**تهدیدات امنیتی خانه هوشمند در لایه  
اشیا و راه های مقابله با آن**

**ارایه دهنده : زهرا دهقانیان**

**استاد راهنما: دکتر رضا صفابخش**

**دانشگاه صنعتی امیرکبیر**

**پاییز ۹۶**

***از پدر عزیزم که در تهیه این گزارش با لطف بی حدشان مرا یاری کردند ، کمال تشکر را دارم .***

چکیده

فهرست

فصل اول : مقدمه

* 1. مقدمه .....................................................................................................................

فصل دوم : بستر تحقیق

2-1- مقدمه......................................................................................................................

2-2- نهدیدات خانه هوشمند .......................................................................................

2-3 چالش های کلیدی ................................................................................................

2-3-1 امنیت ...................................................................................................................

2-3-1-1 محرمانگی ....................................................................................................

2-3-1-2 تمامیت ..........................................................................................................

2-3-1-3 دسترسی پذیری ...........................................................................................

2-3-2 حریم خصوصی ...................................................................................................

2-4 فناوری های موجود...................................................................................................

2-4-1 zigbee.......................................................................................

2-4-2 برچسب هوشمند........................................................................................

2-4-3 ارتباطات میدان نزدیک ......................................................................................

2-4-4 شبکه های موبایلی...................................................................................................

2-4-5 بلوتوث ....................................................................................................................

2-4-6 Z-Wave ..............................................................................................................

2-5 راهکارها ......................................................................................................................

2-5-1 احراز هویت ............................................................................................................

2-5-2 حریم خصوصی .......................................................................................................

2-6 جمع بندی ....................................................................................................................

فصل سوم : نتیجه گیری و پیشنهادات

3-1 نتیجه گیری و پیشنهادات ..........................................................................................

مراجع

فهرست شکل ها

شکل 2-1 سیستم خانه هوشمند .......................................................................................

شکل 2-2 پشته پروتکلی zigbee.................................................................................

شکل 2-3 مدل شبکه zigbee........................................................................................

شکل 2-4 NFC ...................................................................................................................

شکل 2-5 پشته پروتکلی Z-Wave................................................................................

**فصل اول**

**مقدمه**

1-1 مقدمه

**فصل دوم**

**بستر تحقیق**

2-1 مقدمه

اینترنت اشیاء بستری است که در آن شبکه اینترنت موجود از سیستمهای رایانه‌ای به اشیاء یا موجودیتهای دنیای واقعی متصل هستند؛ اشیاء ممکن است شامل موجودیتها، وسایل برقی خانگی، دستگاه‌ها، ابزار و... باشد؛ وقتی این اشیاء طبق زیرساخت مشخص و پروتکلهای استاندارد خاصی به اینترنت متصل می‌شوند، «اینترنت اشیاء» نامیده می‌شود.

اشیاء در اینترنت هوشمند می‌توانند حقیقی یا مجازی و ثابت یا متحرک باشند در حالیکه اشیاء، شرکت‌کنندگان فعال در کل سیستم هستند، اشیاء، می‌توانند با یکدیگر و با انسان تعامل داشته باشند که این ارتباطات به ترتیب، ارتباط شی به شی و ارتباط شی با انسان نامیده می‌شوند.

اینترنت اشیاء شامل هشت حوزه‌ نقل‌وانتقال هوشمند، درمان هوشمند، کشاورزی هوشمند، خانه هوشمند، وسایل نقلیه هوشمند، مدرسه هوشمند، بازار هوشمند، و صنعت هوشمند است.

سیستم خانه هوشمند می‌تواند همانند آنچه در شکل 1 نشان داده شده، پیکربندی شود؛ سیستم خانه هوشمند شامل سه مؤلفه اصلی سرور خانه، دروازه خانه و دستگاه‌های خانه هوشمند است:



شکل 2-1 سیستم خانه هوشمند

ابتدا سرور‌خانه فرآیندهای ذخیره‌سازی، تجمیع و توزیع اطلاعات گردآوری شده از رسانه‌های مختلف موجود در خانه را انجام می‌دهد، سپس دروازه‌خانه، صاحب شبکه دسترسی را به شبکه خانگی متصل می‌کند؛ در نهایت دستگاه‌های خانه هوشمند قادر خواهند بود اطلاعات را میان دستگاه‌ها مبادله کرده و به اینترنت خارجی نیز دسترسی پیدا کند.

مؤلفه‌های تشکیل‌دهنده سیستم خانه هوشمند در مواجهه با تهدیدات داخلی یا خارجی قرار دارند زیرا اغلب این مؤلفه‌ها به اینترنت متصل هستند؛ برای غلبه بر چنین تهدیدات امنیتی، مانند تزریقات بدافزاری، دسترسی احراز هویت شده کاربر، افشای اطلاعات اساسی، لازم است تمهیدات امنیتی مطابق بر مشخصه‌های مؤلفه‌ای سیستم خانه هوشمند به کار گرفته شود.

2-2 تهدیدات خانه هوشمند

خانه های هوشمند از مؤلفه های متعددی تشکیل شده اند؛ این مؤلفه ها همواره در معرض تهدیدات مختلفی قرار دارند. حملات خانه های هوشمند به هفت گروه تقسیم شده اند که عبارتند از:

١- **حملات فیزیکی:** به دستکاری فیزیکی دستگاه ها اطلاق می شود؛ این حملات می تواند به انواع مختلفی از خطرات مانند فعالیت، سوءاستفاده نابهنجار یا استراق سمع، ممانعت یا سرقت منجر شود؛ معمولا یک حمله فیزیکی تمامی اموال را تحت تأثیر قرار می دهد.

٢- **خسارات ناخواسته (تصادفی) :** ممکن است از اطمینان نادرست و نابجا به افراد و آشنایان یا اشتباهات شخصی (مدیریتی، طراحی، عملکرد وغیره) ناشی شود؛ می تواند مراتب جبران ناپذیری همچون نشر اطلاعات، تغییرات غیرمعتبر یا حتی فقدان اطلاعات را با خود به همراه داشته باشد.

٣- **فجایع و قطع برق:** انکار خدمات برای کاربر را با خود به همراه دارد.

۴- **آسیب و فقدان:** نه تنها منجر به تخریب سرویس می شود، بلکه نشر اطلاعات را با خود به همراه دارد؛ در واقع باعث حذف اطلاعات حیاتی می شود.

۵- **خرابیها و بد عملکردها:** مهمترین نقطه شروع حمله توسط مهاجم است؛ مهاجم با بهره جویی از این فرصت، مبادرت به فعالیت، سوءاستفاده نابهنجار و استراق سمع، ممانعت و سرقت می کند.

۶- **استراق سمع، ممانعت و سرقت:** سوءاستفاده ناهنجار به تهدیدات سایبری و نیز حریم شخصی مربوط می شود؛ این دو مقوله به عنوان تهدیدات امنیتی در نظر گرفته می شود؛ مهاجم با تغییر طراحی یا به کارگیری نواقص، یک یا چند دارایی و موجودیت را به خطر خواهد انداخت که در نتیجه منجر به نقض محرمانگی داده های خصوصی یا از دست دادن کنترل یک دستگاه خواهد شد.

٧- **قانونی:** این نوع تهدید مراتبی همچون تهدیدات گذشته خواهد داشت اما نسبت به سایر تهدیدات از وقوع کمتری برخوردار است

2-3 چالش های کلیدی

# زمانی که تمامی اشیاء اطراف انسان قابلیت کاربرد اینترنت را پیدا نموده و در نهایت مفهوم اینترنت اشیاء محقق گردد، انواع جدیدي ازکاربردها موجود خواهند بود. دو مبحث امنیت و حریم خصوصی به عنوان دو مولفه اساسی و مهم در حوزه اینترنت اشیاءنقش پررنگی در این کاربرد ها خواهند که در ادامه به این دو مهم میپردازیم.

2-3-1 امنیت اطلاعات

امنیت اصلی ترین نگرانی شبکه هاي است که در مقیاس بزرگ پیاده سازي می شوند. دنیاي دیجیتال، با داده هاي شخصی و اشتراکی و ثبت شده توسط افراد اشباع شده است و نگرانی هایی را در زمینه امنیت و حفاظت از اطلاعات افراد و دولت ها فراهم کرده است. همچنین مشکلات ناشی شده از انتقال و پردازش داده هاي ناخواسته، موجب نگرانی هاي کاربران و مسائل قانونی شده است. در صورت نقض امنیت ، رخداد حمله و اختلال در عملکرد ، مزایاي هوشمندسازی کمرنگ میشود . چنانچه هکرها کنترل شبکه را به عهده بگیرند رویدادهاي ناگواري به وقوع خواهد پیوست. براي مثال با در دست گرفتن کنترل درب خانه توسط نفوذگران به شبکه می تواند زمینه سرقت از خانه را فراهم کند .

به طور کلی، سرویسهاي امنیتی که در این حوزه قرار است ارائه شوند باید ویژگی هاي محرمانگی، تمامیت و دسترسی پذیری را فراهم نمایند. در ادامه به بررسی این عناصر می پردازیم :

**2-3-1-1 محرمانگی**:

اولین قدم براي برقراري امنیت، برآورد محرمانگی است. محرمانگی بدین معنی است که مهاجم نباید هیچ دانشی از محتواي پیام هاي تبادلی مابین موجودیت هاي حاضر در اینترنت اشیاء همانند یک گرهي حسگر و هر موجودیت اینترنتی دیگري به دست آورد.

# 2-3-1-2 تمامیت :

# در حالت کلی در مبحث امنیت ، موجودیتی "تمام" است که سه ویژگی زیر را داشته باشد :

# یکپارچگی: در تمامی مراحل ارتباط ، داده رد و بدل شده باید بدون تغییر باقی بماند. به عبارت دیگر، هرگونه تغییر )احتمالی( در پیامها باید توسط گیرنده پیام قابل تشخیص باشد.

# تازگی: این ویژگی تضمین می کند که پیامهاي قدیمیتر تکرار نمیشوند. این امر به جهت تضمین کانال ارتباطی در مقابل حملات تکرار مهم است.

# صحت : این ویژگی نیز تضمین کننده ی درستی اطلاعات در تمامی مراحل ارتباط می باشد.

# 2-3-1-3 دسترسی پذیری:

اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند. این بدان معنی است که باید از درست کار کردن و جلوگیری از اختلال در سیستم‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد. سیستم‌های با دسترسی بالا در همه حال حتی به علت قطع برق، خرابی سخت‌افزار، و ارتقاء سیستم در دسترس باقی می‌ماند. یکی از راههای از دسترس خارج کردن اطلاعات و سیستم اطلاعاتی درخواست‌های زیاد از طریق خدمات از سیستم اطلاعاتی است که در این حالت چون سیستم توانایی و ظرفیت چنین حجم انبوه خدمات دهی را ندارد از سرویس دادن بطور کامل یا جزیی عاجز می‌ماند.

**2-3-2 حریم خصوصی**

مفهوم حریم خصوصی همواره همراه با امنیت به کار برده شده است، اما در این تحقیق مناسب است که توجه جداگانه اي به آن شود؛ چرا که در اینترنت اشیاء اطلاعات خصوصی بیشتري نسبت به وضعیت کنونی بر روي شبکه قرار می گیرد. حریم خصوصی شامل قابلیت پنهان نگهداشتن اطلاعات شخصی و همچنین توانایی کنترل آنچه با این اطلاعات اتفاق می افتد است. طبیعت اشیاء متصل و کاربردهاي گسترده، متنوع و همه جا حاضر اینترنت اشیاء و از همه مهمتر، تأثیر این اشیاء در بالابردن کیفیت زندگی باعث نفوذ روزافزون آنها در زندگی روزمرهي انسانها میگردد؛ از طرفی دیگر، چنین سیستمهایی که فعالیتهاي روزانهي افراد را جمع آوري و ثبت می نمایند میتوانند به آسانی به عنوان سیستمهاي جاسوسی و استراق سمع توزیع شده مورد استفاده قرار گیرند.

به دلیل آنکه اطلاعات مربوط به فعالیتهاي روزانهي کاربران )براي نمونه مسیرهاي مسافرتی، عادتهاي خریدکردن و غیره( توسط بسیاري از انسانها در زمره اطلاعات شخصی و محرمانه در نظر گرفته می شوند که نباید فاش شوند، حفظ حریم خصوصی یکی از ملزومات کاربردهاي همه جا حاضر محسوب میگردد . هرچند بسیاري از مردم در ارتباط با موج جدید فناوري که در حال آمدن است یک جنبه احتیاطی در پیشگرفته اند؛ اما واقعیت این است که این دستگاهها به گونه اي طراحی شده اند تا اطلاعات شخصی زندگی انسان را با بیشترین جزییات ممکن، جمع آوري کنند.برای مثال یکی از این اطلاعات خصوصی، سبک زندگی افراد است؛ این که چه ساعاتی را در خانه به سر می بریم، به کجا مسافرت می کنیم، با چه کسانی معاشرت می کنیم، چه فیلم هایی تماشا می کنیم و حتی این که چه غذایی میخوریم .

کمی خطرناک به نظر میرسد،که ما به سرعت اقدام به طراحی و بازیابی راه حلهایی با هدف بهبود زندگی روزمره شهروندان داشته باشیم؛ به طوريکه برخی از جنبه هاي حریم خصوصی یا امنیت اطلاعات را در این زمینه نادیده بگیریم.

ضمن اینکه فناوري هاي کلیدي اینترنت اشیا هنوز به بلوغ خود نرسیده اند و همچنین تحقیقات و کاربردهاي اینترنت اشیا در مراحل اولیه خود هستند. پس براي حضور و فراگیر شدن اینترنت اشیا در زندگی روزمره،

امنیت و و حریم خصوصی باید به طور جدي تري در نظر گرفته شود.

**2-4 فناوری های موجود**

در اینترنت اشیا براي ارتباط و تعامل اشیا با یکدیگر و با شبکه اینترنت فناوري هاي متفاوتی وجود دارد که در اینجا جدیدترین فناوري هاي مورد نیازبراي پیاده سازي آن را معرفی می کنیم.

**2-4-1 Zigbee**

فناوري zigbee جزء فناوري هاي نو ظهوري می باشد که در سال هاي اخیر رشد چشمگیري داشته است. نام zigbee از الگوي غیر ترتیبی زیگزاگی که زنبورها حین گرده افشانی دنبال می کنند، گرفته شده است. . zigbee یک پروتکل مبتنی بر استاندارد IEEE802.15.4 براي کنترل و نظارت بر اهداف و سیستم هایی است که به نرخ بالاي ارسال داده نیاز نداشته ولی هزینه پایین و جریان مصرفی کم از ملزومات آنها به شمار می آید. در این فناوري نود ها می توانند تا زمانی که بی استفاده هستند در حالت خواب قرار بگیرند. zigbee به منظور تعریف یک تکنولوژي ساده تر، ارزانتر و موثرتر از بلوتوث در مصرف انرژي و طول عمر، براي شبکه هاي شخصی بیسیم بوجود آمده است. به کمک Zigbeeمی توان بیش از 64000 وسیله را بطور بیسیم از طریق شبکه به هم متصل نمود.

پشته پروتکل ZigBee شامل چهار لایه است: لایه فیزیکی (PHY) ، لایه کنترل دسترسی رسانه ، لایه شبکه و لایه کاربرد .

از نقطه نظر عملکرد، لایه فیزیکی فراهم کننده ارتباطات رادیویی و لایه کنترل دسترسی میانی، فراهم آورنده انتقال تک گام مطمئن می باشد. لایه شبکه توپولوژي هاي پیچیده تر و مسیریابی را معین می کند و لایه کاربرد مشخص کننده توابع مدیریتی شبکه ودستگاه ها و همچنین قالب پیام را مشخص میکند.



شکل 2-2 پشته پروتکلی zigbee

بسیاري از دستگاههایی که تحت فناوري zigbee عمل می نمایند، نیازمند نرخ داده ارتباطی پایینی می باشند. نمونه بارز این موضوع، بحث روشنایی می باشد که با در نظر گرفتن یک بیت صفر یا یک براي روشن یا خاموش نمودن آن بکار می رود. در نتیجه با توجه به کم مصرف بودن این فناوري باتري میتواند بالغ بر 10 سال کار کند. کاربردهاي زیر از مواردي است که zigbee براي آن توسعه داده شده است:

 هزینه پایین

 توان کم

 نرخ انتقال پایین

 امنیت

 انعطاف پذیري

 قابلیت توسعه آسان و ارزان

 قابلیت اطمینان

اجزاي اصلی که یک شبکه zigbee را در یک محدوده خصوصی تشکیل می دهند شامل:

الف. هماهنگ کننده : این نود نقش اصلی را در شبکه zigbee داشته و مسئولیت هاي مهم از قبیل آغاز کار شبکه واختصاص آدرس

به دستگاه ها بر عهده آن است. در هر شبکه تنها یک هماهنگ کننده موجود است، که تمامی دانش مربوط به شبکه را نگهداري می

کند و بیشترین قدرت محاسباتی و حافظه را نیاز دارد.

ب. مسیریاب : مسیریاب علاوه بر مسیریابی می تواند به عنوان مسیر واسطی جهت انتقال اطلاعات بین وسایل استفاده شود.

ج. دستگاه انتهایی : این نوع نود به عنوان گره برگ در شبکه در نظر گرفته می شود و می تواند تا زمان زیادي غیر فعال بماند و در

نتیجه توان کمی مصرف کند

.

شکل 2-3 مدل شبکه zigbee

**2-4-2 برچسب هوشمند**

فناوري برچسب هوشمند یا RFID بیانگر سیستم هایی است که از امواج رادیویی براي انتقال اطلاعات مربوط به هویت یک شیء استفاده می کنند. این تگها نوع پیشرفته تري از بارکدها هستند چراکه هم قابلیت خواندن و هم قابلیت نوشتن دارند، دادههایی که روي تگهاي RFID ذخیره میشوند را میتوان تغییر داد، به روز رسانی کرد و یا حتی قفل کرد . این فناوري موفق شده است تا قابلیت و کارایی خود را به عنوان یک ابزار مقرون به صرفه در بهبود عملکرد و کاهش زمان و هزینه هاي نیروي انسانی و منابع در بسیاري از موارد ثابت نماید.

افراد با قرار دادن تگ هاي RFID مرتبط در محیط هاي هوشمند ، به اتوماتیکی کردن آن محیط کمک می کنند. در یک سناریوي کلی

وقتی که قسمت هاي تولیدي به پردازش میرسند، به وسیله دستگاه برچسب خوان یک رویداد مانند خواندن شماره RFID و ذخیره آن رخ می دهد، که اطلاعات مهمی را در اختیار ما قرار می دهد. ماشین/ ربات به وسیله این رویداد مطلع می شود و قسمت تولیدي را

برمیدارد.

فناوري هاي استفاده شده در RFID عبارتند از:

 برچسب

 برچسب خوان

 آنتن

 نرم افزار مدیریت اطلاعات

اگر بخواهیم برچسب ها را بر اساس منبع انرژي که استفاده می کنند تقسیم بندي کنیم سه نوع اصلی از آنها را خواهیم داشت. برچسب هاي فعال، غیرفعال و نیمه غیر فعال. برچسب هاي فعال انرژي مورد نیاز خود را از باتري همراهشان دریافت می کنند درحالیکه برچسب هاي غیر فعال به خودي خود داراي منبع انرژي نبوده و براي به کار افتادن باید از انرژي امواج الکترومغناطیسی منتشر شده از برچسب خوان استفاده نمایند و البته محدوده و دامنه خواندن کمتري نسبت به برچسب هاي فعال دارند. نوع دیگري از برچسب نیز برچسب نیمه غیرفعال می باشدکه علاوه بر استفاده از باتري داخلی اش، می تواند از انرژي امواج منتشر شده از برچسب خوان نیز استفاده نماید.

**2-4-3 ارتباطات میدان نزدیک**

ارتباطات میدان نزدیک عبارتست از قابلیت ارتباطی جدید که میتوان براي اتصال امن بین دو دستگاهی که در فاصلهي کمی از یکدیگر قرار دارند استفاده کرد. علاوه بر مجاورت دو گجت لازم است تا هر دوي آنها از سخت افزار مخصوصی بهره ببرند . در حقیقت NFC نسخه جدیدتري از RFID است که برد ارتباطی آن به 4 اینچ محدود شده است. این موضوع NFC را براي کاربردهاي حساس مانند موارد استفاده از کارت اعتباري)مثل پرداختهاي الکترونیک با استفاده از گوگل والت( و یا ورود به محل هاي امنیتی بسیار کارامد می کند. دستگاههایی که از فناوري NFC پشتیبانی می کنند به آسانی این امکان را به کاربر می دهند که اطلاعات مورد نظر را با یک لمس یا نزدیک کردن دستگاه خود به دستگاه دیگر ارسال یا مبادله کنند.



شکل 2-4 NFC

**2-4- 4 شبکه های موبایلی**

توسعه ي 5G ، نسل پنجم شبکههاي مخابراتی موبایل با شتاب بالایی در حال انجام است. علیرغم اینکه هنوز برخی از کشورها شبکهي

ارتباطی خود را به 4G ارتقا ندادهاند، اما نسل پنجم در حال توسعه است و دانشمندان با هیجان بالایی در مورد آن صحبت میکنند. استفاده از پهناي باند بالا، نرخ انتقال دادهي زیاد و تسهیل در ارتباطات مبتنی بر اینترنت همچون مکالمات ویدئویی، تنها گوشهاي از قابلیتهایی است که با پیاده سازي شبکه هاي 5G در اختیار کاربران قرار خواهد گرفت . یکی از مورادي که نیاز به پهناي باند بالا را افزایش میدهد، مفهوم اینترنت اشیا است .

براي مقابله با حجم رو به افزایش دستگاههاي متصل به شبکه که بخشی از اینترنت اشیا محسوب میشود، به سطح جدیدي از اتصالات بیسیم به اینترنت نیاز داریم. نگاهی به سال 2020 ، ما را امیدوار میکند که اجراي پروژههایی نظیر شهرهوشمند، خانه هوشمند، حمل ونقل هوشمند و نظیر آنها تنها با استفاده از شبکههاي 5G میسر خواهد شد .

یکی دیگر از قابلیتهاي کلیدي شبکهي 5G ، پایداري این شبکه است . محققان پایداري شبکه هاي 5G را به اندازهاي بالا عنوان می کنند که میتوان حتی این شبکه ها را از نظر پایداري بهتراز شبکه ي اینترنت فیبرنوري دانست. براساس اطلاعات ارائه شده توسط اریکسون، تاخیر در شبکه ي 5G یک میلی ثانیه است . این قابلیت یکی از ارکان اصلی بکارگیري این فناوري در زمینه هایی است که پایداري اهمیت فوقالعاده اي دارد.

**2-4-5 بلوتوث**

بلوتوث یک فناوري بی سیم براي ارتباط کوتاه برد است که مبتنی بر استاندارد IEEE 802.15.1 می باشد. بلوتوث کم انرژي (BLE)

تبدیل به یک بلوک ساختمانی کلیدي براي اینترنت اشیاء شده است. سازندگان تراشه در تلاشند تا با استفاده از فن آوري، منجر به

کاهش مصرف برق دستگاه شوند و به توسعه دهندگان براي اجراسازي آن کمک کنند . نسخه 4.2 این فناوري در سال 2014 معرفی شد و درآن برخی ویژگیهاي اساسی براي اینترنت اشیاء اضافه شده است

سرعت و امنیت بلوتوث 4.2 نسبت به نسخه هاي قبلی بهینه شده و در عین حال توان مصرفی کمتر است. این ویژگی ها بلوتوث کم انرژي را به رقیبی جدي در برابر فناوري zigbee تبدیل کرده است. یکی از ویژگی هاي اساسی استاندارد بلوتوث این است که نسخه جدید، با نسخه هاي قبلی سازگاري دارند . بلوتوث بر خلاف فرستنده مادون قرمز و گیرنده آن که میبایست در مقابل هم قرار بگیرند تا ارسال اطلاعات صورت گیرد، میتواند در صورت وجود داشتن مانعی در بین راه، انتقال اطلاعات را به درستی انجام دهد .

**2-4-6 Z-Wave**

Z-Wave یک پروتکل ارتباطی بی سیم است که توسط زنسیس طراحی شده است و توسط ائتلاف Z-Wave براي اتوماسیون در محیط

هاي مسکونی و تجاري کم تراکم ترویج شده است.هدف اصلی Z-Wave ارایه یک انتقال مطمئن از پیام هاي کوتاه از یک واحد کنترل به یک یا چند گره دیگر در شبکه است. Z-Wave داراي معماري پنج لایه اي است که عبارتند از: لایه فیزیکی، لایه مک ، لایه انتقال، لایه مسیریابی و لایه کاربرد. لایه مک مربوط به این فناوري، مکانیسمی را تعریف می کند که امکان ارسال فریم را در زمان در دسترس بودن کانال فراهم می کند. در صورتی که کانال در دسترس نباشد، انتقال به زمانی دیگر موکول می شود و این زمان به صورت تصادفی است. لایه انتقال ارتباط بین دو گره متوالی را مدیریت می کند و این لایه یک مکانیسم انتخابی براي انتقال مجدد را براساس تصدیق فراهم می کند Z-Wave . دو نوع از تجهیزات را تعریف می کند: کنترل کننده ها و پیروها. کنترل کننده ها دستورات را صادر و به پیروها ارسال می کنند و تجهیزات پیرو دستورات را اجرا می کنند . لایه مسیریابی Z-Wave عمل مسیریابی را براساس رویکرد مسیریابی از منبع انجام می دهد. وقتی یک کنترل کننده بسته اي را ارسال می

کند، در برگیرنده مسیري که باید طی کند نیز هست. هر بسته می تواند تا چهار hop ارسال شود که براي حالت مسکونی کافی است و سربار ناشی از بسته مسیریابی از منبع را بسیار محدود می کند. هر کنترل کننده داراي جدولی است که توپولوژي کل شبکه را در بر دارد . به کمک Z-Wave میتوان بیش از 232 دستگاه را به صورت بیسیم به هم متصل کرد و در صورت نیاز از پل براي اتصال دستگاه هاي بیشتر استفاده نمود

.

شکل 2-5 پشته پروتکلی Z-Wave

2-5 راهکار ها

در خانه های هوشمند دو راه حل عمده برای تامین امنیت به کار می رود که در ادامه به بررسی این دو مورد خواهیم پرداخت **:**

# **2-5-1 احراز هویت**

# دستگاه ها باید در برابر سیستم های دیگر تصدیق شوند و برای این منظور به یک شناسه منحصر بفرد و کلمه عبور نیاز دارند . هم چنین برای پیاده سازی رمز نگاری (SSH) به کلیدهای احراز هویت برای تایید هویت دستگاه های متصل را دارد . دستگاه های هم چون تلویزیون مدار بسته (CCCTV) و یا دستگاه های DVR ویدئویی و تجهیزات آنتن ماهواره می توانند در این زمینه مورد استفاده قرار گیرند . در هنگام به روز رسانی یک دستگاه باید حتما احراز هویت صورت پذیرد و سرورهای داخلی و دستگاه های مجاز بازیابی شوند .

# **2-5-2 حریم خصوصی**

# دستگاه اینترنت اشیا مجریان اعتماد مبتی بر سخت افزار (Hardware-based) می باشند ولی همزمان از اعتماد بوسیله فرآیندهای خاصی استفاده می کنند تا بدین شکل بتوانند مطالب خود را به صورت خصوصی نگهدارند و در برابر حملات نرم افزارهای غیرقابل اطمینان از آنان محافظت نمایند .

# اطلاعات موجود بر روی تراشه های داده های متصل به اینترنت اشیا می تواند مورد سرقت قرار گیرد برای همین با استفاده از رمز گذاری و رمز گشایی از اطلاعات محافظت می شود . دسستگاه های اینترنت اشیا بوسیله رمزگذاری و استفاده از پروتکل های مانند TSL به انجام تراکنش های حساس مانند تراکنش های مالی می پردازند . TLS می تواند مانع حمله مرد میانی شود و برای موارد محرمانه بسیار پرکاربرد خواهد بود . استفاده از Firewall برای کنترل دسترسی نیز ایده مناسبی می باشد .

2-6 جمع بندی

**فصل سوم**

**نتیجه گیری و پیشنهادات**

3-1 نتیجه گیری

3-2 **طرح پیشنهادی**

سیستم خانه هوشمند مطابق شکل ١ می تواند پیکربندی شود، سیستم خانه هوشمند شامل سه مؤلفه اصلی سرور خانه، دروازه

خانه و دستگاه های خانه هوشمند است. ابتدا سرو رخانه فرآیندهای ذخیره سازی، تجمیع و توزیع اطلاعات گردآوری شده از

رسانه های مختلف موجود در خانه را انجام می دهد، سپس دروازه خانه، صاحب شبکه دسترسی را به شبکه خانگی متصل

می کند؛ در نهایت دستگاه های خانه هوشمند قادر خواهند بود اطلاعات را میان دستگاه ها مبادله کرده و به اینترنت خارجی نیز

دسترسی پیدا کند. مؤلفه های تشکیل دهنده سیستم خانه هوشمند در مواجهه با تهدیدات داخلی یا خارجی قرار دارند زیرا اغلب

این مؤلفه ها به اینترنت متصل هستند؛ برای غلبه بر چنین تهدیدات امنیتی، مانند تزریقات بدافزاری، دسترسی احراز هویت

شده کاربر، افشای اطلاعات اساسی، لازم است تمهیدات امنیتی مطابق بر مشخصه های مؤلفه ای سیستم خانه هوشمند به کار

گرفته شود. استفاده از مکانیزمهای امنیتی اختصاصی بسته به راه حل استفاده شده تغییر می یابد؛ چندین روش از لایه انتقال

به لایه کاربرد به کار گرفته می شوند.

منابع

* ***I****oT Security: Ongoing Challenges* ***and*** *Research Opportunities.* Zhang, Zhi Kai and Yi Cho, Michael Cheng. s.l. : IEEE, 2014.
* *Internet of Things (IoT): A vision, architectural elements, and future directions.* Gubbi, Jayavardhana, et al., et al. s.l. : elsevier, 2013, Future Generation Computer Systems.
* *Survey on secure communication protocols for the Internet of Things.* K.-T. Nguyen, M. Laurent, N. Oualha,. s.l. : Ad-hoc Networks, 2015, pp. 1-15.
* Song, Yuanjun. Security in Internet of Things. Stockholm, Sweden : KTH Information and Communication Technology, 2013.