار خاص (تراشه نورون) است.

۳. برنامه‌های افزودنی تنها با هماهنگی با کنسرسیوم LonMarks مجاز است.

۴. استفاده از معماری ساده باعث شده که وسایل نیازمند اتصال به یک دستگاه کنترل جداگانه باشند.

۵. اکثر طراحان این نوع معماری را توصیه نمی‌کنند، زیرا وقفه‌های شبکه می‌تواند باعث خرابی وسایل شود [۱۸].

۶. در سیستم‌های اتوماسیون ساختمان از فناوری LonWorks بیشتر استفاده می‌شود [۱۹].

با توجه به موارد فوق، اختصاصی بودن سخت‌افزار و مسیریابی پیچیده چالش اصلی استفاده از فناوری LonWorks محسوب می‌شود. جهت رفع این مسائل، بهتر است نسخه جدید از این فناوری طراحی و توسعه یابد که با معماری‌های باز نظیر IP و تجهیزات مربوطه آن سازگار باشد.

در مرجع [۲۰]، برای مدل‌سازی زیرلایه مک[1] در LonWorks

[1] Medium Access Control

از زنجیره مارکوف[1] استفاده شده است. با در نظر گرفتن متغیرهای تعریف شده در استاندارد LonWorks، اگر احتمال تصادم بسته‌ها ($p$) و احتمال ارسال یک بسته در هر برش زمانی ($\tau$) باشد، می‌توان به سادگی نشان داد که احتمال تصادم $p$ بر حسب $\tau$ به صورت زیر قابل محاسبه می‌باشد:

$$p = 1 - (1 - \tau)^{n-1} \qquad (۱)$$

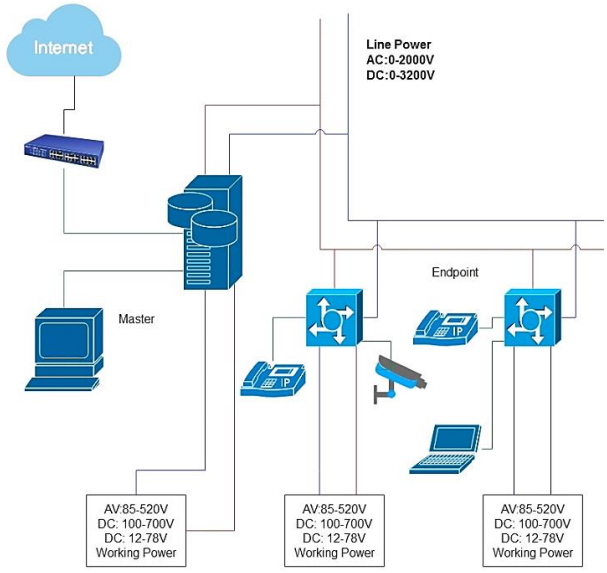
که در این رابطه، $n$ نشاندهنده تعداد گره‌های فعال روی شبکه LonWorks می‌باشد.

### ۴.۲. فناوری HomePlug

فناوری HomePlug به منظور توسعه ارتباطات وسایل خانگی با یکدیگر و اینترنت روی بستر خطوط برق ایجاد شد. حساسیت پایین HomePlug به نویز الکتریکی روی خطوط برق با افزایش فرکانس حامل سیگنال ارتباطی و نرخ ارسال بالا ویژگی‌های اصلی این فناوری محسوب می‌شود.

اولین نسخه HomePlug، با نام HomePlug1.0، در سال ۲۰۰۱ منتشر شد. در ادامه در سال ۲۰۰۵، HomePlugAV (برای داده‌های صوتی-تصویری) ارائه شد که لایه فیزیکی آن نرخ داده‌ها را از حدود ۱۳ مگابیت بر ثانیه به ۲۰۰ مگابیت بر ثانیه افزایش داد [۱۸]. پس از آن، HomePlug Green PHY در سال ۲۰۱۰ عرضه شد و برنامه‌های کاربردی شبکه هوشمند برق به عنوان یک فناوری سازگار با HomePlugAV را با هزینه و مصرف انرژی کمتر و کاهش توان عملیاتی فراهم نمود. در همین سال، موسسه IEEE1901 به تصویب رسید و HomePlugAV به عنوان پایه فناوری برای استاندارد داخلی FFT-OFDM PHY تبدیل به یک استاندارد بین‌المللی شد. HomePlug کلیه محصولات استاندارد IEEE1901 سازگار با سه نسخه HomePlugAV، HomePlug Green PHY و HomePlug AV2 را شامل می‌شود [۲۱].

استاندارد HomePlug C&C بر روی مدل مرجع OSI طراحی شده است. این استاندارد به همراه HomePlug1.0 قابلیت پهنای باند و هزینه کم ارتباطی با اطمینان بالا را برای برنامه‌های محیط خانه هوشمند فراهم می‌کند. وسایل HomePlug C&C صرف‌نظر از نوع محصول، فروشنده و برنامه با یکدیگر قابلیت همکاری دارند. پشته پروتکل HomePlug C&C به لایه پیوند داده متصل بوده و توابع و سرویس‌های متمم را فراهم می‌کند. برای این کار HomePlug C&C مدل هفت لایه‌ای OSI را به دو لایه میزبان و واسط تقسیم می‌کند. لایه واسط شامل سه لایه اول مدل مرجع است یعنی لایه فیزیکی، لایه پیوند داده یا مک و لایه شبکه که انتقال داده‌ها، کشف و کنترل خطا و مسیریابی را به عهده دارند. لایه میزبان شامل چهار لایه بالاتر است که زبان توصیف رایج را برای تعریف وسایل در رابطه با سرویس‌ها پشتیبانی شده، خاصیت‌ها و فعالیت‌های سرویس و قسمت‌هایی همچون اجرای پروفایل وسایل و اتصال سرویس‌های لایه‌های پایین‌تر ارائه می‌دهد. در شکل (۵)، ساختار شبکه ارتباطی HomePlug نمایش داده شده است.




**شکل (۵): فناوری HomePlug**

برخی مزایای HomePlug C&C عبارتند از:

۱. سرعت انتقال اطلاعات بالا و توانایی آدرس‌دهی ۲۵۶۰۰ وسیله روی شبکه
۲. قابلیت انتقال تصویر، داده و تلفن بر روی یک باس
۳. قابلیت اضافه شدن به هر وسیله و برنامه در خانه هوشمند

[1] Markov Chain

۴. نصب راحت و ایجاد شبکه امن بدون نیاز به مهارت یا فرآیند پیچیده
۵. قابلیت همکاری بین وسایل از تولیدکنندگان متفاوت با توسعه دادن پشته پروتکلی
۶. امکان آغاز ارتباطات توسط هر وسیله یا برنامه و همچنین امکان ارسال وضعیت به مبدا پیام [۱۸].
۷. برای مواردی که نیاز به ارسال داده روی زوج سیم برای طول بالای ۱۰۰ متر باشد، اترنت قابل استفاده نیست، اما از مودم‌های HomePlug می‌توان استفاده نمود [۲۲].

معایب HomePlug عبارتند از:

۱. ضرورت اتصال به پریز برق در این فناوری بسیار محدودکننده است.
۲. نباید آداپتور HomePlug را به تجهیز محافظ برق نظیر کاهش‌دهنده ولتاژ[1] یا تهویه مطبوع[2] متصل باشد، زیرا احتمالا سیگنال‌های آن از بین می‌روند.
۳. در صورتی که به تجهیز کامپیوتری با پورت USB متصل شده باشد، باید یک آداپتور HomePlug بزرگ و جاگیر نیز استفاده شود.
۴. به طور معمول آداپتور PC Cardها مجهز به HomePlug نیست [۱۸].

با توجه به محدودیت‌های فوق به نظر می‌رسد استفاده از سایر بسترها نظیر امواج رادیویی و سیم‌کشی‌های اختصاصی می‌تواند فناوری HomePlug را تا حد زیادی بهبود دهد. البته لازم است راه‌های مسیریابی برای وسایل خانگی که مجهز به چندین واسط ارتباطی هستند، اصلاح گردد.

در مرجع [۲۳]، مدل‌های موجود برای تحلیل زیرلایه مک در استاندارد HomePlug مورد بررسی قرار گرفته و از مدل زنجیره مارکوف، رابطه‌ای مشابه با رابطه (۱)، برای احتمال ارسال بسته در یک برش زمانی و احتمال تصادم بسته‌ها استخراج شده است. همچنین با فرض اینکه نرخ تولید بسته‌ها در شبکه $\lambda$ باشد، تابع توزیع طول صف (بافر) در هر گره تعیین شده است. همچنین میزان بروندهی هر گره با فرض داشتن بافری با طول نامتناهی، به صورت زیر به دست آمده است:

$$s = \rho \frac{L}{\chi} \qquad (۲)$$

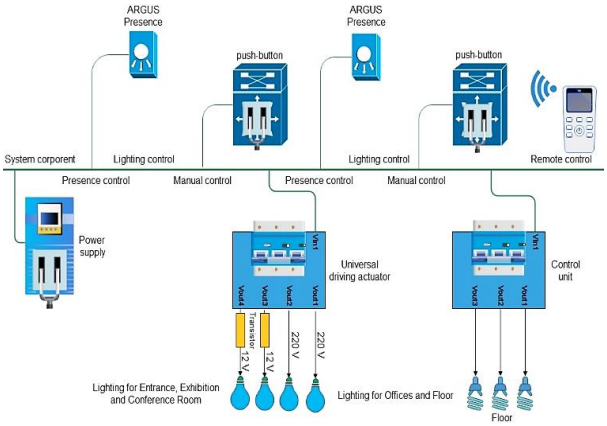
که در این رابطه، $L$ طول بسته‌ها، $\rho$ میانگین طول صف و $\chi$ میانگین زمان مورد نیاز برای آزاد کردن یک بسته می‌باشد.

## ۵.۲. فناوری KNX

فناوری KNX یک استاندارد بر مبنای مدل لایه‌بندی OSI بوده و در واقع یک پروتکل شبکه است. این فناوری جهت ایجاد همگرایی و تجمیع سه استاندارد قدیمی زیر برای خانه‌های هوشمند در اتحادیه اروپا ایجاد شده است [۱۵]:

۱. پروتکل سیستم خانه اروپا (EHS)[3]
۲. Bati BUS
۳. نصب باس اروپایی (EIB)[4]

فناوری مورد استفاده در دستگاه‌های KNX جدید با سیستم قدیمی IRB سازگار بوده، بنابراین تمام تجهیزات پشتیبانی‌کننده KNX یا IRB به طور متقابل سازگار هستند. فناوری KNX فارغ از هرگونه سکوی سخت‌افزاری طراحی شده است. یک وسیله در شبکه KNX می‌تواند توسط هر سخت‌افزاری از یک میکروکنترلر ۸ بیتی تا یک کامپیوتر شخصی کنترل شود [۲۴]. در شکل (۶)، معماری KNX نمایش داده شده است.




**شکل (۶): معماری پروتکل KNX**

[1] Surge Suppressor
[2] Line Conditioner
[3] European Home System Protocol (EHS)
[4] European Installation BUS (EIB)

تجهیزات KNX قابلیت‌های مختلفی دارند که عبارتند از:

- قابلیت حالت خودکار: آنها به صورت خودکار خود را برنامه‌ریزی می‌نمایند و نصب آنها ساده است.
- قابلیت حالت آسان: به آموزش‌های ابتدایی برای نصب نیاز دارند. رفتار آنها از پیش برنامه‌ریزی شده و متغیرهای قابل برنامه‌ریزی دارند که متناسب با نیاز کاربر تعریف می‌شوند.
- قابلیت حالت سیستم: در ساخت سیستم‌های اتوماسیون سفارشی بکار گرفته می‌شوند. تجهیزات حالت سیستم هیچ پیش‌فرض اولیه‌ای نداشته و توسط تکنسین‌های مجرب نصب و برنامه‌ریزی می‌شوند.

بسترهای ارتباطی زیر در KNX قابل استفاده هستند:

- بستر زوج-سیم TP: این بستر بیشتر در فرانسه کاربرد دارد و امروزه اکثر سازندگان به TP1 روی آورده‌اند.
- بستر زوج-سیم TP1: بیشتر از ۹۰٪ از محصولات فعلی KNX بر این مبنا هستند. در TP1 انتقال اطلاعات با کیفیت بالا و با قیمت پایین فراهم شده است. توپولوژی TP1 بسیار انعطاف‌پذیر بوده و شامل خطی، ستاره‌ای، درختی و یا تلفیقی از آنها است. برای ارسال اطلاعات، یک سیگنال کد شده در باند پایه با نرخ انتقال ۹۶۰۰ بیت بر ثانیه در نظر گرفته شده است. تجهیزاتی که به TP1 متصل می‌شوند، می‌توانند از طریق باس اصلی تغذیه شوند.
- فناوری خطوط برق PL110: در حال حاضر شرکت‌های محدودی PL110 را پشتیبانی می‌کنند اما کماکان یک بازه کامل از محصولات را برای روشنایی، پرده و کرکره‌ها، سیستم‌های سرمایشی و گرمایشی ارائه می‌دهد و دارای نرخ ارسال اطلاعات ۱۲۰۰ بیت بر ثانیه می‌باشد.
- فناوری خطوط برق PL132: امروزه این فناوری توسط سازندگان کمتری تولید می‌شود. نرخ ارسال اطلاعات در آن ۲۴۰۰ بیت بر ثانیه می‌باشد. در عمل، در حال حاضر محصولاتی برای این استاندارد تولید نمی‌شود و احتمال دارد در آینده، کنار گذاشته شود.
- فناوری KNXRF: این فناوری، در خانواده KNX یک فناوری تازه‌وارد محسوب می‌شود. پیش‌بینی می‌شود در آینده نزدیک بسیاری از تولیدکنندگان به این استاندارد روی بیاورند. این فناوری از امواج رادیویی با فرکانس حامل ۸۶۸/۳۰ مگاهرتز و نرخ ارسال اطلاعات ۱۶۳۸۴ بیت بر ثانیه (تقریبا برابر با TP1) استفاده می‌کند [۱۵]، [۲۵].
- پروتکل اینترنتی KNX net/IP: اخیرا به عنوان یکی از بسترهای KNX معرفی شده است و از آنجا که مطابق پروتکل IP طراحی شده انتظار می‌رود در آینده به یکی از مهم‌ترین بسترهای انتقال اطلاعات تبدیل شود.

ویژگی‌های فنی KNX عبارتند از:

۱. باز بودن پروتکل: امکان ارتباط با دیگر تجهیزات سیستم جامع مدیریت ساختمان وجود دارد.
۲. عمر بالای تجهیزات: در رله‌های مکانیکی تا سه میلیون بار و سایر تجهیزات الکتریکی تا یک میلیون بار عملکرد را پشتیبانی می‌کنند.
۳. امنیت بالای شبکه: از کلیدهای رمزنگاری به اندازه کافی بزرگ استفاده می‌کند.
۴. قابل کنترل با نرم‌افزار گرافیکی توسط کامپیوتر: کلیه مکان‌ها به صورت گرافیکی نمایش می‌دهد.
۵. ایمنی بالا در استفاده: با بکارگیری ولتاژ ۲۹ ولت در محل کلیدهای کنترلی.
۶. نویزپذیری و نویزگذاری خیلی پایین: به دلیل استفاده از کابل‌های مجزا و شیلددار.
۷. انعطاف‌پذیری: هر وسیله یک ریزپردازنده دارد که باعث انعطاف‌پذیری سیستم در تغییر دادن آنها می‌شود.
۸. تنوع پیاده‌سازی: KNX می‌تواند به شکل‌های مختلف برای کاربردهای مختلف داخل یک خانه پیاده‌سازی شود [۲۶].

محدودیت‌ها و معایب KNX شامل موارد زیر است:

۱. پروتکل KNX و تجهیزات هوشمند آن برای مشتری‌های غیرحرفه‌ای بسیار پیچیده است. برنامه‌نویسی با پروتکل KNX شبیه توسعه برنامه پایگاه داده می‌باشد و نیازمند تخصص بالا و صرف زمان زیادی است.

۲. برنامه نوشته شده هر ماژول قابل رویت برای برنامه‌نویس بعدی که به منزل برای خدمات مراجعه می‌کند، نبوده و در صورت اصلاح یک برنامه در ماژول امکان از بین رفتن برنامه قبلی وجود دارد. لذا برای جلوگیری از بروز مشکلات در اجرای درخواست‌های مصرف‌کننده هر نوع برنامه‌ریزی ماژول‌ها باید در آرشیو شرکت فروشنده بایگانی شود و برنامه‌نویس در زمان مراجعه برای ارائه خدمات، فایل برنامه را به همراه داشته باشد [۱۷]، [۲۴].

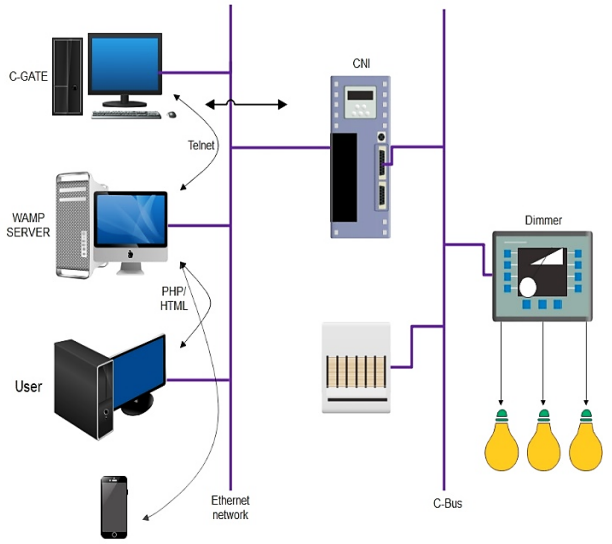
با توجه به نکات گفته شده، KNX از نظر ارتباطات فناوری جامع و انعطاف‌پذیری محسوب می‌شود. اما بخش نرم‌افزاری این فناوری نیاز به اصلاحات اساسی جهت تسهیل برنامه‌ریزی و عیب‌یابی وسایل مختلف دارد.

## ۶.۲. فناوری C-BUS

فناوری C-BUS یک پروتکل ارتباطی بر اساس مدل هفت لایه‌ای OSI است و در آمریکا تحت نام D-Square شناخته می‌شود. فناوری C-BUS در سیستم‌های هوشمند خانگی و سیستم‌های کنترل روشنایی ساختمان‌های تجاری استفاده می‌شود. این فناوری از یک کابل ولتاژ پایین اختصاصی و یا شبکه بی‌سیم برای ارسال پیام‌های کنترلی استفاده می‌کند و امکان انتقال داده بین این دو بستر وجود دارد. این امر قابلیت اطمینان ارتباطات را بالا برده و آن را نسبت به سایر فناوری‌ها نظیر X10 برای ساختارهای بزرگ کاربردی‌تر می‌کند.

سیستم کابلی C-BUS از کابل‌های استاندارد Cat-5 UTP استفاده می‌کند و نیازی به قطع‌کننده جریان در پایان خط ندارد. شرکت Clipsal نوع خاصی از کابل‌ها Cat-5 را برای استفاده در پنل‌های توزیع برق تولید می‌کند و به منظور اطمینان از جداسازی الکتریکی کافی بین ولتاژ اصلی برق موجود در پنل‌های توزیع و سیگنال‌های ضعیف C-BUS ساخته شده است. در خارج از پنل‌های توزیع می‌توان از کابل‌های استاندارد دسته Cat-5 UTP استفاده کرد. سیم‌کشی شبکه C-BUS از یک طرح معماری باز استفاده می‌کند. حداکثر طول کابل می‌تواند ۱۰۰۰ متر باشد و با استفاده از تجهیز پل[1] می‌توان طول را افزایش داد.

حداکثر ۲۲۵ شبکه C-BUS در یک تاسیسات می‌تواند وجود داشته باشد. البته اگر از فناوری اترنت C-BUS استفاده شود، این محدودیت رفع می‌شود. بیشترین تعداد شبکه‌هایی که به طور سری به شبکه محلی، توسط پل‌ها متصل هستند، می‌تواند ۷ عدد باشد. هر بخش از شبکه C-BUS برای به راه افتادن نیاز به جریان الکتریکی ۱۸ میلی‌آمپر و ولتاژ ۱۵ تا ۳۶ ولت دارد، در حالی که برخی از بخش‌های C-BUS ممکن است تا ۴۰ میلی‌آمپر مصرف کنند. البته می‌توان روی شبکه C-BUS بیش از یک منبع تغذیه قرار داد. به علاوه، هر شبکه C-BUS نیازمند حداقل یک مولد زمان برای هماهنگ‌سازی گره‌ها می‌باشد. در شکل (۷)، سیستم C-BUS نمایش داده شده است.




**شکل (۷): سیستم C-BUS**

ویژگی‌های فنی C-BUS عبارتند از:

۱. سرعت انتقال اطلاعات بسیار بالا (۲۰۰ مگابیت بر ثانیه)

[1] Bridge

۲. عمر تجهیزات ۳۰۰۰۰۰ بار است (البته عمر مفید آنها ۱۰ برابر کمتر از KNX است) [۱۳].

محدودیت‌ها و معایب C-BUS عبارتند از:

۱. هزینه اجرای پروژه بالاست.
۲. تنها یک شرکت سازنده دارد (وابستگی مصرف‌کننده به یک شرکت و محصولات آن) و انتخاب چندانی برای مشتریان وجود ندارد.

با توجه به نکات بحث شده، چالش اصلی فناوری C-BUS عدم سازگاری آن با سایر فناوری‌های ارتباطی خانه‌های هوشمند است. لذا جهت توسعه این فناوری لازم است که تجهیزات درگاهی خاصی جهت برقراری ارتباط میان شبکه‌های C-BUS و سایر شبکه‌ها نظیر X10، KNX، LonWorks و HomePlug طراحی و ساخته شود. همچنین ساخت واسط ارتباطی جدید برای بهره‌گیری از خطوط برق برای انتقال اطلاعات در مواردی که وسایل نیاز به نرخ ارسال اطلاعات بالا ندارند، می‌تواند این فناوری را کاربردی‌تر سازد.

## ۳. فناوری‌های بی‌سیم

در این بخش، به فناوری‌های ارتباطی بی‌سیم در خانه‌های هوشمند پرداخته می‌شود.

### ۱.۳. فناوری بلوتوث

فناوری بلوتوث یک ارتباط کم هزینه بی‌سیم برای وسایل قابل حمل با حداکثر نرخ ارسال داده حدود ۱ مگابیت بر ثانیه در فاصله کمتر از ۱۰۰ متر فراهم می‌کند. ساختار سخت‌افزاری بلوتوث همانند دیگر سیستم‌های بی‌سیم، شامل بخش‌های ارتباطات رادیویی، پردازش پروتکل و یک ریزپردازنده با حافظه ROM یا حافظه فلش برای نگهداری اطلاعات است [۲۷]، [۲۸]. در فناوری بلوتوث، ارتباطات پایه مبتنی بر Piconet است که از یک گره کارگزار[1] و حداکثر هفت گره پیرو[2] فعال تشکیل شده است. در یک خانه ممکن است چند Piconet باشد که از طریق گروه‌هایی که نقش پل را ایفا می‌کنند، به هم متصل شوند (شکل ۸ را مشاهده کنید). دقت داشته باشید که به مجموعه‌ای از پیکونت‌های متصل به هم Scatternet گفته می‌شود.

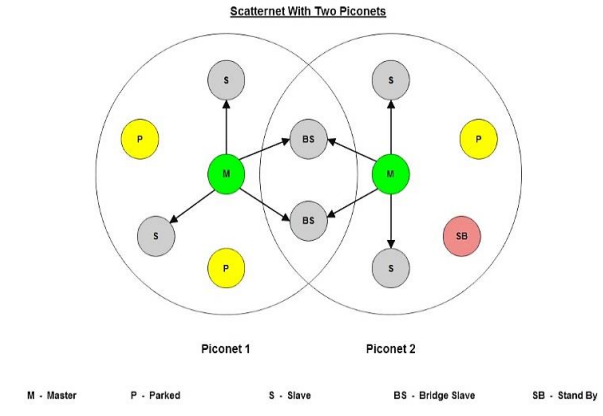
در یک Piconet علاوه بر ۷ گره فعال پیرو، ممکن است تا ۲۵۵ گره غیرفعال وجود داشته باشد. این گره‌ها وسایلی هستند که گروه اصلی آنها را در حالت استراحت و کم توان قرار داده تا مصرف باطری آن کاهش یابد. یک ایستگاه در حالت غیرفعال هیچ کاری انجام نمی‌دهد و فقط به سیگنال فعال‌سازی خود یا سیگنال Beacon که از گروه کارگزار می‌رسد، پاسخ می‌دهد. گره‌های پیرو (مثل صفحه کلیدها، موس و چابگر) تقریبا غیرهوشمند و ساده هستند و اساسا آنچه را که گره کارگزار به آنها دستور بدهد، اجرا می‌کنند. زمانبندی ارسال‌ها در Piconet مبتنی بر TDM است که در آن گروه کارگزار بر سیگنال ساعت نظارت دارد و تعیین می‌کند که چه دستگاه‌های و در کدام برش زمانی مخابره داشته باشد. تبادل اطلاعات صرفا بین گره کارگزار و گروه‌های پیرو انجام می‌شود و ارتباط مستقیم دو گره پیرو ممکن نیست [۲۷].

بلوتوث از باند رادیویی ISM ۲/۴ گیگاهرتز برای ارتباطات خود استفاده می‌کند و بر پایه خصوصیات زیر بنا شده است:

۱. محدوده اسمی مورد نیاز ۱۰ متر و قدرت سیگنال آن صفر دسی‌بل‌میلی‌وات تنظیم شده است. البته امکان تقویت شدن به وسیله تقویت‌کننده منبع خارجی تا ۱۰۰ متر با قدرت مثبت ۲۰ دسی‌بل‌میلی‌وات را دارد.
۲. استفاده از فناوری طیف گسترده FHSS که سیگنال آن ۱۶۰۰ بار در ثانیه، فرکانس حامل جلوگیری از تداخل ناخواسته را تغییر می‌دهد.
۳. پشتیبانی از USB، UART و واسط‌های معمولی صوت دیجیتال PCM.
۴. حداکثر نرخ انتقال داده (ناهمزمان) ۷۳۲ کیلوبیت بر ثانیه یا ارسال صوت دوطرفه (همزمان) ۴۲۳ کیلوبیت بر ثانیه روی یک ارتباط واحد.

[1] Master
[2] Active Slave Node

۵. دستگاه‌های مجهز به تراشه‌های بلوتوث به طور خودکار یکدیگر را تشخیص داده و ارتباط برقرار می‌کنند.
۶. فناوری بلوتوث انرژی کمی برای برقراری ارتباط نیاز دارد. هر سیگنال که گوشی تلفن همراه دریافت می‌کند، فقط ۱ میلی‌وات از باتری آن را مصرف می‌کند.




**شکل (۸) : معماری شبکه فناوری بلوتوث**

در مرجع [۲۹]، لایه فیزیکی و زیرلایه مک فناوری بلوتوث بررسی و تحلیل شده است. میزان بروندهی شبکه از رابطه زیر قابل محاسبه می‌باشد:

$$s = \frac{L}{connInterval} \qquad (۳)$$

که در آن، $L$ طول بسته (تعداد بیت‌ها) و $connInterval$ فاصله زمانی بین دو رویداد متوالی می‌باشد که ضریبی از ۱/۲۵ میلی‌ثانیه است که حداقل آن ۷/۵ میلی‌ثانیه و حداکثر آن ۴ ثانیه است.

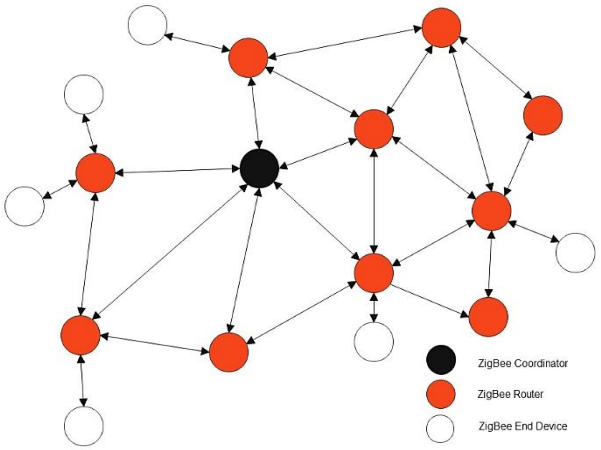
مسائل تعیین آدرس و رمزگذاری در لایه فیزیکی بلوتوث انجام می‌شود. برای این منظور بلوتوث یک رویکرد چالش–پاسخ و یک کلید رمزنگاری که با یک شماره شناسایی شخصی (PIN) که کاربر ایجاد کرده را استفاده می‌کند. این امر سبب می‌شود که کاربر قادر باشد ارتباط را برقرار نماید و همچنین امکان تولید دنباله‌ای از کلیدهای رمزنگاری برای انتقال داده‌های بعدی را داشته باشد. مانند هر سیستم رمزنگاری دیگری در بلوتوث کلیدهای طولانی از کلیدهای کوتاه امن‌تر هستند. اگر هکری بتواند کلید عبور را کشف کند، می‌تواند کلیدهای آغازین را محاسبه کند. در واقع، استفاده از کلید آغازین جایگزین پیوندهای رمزنگاری یک نقطه ضعف اساسی در این فناوری محسوب می‌شود. بنابراین بهتر است که ارتباطات اولیه هر دو دستگاه بلوتوث در محل امنی صورت بگیرد. چرا که مهاجم می‌تواند داده‌های انتقالی که بر روی یک دستگاه بلوتوث فرستاده می‌شود را ضبط کرده و از آن برای دست یافتن به PIN استفاده نماید. همچنین استفاده از یک کلید عبوری ثابت و کوتاه در تمام مواقع نیز می‌تواند امنیت یک ارتباط بلوتوث را به خطر بیندازد. بهترین حالت امنیتی این است که از کلیدهای پیچیده ترکیبی استفاده شود [۱۳]، [۱۸]، [۳۰]، [۳۱].

با توجه به نکات فوق، امنیت یک چالش اصلی برای فناوری بلوتوث می‌باشد. به دلیل تنوع زیاد وسایلی که با این فناوری کار می‌کنند، جهت رفع این مشکل می‌بایست از رویکردهای امنیتی تکمیلی نظیر رمزنگاری انتها–به–انتها در لایه کاربرد تجهیزات بهره برد. ساختار کوچک Piconet و محدودیت نرخ ارسال اطلاعات از ایرادات بنیادین بلوتوث برای استفاده در خانه‌های هوشمند محسوب می‌شوند. لذا بهتر است یکی دیگر از فناوری‌های ارتباطی به عنوان زیرساخت ارتباطات در خانه هوشمند استفاده شود و از بلوتوث فقط برای ارتباط وسایل با زیرساخت استفاده گردد.

### ۲.۳. فناوری ZigBee

فناوری ZigBee برای ارتباطات شبکه‌ای بی‌سیم برد کوتاه کم هزینه توسعه یافته است. این فناوری از فرستنده و گیرنده‌های دیجیتال کم مصرف برای شبکه‌های شخصی بی‌سیم با نرخ ارسال داده پایین استفاده می‌کند. فناوری ZigBee به منظور تعریف یک فناوری ساده‌تر، ارزان‌تر و انعطاف‌پذیرتر از بلوتوث به وجود آمده است. با ZigBee می‌توان بیش از ۶۴۰۰۰ وسیله را در یک شبکه به هم متصل نمود. این استاندارد به دلیل فقدان فناوری‌هایی با نرخ ارسال کم و سیکل اتصال پایین نظیر ارتباطات خانه هوشمند ایجاد شده است. همچنین فناوری ZigBee برای محیط کنترل متمرکز که تعداد زیادی وسیله یا حسگرهایی مبتنی بر باتری وجود دارد و حجم داده کمی رد و بدل می‌شود، مناسب است [۱۷]، [۳۲].

در ZigBee سه نوع گره در شبکه تعریف می‌شود: (۱) گره هماهنگ‌کننده که بر آرایش و امنیت شبکه نظارت می‌کند، (۲) گره‌های با قابلیت کارکرد کامل که به صورت مسیریاب‌های معمولی استفاده می‌شوند و برای پشتیبانی از توپولوژی‌های مختلف استفاده می‌شود و (۳) گره‌های با قابلیت کارکرد کم که در گوشه‌های شبکه می‌توانند مورد استفاده قرار گیرند و عملکردهای حسی یا کنترلی خاص دارند. با این سه نوع وسیله، ZigBee می‌تواند از طیفی از طرح‌های شبکه شامل ستاره و درخت خوشه و مش پشتیبانی کند. ساختار شبکه ZigBee در شکل (۹) نمایش داده شده است.




**شکل (۹): شبکه ZigBee**

ویژگی‌های فنی ZigBee عبارتند از:

۱. کار در محدوده فرکانس ۲/۴ گیگاهرتز با سرعت انتقال ۲۵۰ کیلوبیت بر ثانیه، همچنین ممکن است از بازه فرکانسی ۹۱۵ مگاهرتز در آمریکا با سرعت ۴۰ کیلوبیت بر ثانیه و ۸۶۸ مگاهرتز در اروپا با سرعت ۲۰ کیلو بیت بر ثانیه استفاده شود.
۲. برد ۱۰ تا ۱۰۰ متر با توجه به قدرت فرستنده و ویژگی‌های محیط.
۳. مصرف توان کم، نرخ ارسال پایین، امنیت و قابلیت اطمینان بالا.
۴. امکان پشتیبانی از بیش از ۶۵۶۳۵ وسیله در هر شبکه.
۵. انعطاف در شبکه‌بندی با توپولوژی‌های چندگانه نظیر مش.
۶. قابلیت تعریف به عنوان دستگاه انتهایی و حالت خواب برای کاهش مصرف انرژی.
۷. تعریف پروفایل‌های مختلف برای برقراری ارتباط بین دستگاه‌ها به صورت بهینه [۲۸]، [۳۳].

برخی از معایب عمده فناوری ZigBee عبارتند از:

۱. راه‌اندازی شبکه ZigBee به دستگاه‌های اضافی نیاز دارد که هزینه را افزایش می‌دهد.
۲. لوازم خانگی که فناوری ZigBee را اجرا می‌کنند با سایر فناوری‌های شبکه نظیر WiFi سازگار هستند و اصولا نیازی به این فناوری در خانه‌های هوشمند نیست.
۳. فناوری ZigBee دارای نرخ انتقال داده کم است و پشتیبانی از پروتکل IP را ندارد [۱۳]، [۳۲]، [۳۴].

با توجه به موارد ویژگی‌های فنی ZigBee، می‌توان گفت در طراحی این فناوری بی‌سیم، بلوغ کافی وجود داشته است و نکات مهمی نظیر مقیاس‌پذیری، مصرف انرژی و امنیت در آن کاملا لحاظ شده است. تنها چالش مهم این فناوری، سرعت انتقال اطلاعات در آن است که در طراحی و ساخت درگاه ارتباطی میان ZigBee و سایر پروتکل‌های ارتباطی خانه‌های هوشمند می‌توان این مشکل را برطرف نمود. زیرا می‌توان بخشی از ارتباطات خانه هوشمند که نیازمند سرعت بالا است را با استفاده از یک فناوری دیگر پیاده‌سازی نمود.

در مرجع [۳۵]، عملکرد زیرلایه مک فناوری ZigBee بررسی شده و مشابه کارهای تحلیلی اشاره شده در فناوری‌های قبل، از زنجیره مارکوف برای مدل‌سازی تصادم استفاده شده است. میزان بروندهی شبکه از رابطه (۴) که در زیر نشان داده شده است، به دست می‌آید:

$$s = \frac{E[successful\ data\ tranmission]}{E[time\ interval]} \qquad (۴)$$

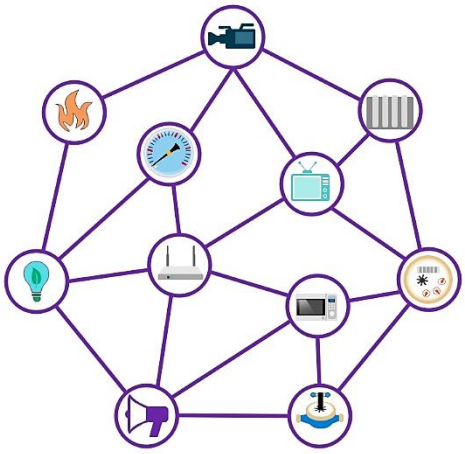
علاوه بر این، این مرجع با مدل‌سازی مصرف انرژی برای ارسال و دریافت بسته‌های داده و بسته‌های تصدیق، فرمولی برای میانگین مصرف انرژی گره‌ها ارائه کرده است. همچنین در مرجع [۳۶]، یک روش خوشه‌بندی برای کاهش انرژی در شبکه مبتنی بر فناوری ZigBee ارائه شده است.

### ۳.۳. فناوری Z-Wave

فناوری Z-Wave یک فناوری ارتباطی بی‌سیم برای کاربردهایی مانند اتوماسیون خانگی و شبکه‌های حسگر می‌باشد که توسط شرکت‌های Zensys و Z-Wave ارائه شده است. این فناوری برای توان و پهنای باندهای کم طراحی شده است. این فناوری یک شبکه با کیفیت بالا و قیمتی که معادل کسری از قیمت فناوری‌های مشابه آن می‌باشد را در اختیار کاربران می‌گذارد. این امر با تمرکز بر روی استفاده از پهنای باند کم و جایگزینی سخت‌افزارهای گران قیمت با روش‌های نرم‌افزاری امکان‌پذیر شده است. این فناوری مبتنی بر یک پشته پروتکلی کوچک به منظور ایجاد قابلیت اطمینان بالا ارائه شده است [۲۷]. فناوری شبکه مش برای Z-Wave می‌تواند دستورات را به صورت دوطرفه از یک وسیله به وسیله دیگری منتقل نماید، حتی در شرایطی که موانع و یا نقاط کور رادیویی در محل موجود باشد. فناوری Z-Wave به صورت تراشه‌هایی در دسترس است و پروتکل آن درون تراشه جاسازی شده است. همچنین در آن یک حافظه فلش جهت استفاده تولیدکنندگان محصولات برای بارگذاری نرم‌افزارها تعبیه شده است و برخی از اطلاعات سخت‌افزار آن در اختیار عموم قرار داده شده است. به دلیل این که Z-Wave روی فرکانس مخصوصی کار می‌کند با هیچ یک از دیگر وسایل بی‌سیم مثل تلفن‌ها و مودم‌ها تداخل فرکانسی ندارد. توپولوژی مش شبکه Z-Wave پوششی به مراتب بیش از یک خانه را فراهم می‌کند. البته از آنجا که تجهیزات Z-Wave برای ارسال سیگنال نباید در حالت خواب باشند، اکثر دستگاه‌هایی که با باتری کار می‌کنند، به عنوان تکرارکننده استفاده نمی‌شوند. یک شبکه می‌تواند شامل ۱۳۲ گره باشد که این تعداد با ایجاد پل میان شبکه‌ها قابل افزایش خواهد بود [۳۷]. در شکل (۱۰)، ساختار شبکه مش فناوری Z-Wave نمایش داده شده است.

ویژگی‌های فنی Z-Wave عبارتند از:

۱. سادگی نصب و آدرس‌دهی خودکار برای مدیریت شبکه
۲. هزینه کم به دلیل تجمیع سیستم بر روی یک تراشه.
۳. مصرف برق بسیار پایین با کمک پشته پروتکلی کوچک و ساختار فریم فشرده شده.
۴. ابعاد بسیار کوچک سخت‌افزار که آن را برای مجتمع شدن با دیگر وسایل مناسب می‌کند.
۵. عملکرد خوب در جلوگیری از تداخل‌ها و نویزها با پشتیبانی از دو روش تایید، الگوریتم عقب‌گرد و پرهیز از تصادم.
۶. نرخ ارسال اطلاعات مناسب (۴۰ کیلو بیت بر ثانیه).
۷. استفاده از باند فرکانسی اختصاصی ۸۶۸ مگاهرتز.



**شکل (۱۰): ارتباطات Z-Wave**

البته در Z-Wave رویکردهای امنیتی مناسبی پیاده‌سازی نشده است [۱۳]، [۱۸]. بنابراین برای توسعه این فناوری بی‌سیم می‌بایست طراحی پروتکل‌های امنیتی برای آن در اولویت قرار داده شود. نرخ ارسال اطلاعات در Z-Wave کم است و برای برخی کاربردهای انتقال اطلاعات صوت و تصویر مناسب نیست. همچنین برای سازگاری و قابلیت همکاری Z-Wave با سایر فناوری‌های ارتباطی خانه‌های هوشمند تاکنون کاری انجام نشده است. لذا بهتر است درگاه‌های ارتباطی میان Z-Wave و

سایر فناوری‌ها طراحی و تولید شود تا در بخشی از ارتباطات در خانه‌های هوشمند که نیازمند سرعت بالاتر هستند، از سایر فناوری‌های ارتباطی بتوان بهره برد.

### ۴.۳. فناوری EnOcean

فناوری EnOcean در سال‌های اخیر توسط شرکتی با همین نام معرفی شده است. این فناوری ارتباط بی‌سیم مبتنی بر برداشت انرژی است. بوردهای الکترونیکی EnOcean توان مصرفی بسیار ناچیزی دارند و قادرند از طریق نور یا دمایی که از محیط جذب می‌کنند توان مورد نیاز جهت برقراری ارتباطات رادیویی را تامین کنند. برد رادیویی گره‌های EnOcean در فضای باز به ۳۰۰ متر و در داخل ساختمان به ۳۰ متر می‌رسد و بسته‌های داده در آن با طول ۱۴ بایت و با نرخ ۱۲۵ کیلوبیت بر ثانیه ارسال می‌شود [۳۸].

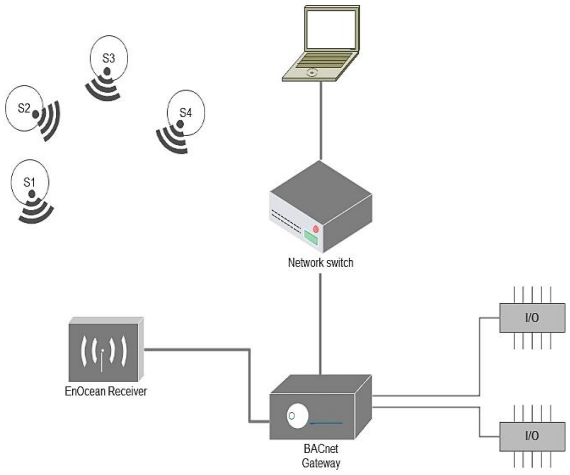
کاربرد اصلی این فناوری در خانه هوشمند برای مواردی است که قصد نداشته باشیم توان گره‌ها را از طریق برق یا باتری تامین کنیم. برای مثال می‌توان از این فناوری در حسگرهای نشت گاز، دما، رطوبت، روشنایی، و غیره استفاده نمود. توجه داشته باشید که این فناوری در خانه هوشمند به عنوان یک فناوری ارتباطی مستقل استفاده نمی‌شود، بلکه برای برقراری برخی از ارتباطات نظیر جمع‌آوری داده‌های حسگرها کاربرد دارد. برای نمونه در شکل (۱۱)، ساختار شبکه ارتباطی EnOcean در یک ساختمان هوشمند در کنار فناوری BACnet نمایش داده شده است.

مزیت اصلی این فناوری نسبت به سایر فناوری‌ها، عدم نیاز گره‌های آن به باتری و برق جهت تامین انرژی است. لذا گره‌ها می‌توانند در هر گوشه از دیوار یا سقف اتاق‌ها نصب شوند. در مقابل، ایراد اصلی این فناوری محدودیت‌های آن در قدرت پردازش گره‌ها، میانگین نرخ ارسال داده و امکان ایجاد ساختارهای شبکه‌ای بزرگ می‌باشد. لذا این فناوری نمی‌تواند به عنوان یک فناوری مستقل در خانه‌های هوشمند با امکانات متنوع استفاده شود [۳۸].

در مرجع [۳۸]، از قضایای نظریه صف و مدل مارکوف مخفی برای مدل‌سازی زیرلایه مک استفاده شده است و فرمول احتمال تصادم بسته‌ها به دست آمده و فرمولی برای برندهی برای یک نرخ سرویس معین به صورت زیر ارائه شده است.

$$s = \sum_{d} \sum_{m} p_s(m) \lambda_m r_d \frac{1}{\mu} \qquad (۵)$$

که در آن، $m$ نشان‌دهنده کلاس داده، $d$ نشان‌دهنده نوع وسیله، $\lambda_m$ نرخ تولید بسته‌ها، $p_s(m)$ احتمال موفقیت در ارسال بسته، $r_d$ طول پنجره عقب‌نشینی پس از تصادم و $\mu$ نرخ سرویس‌دهی صف در ارسال بسته ها می‌باشد.




**شکل (۱۱): مثالی از استفاده از فناوری EnOcean در کنار شبکه BACnet [۳۹]**

### ۵.۳. مقایسه فناوری‌های ارتباطی

در جدول (۱)، فناوری‌های مورد بحث در این مقاله و استاندارد هر یک عنوان شده است و در ادامه به طور مختصر این فناوری‌ها از جنبه‌های کاربردی نظیر نوع کاربرد، سازگاری با سایر فناوری‌ها، هزینه، سادگی در پیاده‌سازی و بستر ارتباطی با یکدیگر مقایسه شده‌اند. توجه داشته باشید که معیار هزینه و سادگی در پیاده‌سازی به صورت نسبی برای نصب امکانات معمول در خانه‌های هوشمند ارائه شده است و ممکن است این معیارهای نسبی در برخی شرایط خانه‌های هوشمند اندکی متفاوت باشد.

**جدول (۱): مقایسه فناوری های ارتباطی در اتوماسیون های خانگی و صنعتی**

| نام فناوری | استاندارد | نوع کاربری | سازگاری با سایر فناوری‌ها | هزینه | پیاده‌سازی | بستر ارتباطی | چالش‌ها |
|---|---|---|---|---|---|---|---|
| KNX | ISO/IEC14543 | اتوماسیون ساختمانی | دارد | بالا | پیچیده | سیمی PLC و بی‌سیم (غیر متداول) | نقص در نرم‌افزار مدیریت تجهیزات |
| X10 | X10 Standard | اتوماسیون خانگی | دارد | پایین | ساده | سیمی | عدم اطمینان از انتقال پیام و کنترل محدود ارسال |
| LonWorks | ISO-14908 | اتوماسیون خانگی و صنعتی | دارد | متوسط | متوسط | سیمی PLC و بی‌سیم (غیر متداول) | اختصاصی بودن سخت‌افزار و پروتکل |
| ZigBee | IEEE802.15.4 | اتوماسیون خانگی و صنعتی | دارد | پایین | ساده | بی‌سیم | پایین بودن نرخ ارسال داده |
| Z-Wave | IEEE802.11 | اتوماسیون خانگی | دارد | پایین | ساده | بی‌سیم | پایین بودن نرخ ارسال داده |
| INSTEON | X10 Standard | اتوماسیون خانگی | دارد | پایین | ساده | سیمی، بی‌سیم | پایین بودن نرخ ارسال داده و تکرار بی‌رویه پیام‌ها |
| HomePlug | IEEE1901 | اتوماسیون خانگی | دارد | پایین | ساده | سیمی | نیاز هر سخت‌افزار خاص برای هر اتصال به برق |
| C-BUS | ISO/IEC 11801 | اتوماسیون خانگی و ساختمانی | ندارد | پایین | متوسط | سیمی، بی‌سیم | انحصاری بودن تجهیزات و عدم سازگاری با سایر فناوری‌ها |
| Bluetooth | IEEE802.15.1 | اتوماسیون خانگی | دارد | پایین | متوسط | بی‌سیم | محدودیت در ساختار شبکه و امنیت |
| EnOcean | ISO/IEC14543-3-10 | اتوماسیون خانگی | ندارد | پایین | ساده | بی‌سیم | محدودیت در ابعاد شبکه و عدم سازگاری با سایر فناوری‌ها |

## ۴. نتیجه‌گیری

در این مقاله به فناوری‌های ارتباطی متداول در خانه‌های هوشمند پرداخته شد. این فناوری‌ها از جهات مختلفی نظیر بستر مخابراتی (سیم‌کشی اختصاصی، سیم‌کشی برق، بی‌سیم)، تنوع در پشتیبانی تجهیزات، ساختار شبکه، مقیاس‌پذیری شبکه، امنیت و سازگاری با سایر فناوری‌های مرتبط مورد بررسی قرار داده شد. همچنین در مورد محدودیت‌های موجود و چالش‌های پیش‌رو برای توسعه هر فناوری بحث شد. بررسی‌های ما نشان می‌دهد در میان فناوری‌های مبتنی بر خطوط برق ساختمان، X10 به لحاظ ساگی، پشتیبانی از تجهیزات متنوع خانگی و سازگار با سایر فناوری‌ها از مزیت نسبی برخوردار است. در میان فناوری‌ها با سیم‌کشی اختصاصی، KNX کیفیت ارتباطات و امنیت بهتری را فراهم می‌کند. در میان فناوری بی‌سیم خانه‌های هوشمند، فناوری ZigBee از نظر مقیاس‌پذیری شبکه و امنیت مناسب‌تر است، ولی قابلیت همکاری پایینی با سایر فناوری های ارتباطی دارد. در اینجا ذکر این نکته لازم است که طبق بررسی‌ها، تمامی فناوری‌های ارتباطی متداول در خانه‌های هوشمند دارای مزایا و ویژگی‌ها و همچنین محدودیت‌های خاصی هستند، بنابراین می‌بایست طراحان سیستم‌ها بر اساس نیازمندی‌ها و شرایط موجود در ساختمان فناوری مناسب را انتخاب نمایند.

**تعارض منافع: نویسندگان اعلام می‌کنند که هیچ تعارض منافعی ندارند.**

# مراجع


[1] A.S. Al-sumaiti, M.H. Ahmed, and M.M.A. Salama, “Smart home activities: A literature review,” Electr. Power Compon. Syst., vol. 42, no. 3-4, pp. 294-305, 2014, doi: 10.1080/15325008.2013.832439.

[2] G. Graditi, M.G. Ippolito, R. Lamedica, A. Piccolo, A. Ruvio, E. Santini, P. Siano, and G. Izzo, “Innovative control logics for a rational utilization of electric loads and air-conditioning systems in a residential building,” Energy Build., vol. 102, pp. 1-17, 2015, doi: 10.1016/j.enbuild.2015.05.027.

[3] S.J. Darby, “Smart technology in the home: time for more clarity,” Build. Res. Inf., vol 46, no. 1, pp. 140-147, 2018, doi: 10.1080/09613218.2017.1301707.

[4] M. Rahimi, M. Songhorabadi, and M.H. Kashani, “Fog-based smart homes: a systematic review,” J. Netw. Comput. Appl., vol. 153, p. 102531, 2020, doi: 10.1016/j.jnca.2020.102531.

[5] M.O.B. Yassein, I. Hmeidi, F. Shatnawi, W. Mardini, and Y.M. Khamayseh, "Smart home is not smart enough to protect you- protocols, challenges and open issues,” in 10th Int. Conf. Emerg. Ubiquitous Syst. Pervasive Networks (EUSPN), Coimbra, Portugal, 2019, pp. 134-141, doi: 10.1016/j.procs.2019.09.453.

[6] P. Kumar, A. Braeken, A.V. Gurtov, J.H. Iinatti, and P.H. Ha., “Anonymous secure framework in connected smart home environments,” IEEE Trans. Inf. Forensics Secur., vol. 12, no. 4, pp. 968-979, 2017, doi: 10.1109/TIFS.2016.2647225.

[7] B.K. Sovacool and D.D.F. Del Rio, “Smart home technologies in Europe: a critical review of concepts, benefits, risks and policies,” Renew. Sustain. Energy Rev., vol. 120, p. 109663, 2020, doi: 10.1016/j.rser.2019.109663.

[8] R. El-Azab, “Smart homes: Potentials and challenges,” Clean Energy, vol. 5, no. 2, pp. 302-315, 2021, doi: 10.1093/ce/zkab010.

[9] S.N. Makhadmeh, A.T. Khader, M.A. Al-Betar, S. Naim, A.K. Abasi, and Z.A.A. Alyasseri, “Optimization methods for power scheduling problems in smart home: survey,” Renew. Sustain. Energy Rev., vol. 115, p. 109362, 2019, doi: 10.1016/j.rser.2019.109362.

[10] N. Panwar, S. Sharma, S. Mehrotra, L. Krzywiecki, and N. Venkatasubramanian, “Smart home survey on security and privacy,” arXiv preprint arXiv: 1904.05476, 2019.

[11] F. Saeidnejad and M. Majidi, “A survey on the security of communication networks used in power distribution networks,” Soft Comput. J., vol. 10, no. 2, pp. 16-31, 2022, doi: 10.22052/scj.2022.242847.0 [In Persian].

[12] H. Barangi, F. Raji, and A.A. Khasseh, “Blockchain security and privacy research analysis: a bibliometric study,” Soft Comput. J., vol. 9, no. 1, pp. 40-55, 2020, doi: 10.22052/scj.2021.111451 [In Persian].

[13] D. Mocrii, Y. Chen, and P. Musilek, “IoT-based smart homes: A review of system architecture, software, communications, privacy and security,” Internet Things, vol. 1-2, pp. 81-98, 2018, doi: 10.1016/j.iot.2018.08.009.

[14] A. Kailas, V. Cecchi, and A. Mukherjee, “Chapter 2-a survey of contemporary technologies for smart home energy management,” in Handbook of Green Information and Communication Systems, Academic Press, pp. 35-56, 2013, doi: 10.1016/B978-0-12-415844-3.00002-4.

[15] T.D.P. Mendes, R. Godina, E.M.G. Rodrigues, J.C.O. Matias, and J.P.S. Catalao, “Smart home communication technologies and applications: wireless protocol assessment for home area network resources,” Energies, vol. 8, no. 7, pp. 7279-7311, 2015, doi: 10.3390/en8077279.

[16] E. Shailendra and P.K. Bhatia, “Analyzing home automation and networking technologies,” in IEEE Potentials, vol. 37, no. 1, pp. 27-33, 2018, doi: 10.1109/MPOT.2015.2493184.

[17] M. Poulakis, S. Vassaki, G.T. Pitsiladis, C. Kourogiorgas, A. Panagopoulos, G. Gardikis, and S. Costicoglou, “Wireless sensor network management using satellite communication technologies,” in Emerging Communication Technologies Based on Wireless Sensor Networks, CRC Press, pp. 201-232, 2016, doi: 10.1201/b20085-12.

[18] R. Heartpeld, G. Loukas, S. Budimir, A. Bezemskij, J.R.J. Fontaine, A. Filippoupolitis, and E.B. Roesch, “A taxonomy of cyber- physical threats and impact in the smart home,” Comput. Secur., vol. 78, pp. 398-428, 2018, doi: 10.1016/j.cose.2018.07.011.

[19] K. Lohia, Y. Jain, C. Patel, and N. Doshi, “Open communication protocols for building automation systems,” in 10th Int. Conf. Emerg. Ubiquitous Syst. Pervasive Networks (EUSPN), Coimbra, Portugal, 2019, pp. 723-727, doi: 10.1016/j.procs.2019.11.020.

[20] M. Wang, E. Lin, E. Woertz, and M. Kam, “Collision resolution simulation for distributed control architectures using LonWorks,” in IEEE Int. Conf. Autom. Sci. Eng. (CASE) Edmonton, Alberta, Canada, 2005, pp. 319-326, doi: 10.1109/COASE.2005.1506789.

[21] L. Yonge, J. Abad, K. Afkhamie, L. Guerrieri, S. Katar, H. Lioe, P. Pagani, R. Riva, D.M. Schneider, and A. Schwager, “HomePlug AV2: next-generation broadband over power line,” in MIMO power line communications, CRC Press, pp. 391-426, 2014.

[22] A.G. Merkulov and V.P. Shuvalov, “The perspectives and practice of plc homeplug av modems application in the network devices and industrial tools,” in 1st Global Power Energy Commun. Conf. (GPECOM), Nevsehir, Turkey,

2019, pp. 46-49, doi: 10.1109/GPECOM.2019.8778575.

[23] C. Cano and D. Malone, “On efficiency and validity of previous Homeplug MAC performance analysis,” Comput. Networks, vol. 83, pp. 118-135, 2015, doi: 10.1016/j.comnet.2015.03.005.

[24] J. Vanus, J. Belesova, R. Martinek, P. Bilik, J. Zidek, and L. Koval, L., “Development of software tool for operational and technical functions control in smart home with knx technology,” IFAC-PapersOnline, vol. 49, no. 25, pp. 431-436, 2016, doi: 10.1016/j.ifacol.2016.12.088.

[25] S. Marksteiner, V. J. Exposito Jimenez, H. Valiant and H. Zeiner, "An overview of wireless IoT protocol security in the smart home domain," in Internet Things Bus. Model. Users Networks, Copenhagen, Denmark, 2017, pp. 1-8, doi: 10.1109/CTTE.2017.8260940.

[26] F. Sapundzhi, “A survey of knx implementation in building automation,” TEM J., vol. 9, no. 1, pp. 144-148, 2020, doi: 10.18421/TEM91-20.

[27] O. Horyachyy, “Comparison of wireless communication technologies used in a smart home: analysis of wireless sensor node based on Arduino in home automation scenario,” Master thesis, Faculty of Computing, Blekinge Institute of Technology, Karlskrona Sweden, 2017.

[28] V.A. Orfanos, S.D. Kaminaris, D. Piromalis, and P. Papageorgas, “Smart home automation in the iot era: a communication technologies review,” in AIP Conf. Proc., 2020, p. 20054, doi:10.1063/5.0032939.

[29] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, and D. Formica, “Performance evaluation of Bluetooth low energy: a systematic review,” Sensors, vol. 17, no. 12, p. 2898, 2017, doi: 10.3390/s17122898.

[30] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D.A. Wagner, “Smart locks: Lessons for securing commodity internet of things devices,” in Proc. 11th ACM Asia Conf. Comput. Commun. Secur. (AsiaCCS), Xi’an, China, 2016, pp. 461-472, doi: 10.1145/2897845.2897886.

[31] F. Xu, W. Diaoyz, Z. Li, J. Chen, and K. Zhang, “BadBluetooth: breaking android security mechanisms via malicious bluetooth peripherals,” in 26th Ann. Netw. Distrib. Syst. Secur. Symp. (NDSS), San Diego, California, USA, 2019.

[32] A. Hafeez, N.H. Kandil, B. Al-Omar, T. Landolsi, and A.-R. Al-Ali, “Smart home area networks protocols within the smart grid context,” J. Commun., vol. 9, no. 9, pp. 665-671, 2014, doi: 10.12720/jcm.9.9.665-671.

[33] G.M. Toschi, L.B. Campos, and C.E. Cugnasca, “Home automation networks: a survey,” Comput. Stand. Interfaces, vol. 50, pp. 42-54, 2017, doi: 10.1016/j.csi.2016.08.008.

[34] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, “Review of communication technologies for smart homes/building applications,” in IEEE Innov. Smart Grid Technol. Asia (ISGT ASIA), Bangkok, Thailand, 2015, pp. 1-6, doi: 10.1109/ISGT-Asia.2015.7437036.

[35] Z. Chen, C. Lin, H. Wen, and H. Yin, “An analytical model for evaluating IEEE 802.15. 4 CSMA/CA protocol in low-rate wireless application,” in 21st Int. Conf. Adv. Inf. Networking Appl. (AINA), vol. 2, Niagara Falls, Canada, 2007, pp. 899-904, doi: 10.1109/AINAW.2007.77.

[36] S. Tabatabaei, “An energy efficient clustering method using bat algorithm and mobile sink in wireless sensor networks,” Soft Comput. J., vol. 8, no. 2, pp. 102-115, doi: 10.22052/8.2.102 [In Persian].

[37] S.J. Danbatta and A. Varol, “Comparison of zigbee, z-wave, wi-fi, and bluetooth wireless technologies used in home automation,” in 7th Int. Symp. Digital Forensics Secur. (ISDFS), Barcelos, Portugal, 2019, pp. 1-5, doi: 10.1109/ISDFS.2019.8757472.

[38] J. Ploennigs, U. Ryssel, and K. Kabitzsch, “Performance analysis of the EnOcean wireless sensor network protocol,” in Proc. 15th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA), Bilbao, Spain, 2010, pp. 1-9, doi: 10.1109/ETFA.2010.5641313.

[39] J. Tonejc, J. Kaur, A. Karsten, and S. Wendzel, “Visualizing BACnet data to facilitate humans in building-security decision-making,” in 3rd Int. Conf. Hum. Aspects Inf. Secur. Priv. Trust, Los Angeles, CA, USA, 2015, pp.693-704, 2015, doi: 10.1007/978-3-319-20376-8_62.