به نام خدا

گزارش پروژه درس سیستم های هوشمند دیجیتال
Zigbee

دکتر سید احمد معتمدی

حسین غلامی

مقدمه

ZigBeeیک تکنولوژی بر مبنای استاندارد IEEE 802.15.4 است که برای دسته ای از پروتکل های ارتباطی سطح بالا طراحی شده و به کمک رادیو های دیجیتال کوچک و کم مصرف از آن برای ساخت شبکه های شخصی بی سیم برای مصارفی چون اتوماسیون خانگی، جمع آوری داده های دستگاه های پزشکی و سایر نیاز های با پهنای باند کم برای پروژه های کوچک مقیاس که به ارتباط بی سیم نیاز دارند استفاده می شود.

هدف تکنولوژیکی که توسط ZigBee تعریف شده، ساده تر و ارزان تر بودن نسبت به سایر شبکه های شخصی بی سیم (WPAN) مانند بلوتوث یا وای فای است. کاربرد های این تکنولوژی شامل چراغ های برق بی سیم، کنترل کننده های مصرف برق به همراه نمایشگر های داخل خانه، سیستم های مدیریت ترافیک و سایر تجهیزات مصرفی و صنعتی که به انتقال داده بی سیم، کوتاه برد و با نرخ انتقال پایین نیاز دارند می باشد.

مصرف توان کم این سیستم فاصله انتقال را به 10 تا 100 متر شعاع دید محدود می کند که میزان دقیق آن به توان خروجی خصوصیات محیطی بستگی دارد. دستگاه های ZigBee می توانند با گذراندن داده ها از یک شبکه توری از دستگاه های واسطه آن ها را در فواصل طولانی نیز منتقل کنند ZigBee .معمولا در کاربرد های با نرخ انتقال داده کم که به عمر باتری طولانی و شبکه های ایمن نیاز دارند استفاده می شود)شبکه های ZigBee با کلید های رمزنگاری متقارن 128 بیتی ایمن شده اند ZigBee.(نرخ انتقال داده تعریف شده ای برابر 250 کیلوبیت در ثانیه دارد که برای انتقال داده ها به صورت متناوب از یک سنسور یا دستگاه ورودی بسیار مناسب است.

ایده ZigBee در سال 1998 ایجاد شد این سیستم در سال 2003 استانداردسازی شد و در سال 2006 مجددا مورد بازبینی قرار گرفت. نام این سیستم به نوعی رقص در میان زنبور های عسل اشاره دارد که وقتی به کندو بر می گردند آن را انجام می دهند.

بررسی اجمالی

ZigBeeیک استاندارد شبکه توری بی سیم کم هزینه و کم مصرف است که هدف آن توسعه استفاده از دستگاه های با طول عمر باتری طولانی در کاربردهای مختلف کنترل و نظارت بی سیم می باشد. دستگاه های ZigBee زمان تاخیر کمی دارند که باعث کمتر شدن جریان متوسط مصرفی می شود. چیپ های ZigBee عمدتا با به همراه رادیو ها و میکروکنترلر هایی که حافظه فلش بین 60-256 کیلوبایت دارند به کار می رود ZigBee.در باند های رادیویی صنعتی، علمی و پزشکی به کار می رود. فرکانس 2.4 گیگاهرتز متداول ترین فرکانس در استاندارد های جهانی می باشد. این فرکانس در چین برابر 784 مگاهرتز، در اروپا برابر 858 مگاهرتز و در آمریکا و استرالیا برابر 915 مگاهرتز می باشد. نرخ انتقال داده ها از 20 کیلوبیت بر ثانیه(باند 868 مگاهرتز) تا 250 کیلوبیت بر ثانیه(باند 2.4 گیگاهرتز) متغیر است. لایه شبکه ZigBee به طور بالقوه از شبکه های ستاره ای و درختی و شبکه های توری عمومی پشتیبانی می کند. هر شبکه باید یک دستگاه هماهنگ کننده داشته باشد که هدف از ساخت آن کنترل پارامتر های شبکه و تعمیر و نگهداری عمومی از آن است. در شبکه های ستاره

ای، هماهنگ کننده باید به عنوان گره مرکزی مورد استفاده قرار گیرد. هر دو نوع شبکه ی درختی و توری امکان استفاده از روتر های ZigBee را برای افزایش ارتباطات در سطح شبکه فراهم کرده اند.

ZigBeeبر پایه لایه فیزیکی و لایه نظارت بر دسترسی به رسانه انتقال که در استاندارد IEEE 802.15.4 برای شبکه های شخصی بی سیم با انرخ انتقال پایین تعریف شده، ساخته شده است. این طراحی شامل 4 جز کلیدی اضافی نیز می شود: لایه شبکه – لایه کاربرد- اشیا دستگاه -ZigBee (ZDO) و اشیا کاربردی تعریف شده توسط تولید کننده که اجازه شخصی سازی را به استفاده کنندگان می دهند و از یکپارچه سازی سیستم حمایت می کنند . ZDOها مسئولیت برخی از وظایف مانند ثبت و نگهداری نقش های دستگاه، مدیریت درخواست برای اتصال به شبکه و همچنین پیدا کردن دستگاه و امنیت آن را به عهده می گیرند.

ZigBeeیکی از استاندارد های جهانی پروتکل ارتباطات است که توسط کارگروهی ویژه تحت IEEE 802.15 تعریف شده است. این استاندارد چهارمین استاندارد موجود در این شاخه است و همچنین جدیدترین استاندارد در این زمینه به شمار می رود و در دستگاه هایی نرخ انتقال داده و مصرف توان بسیار پایین دارند و در واقع ویژگی اصلی آن ها طول عمر دراز مدت باتری آن ها است، به کار می رود. استاندارد های دیگر مانند Bluetoothیا IrDA برای کاربرد های با نرخ انتقال داده بالا مانند صدا، تصویر و یا ارتباطات LAN طراحی شده اند.

تاریخچه

شبکه های دیجیتال رادیویی خود سازمان دهنده و تک کاره مشابه ZigBee در دهه 1990 به وجود آمدند. ZigBee تحت استاندارد IEEE 802.15.4-2003 در 14 دسامبر 2004 به تصویب رسید. ZigBee Alliance در دسترس بودن نسخه اول این تکنولوژی را در 13 ژوئن 2005 اعلام کرد که از آن به عنوان ZigBee 2004 یاد می شود.

ZCL

در سپتامبر 2006، ساختار ZigBee 2006 به صورت رسمی اعلام شد و نسخه سال 2004 را از رده خارج کرد (نسخه سال 2006 ساختار پیام/اشتراک مقدار کلیدی موجود در نسخه سال 2004 را با یک "کتابخانه خوشه" جایگزین کرد). این کتابخانه مجموعه ای از دستورات استانداردسازی شده است که تحت گروه هایی به نام خوشه ها سازمان دهی شده اند. این خوشه ها نام هایی چون انرژی هوشمند، اتوماسیون خانگی و ZigBee Light Linkدارند.

در ژانویه سال 2017 این نام به Dotdot تغییر پیدا کرد و به عنوان پروتکل جدیدی معرفی شد که با علامت |::نمایش داده می شود. آن ها همچنین اعلام کردند این پروتکل بر روی انواع دیگر شبکه ها و با استفاده از پروتکل اینترنت اجرا خواهد شد و با استاندارد های دیگر نظیر Thread ارتباط برقرار خواهد کرد.

ZigBee PRO

ZigBee PROکه با نام ZigBee 2007 نیز شناخته می شود در 31 اکتبر 2007 ارائه شد و در همان سال به تایید نهایی رسید ZigBee PRO .به طور کامل قابلیت سازگاری با دستگاه های ZigBee 2006 را دارا می‌باشد. یک دستگاه ZigBee 2007 می تواند به عضویت یک شبکه ZigBee 2006 در بیاید و به راحتی در آن کار کند و بر عکس. به دلیل اختلافات موجود در زمینه گزینه های مسیریابی، دستگاه های ZigBee PRO باید در یک شبکه ZigBee 2006 به دستگاه انتهایی غیر مسیریاب (ZigBee(ZED تبدیل شوند و همین طور دستگاه های ZigBee 2006باید در شبکه های ZigBee PRO به ZED تبدیل شوند. برنامه های در حال اجرا بر روی این دستگاه ها بدون توجه به stack profile زیر آن ها به طور مشابه اجرا می شوند. اولین پروفایل کاربردی ZigBee(اتوماسیون خانگی) در 2 نوامبر 2007 معرفی شد.

موارد استفاده

پروتکل های ZigBee برای کاربرد های با مصرف توان کم و با نرخ انتقال پایین طراحی شده اند. شبکه ای که از طریق این پروتکل اجرا می شود تنها از نقادیر بسیار کمی انرژی/ توان استفاده خواهد کرد- دستگاه هایی که از این پروتکل استفاده می کنند باید طول عمر باتری حداقل 2 ساله داشته باشند تا بتوانند گواهی نامه مخصوص ZigBeeرا دریافت کنند.

کاربرد های متداول شامل موارد زیر می شوند:

سرگرمی های خانگی و کنترل: اتوماسیون خانگی مانندQIVICON ، روشنایی هوشمند، کنترل دمای پیشرفته، کاربرد های ایمنی و امنیتی- فیلم و موسیقی

حسگر شبکه بی سیم: که با سنسور های تکی مانند Telosb یا Tmote یا Memsic آغاز شد

کنترل صنعتی

تشخیص جاسازی شده

جمع آوری داده های پزشکی

هشدار دود و ورود فرد غریبه

اتوماسیون ساختمان

استاندارد ها و پروتکل‌ها

ZigBee Allianceمجموعه از شرکت ها است استاندارد ZigBee را نگهداری کرده و منتشر می کنند. عبارت ZigBeeعلامت تجاری ثبت شده این گروه به شمار می رود و یک استاندارد فنی تنها به شمار نمی رود. این مجموعه، پروفایل های کاربردی را منتشر می کند که به فروشندگان تجهیزات اصلی (OEM)اجازه می دهد تا محصولات سازگاری را ایجاد کنند. ارتباط بین ZigBee و IEEE 802.15.4 شبیه ارتباط بین IEEE 802.11 و Wi-Fi Allianceمی باشد.

پروتکل ها

لیست کاربرد هایی که تا به حال منتشر شده یا در حال توسعه یافتن می باشند به شرح زیر است:

نسخه های عرضه شدهZigBee :

- اتوماسیون خانگی 1.2
- انرژی هوشمند b1.1
- خدمات مخابراتی 1
- مراقبت های پزشکی 1.0
- RF4CE-کنترل از راه دور 1.0
- RF4CE-دستگاه ورودی 1.0
- کنترل از راه دور 2.0
- Light Link 1.0
- IP 1.0
- اتوماسیون ساختمان های تجاری 1.0
- Gateway 1.0

نسخه های در حال توسعهZigBee

- انرژی هوشمند2.0 ZigBee
- انرژی هوشمند 1.3/1.2
- Light Link 1.1
- اتوماسیون خانگی 1.3

نسخه 2 انرژی هوشمند ZigBee پروتکل اینترنتی را برای زیرنظر گرفتن، کنترل کردن، اطلاع رسانی و اتوماتیک کردن استفاده از آب و انرژی تعریف می کند. این نسخه یک بروزرسانی نسبت به نسخه شماره 1 محسوب می شود. این پروتکل همچنین خدماتی چون شارژ وسایل نقلیه الکتریکی با اتصال به پریز برق، نصب تنظیم و دانلود نرم افزار سیستم، خدمات پیش پرداخت، اطلاعات کاربری و پیام رسانی، کنترل بار، پیک سایی و سایر اطلاعات عمومی و رابط های مختلف برای شبکه های بی سیم و سیمی ارائه می کند. این پروتکل توسط شرکای زیر در حال توسعه و طراحی می باشد:

- انجمن HomeGrid که مسئولیت بازاریابی و به دست آوردن گواهی تکنولوژی و محصولات ITU-T G.hnرا بر عهده دارد.
- HomePlug Powerline Alliance
- انجمن بین المللی مهندسین خودروSAE International
- SunSpec Alliance
- Wi-Fi Alliance

انرژی هوشمند ZigBee بر ZigBee IP تکیه کرده که یک لایه شبکه می باشد که ترافیک استاندارد IPv6 را به IEEE 802.15.4تغییر مسیر می دهد. این کار از طریق فشرده سازی هدر IP انجام می گیرد.

در سال 2009، کنسرسیوم RF4CE و ZigBee Alliance توافق کردند تا به طور مشترک استانداردی را برای کنترل از راه دور های با فرکانس رادیویی تدوین کنند ZigBee RF4CE .نیز در همین راستا و برای طیف گسترده ای از محصولات الکترونیکی مصرفی مانند تلویزیون ها و گیرنده های دیجیتال طراحی شد و قول مزایای بسیار بیشتر نسبت به کنترل های موجود در بازار را به مشترکین داد. این مزایا شامل ارتباط قوی تر، افزایش قابلیت اطمینان پذیری، انعطاف پذیری و ویژگی های بهبود یافته، چندمنظوره بودن و قابلیت کار کردن از پشت موانع می باشند ZigBee RF4CE .مقداری از بار شبکه را تحمل می کند و از همه ویژگی های شبکه های توری پشتیبانی نمی کند. اغلب از این ویژگی ها برای تنظیمات با حافظه کمتر در دستگاه های با هزینه کم مانند کنترل ها، صرف نظر می شود.

با معرفی دومین پروفایل کاربردی ZigBee RF4CE در سال 2012 و به دست گرفتن بخشی از بازار، تیم ZigBee RF4CEبررسی کلی استاندارد فعلی موجود، کاربرد ها و آینده این تکنولوژی را بر عهده دارد.

تجهیزات رادیویی

طراحی رادیویی استفاده شده در ZigBee به دقت بهینه سازی شده تا در تولید در مقیاس بزرگ کمترین هزینه را داشته باشد. این بخش تنها چند مرحله انالوگ به کار برده و هرجا ممکن بوده از مدار های دیجیتال استفاده کرده است.

اگرچه خود رادیو ها گران نیستند اما فرآیند انتخاب شدن آن ها توسط ZigBee شامل بررسی کامل مشخصات موردنیاز لایه فیزیکی می باشد. همه ی رادیو هایی از یک فتوماسک نیمه رسانای تایید شده تولید شده اند از مشخصات RF یکسانی بهره می برند. لایه فیزیکی که تایید نشده باشد و ناگهان دیگر به خوبی عمل نکند می تواند عمر باتری سایر دستگاه های موجود در شبکه ZigBee را نیز کاهش دهد. رادیو های ZigBee محدودیت های سنگینی در زمینه توان و پهنای باند مصرفی دارند. در نتیجه این رادیو ها اغلب با راهنمایی های ذکر شده در بند 6 استاندارد 802.15.4-2006 تست می شوند. بسیاری از تولید کنندگان قصد دارند رادیو و میکروکنترلر را بر روی یک چیپ ادغام کنند که منجر به تولید دستگاه های کوچکتر خواهد شد.

این استاندارد عملیات در باند های رادیویی صنعتی،علمی و پزشکی در فرکانس های 2.4 گیگاهرتز(جهانی)، 915 مگاهرتز(امریکا و استرالیا) و 868 مگاهرتز(اروپا) را مشخص می کند. در باند 2.4 گیگاهرتزی 16 کانال تقسیم بندی شده اند و هر کانال با سایر کانال ها 5 مگاهرتز فاصله دارد که البته هر کانال تنها از 2 مگاهرتز استفاده می کند. رادیو ها از روش- DSSS که توسط جریان دیجیتالی که وارد مدولاتور می شود کنترل می شود – استفاده می کنند. کلیدگذاری تغییر فازی دو زوجی (BPSK) در باند های 868 و 915 مگاهرتزی مورد استفاده قرار می گیرد و کلید گذاری تغییر فازی افست (OQPSK) که به ازای هر نشانه دو بیت را انتقال می دهد در باند 2.4 گیگاهرتزی مورد استفاده قرار می گیرد.

نرخ انتقال داده خام داده ها به صورت بی سیم برابر 250 کیلوبیت بر ثانیه به ازای هر کانال در باند 2.4 گیگاهرتزی، 40 کیلوبیت بر ثانیه به ازای هر کانال در باند 915 مگاهرتز و 20 کیلوبیت بر ثانیه در باند 868 مگاهرتز می باشد. مقدار نرخ انتقال واقعی کمتر از مقدار بیشینه مشخص شده می باشد که علت آن تاخیر های پردازشی و سربار شدن بسته ها می باشد. برای کاربرد های داخلی با فرکانس 2.4 گیگاهرتز، فاصله انتقال می تواند بین 10 متر تا 20 متر باشد که مقدار دقیق آن به مواد مورد استفاده در ساختمان، تعداد دیوار هایی که باید از آن عبور کرد و توان خروجی برقی که در آن ناحیه جغرافیایی مجاز است بستگی دارد. در موارد خارجی با زاویه دید، فاصله می تواند بسته به توان خروجی و خصوصیات محیط تا 1500 متر هم برسد. توان خروجی رادیو ها معمولا بین 0 تا 20 دسی بل(1-100 میلی وات) می باشد.

نوع دستگاه های ZigBee و حالت عملکرد آن ها

دستگاه های ZigBee به سه نوع تقسیم می شوند:

هماهنگ کننده(ZC) ZigBee

توانمند ترین قطعه در بین انواع قطعه ها، هماهنگ کننده ریشه شبکه درختی را تشکیل می دهد که ممکن است به شبکه های دیگر پل شود. در هر شبکه دقیقا یک هماهنگ کننده ZigBee وجود دارد زیرا این قطعه است که در ابتدا شبکه را به راه انداخته است)مشخصات ZigBee LightLink می تواند بدون هماهنگ کننده نیز کار کند که آن را برای محصولات خانگی قابل استفاده تر می کند .(این قطعه اطلاعات شبکه را در خود ذخیره می کند و به عنوان Trust Center و محل ذخیره ای برای کلید های امنیتی به کار می رود.

مسیریاب (روتر)(ZR) ZigBee

علاوه بر اجرای یک تابع کاربردی، یک ZR می تواند به عنوان یک مسیریاب واسطه نیز عمل کند و داده ها را از دستگاه های دیگر گرفته و عبور دهد.

پایانه های(ZED) ZigBee

تنها این قابلیت را دارد تا با گره مادر(هماهنگ کننده یا مسیریاب) مذاکره کند ولی نمی تواند داده های دستگاه های دیگر را از خود عبور دهد. این ارتباط به گره اجازه می دهد تا عمده زمان مصرف را در حالت خواب باشد و در نتیجه باعث افزایش طول عمر باتری شود. یک ZED به حداقل میزان حافظه نیاز دارد و در نتیجه تولید آن از ZR یا ZC ارزان تر است.

پروتکل های فعلی ZigBee از شبکه های Beacon دار و یا فاقد Beacon پشتیبانی می کنند. در شبکه های فاقدBeacon ، از یک مکانیزم دسترسی کانالی CSMA/CA استفاده می شود. در چنین شبکه ای، دریافت کننده ی روتر تقریبا همیشه فعال است و به منبع تغذیه قوی تری نیاز دارد. در عین حال این حالت امکان استفاده از شبکه های غیرهمگن را می دهد که در آن برخی از دستگاه ها به طور دائم در حال دریافت اطلاعات هستند در حالی که برخی دستگاه های دیگر تنها زمانی داده ها را منتقل می کنند که یک عامل محرک خارجی وجود داشته باشد. مثال متداول یک شبکه غیر همگن، یک کلید برق بی سیم است. گره ZigBee در لامپ ممکن است به طور دائم دریافت اطلاعات داشته باشد زیرا به منبع اصلی متصل است در حالی که یک کلید برق که با باتری کار می کند تا زمانی که وضعیت کلید تغییر نکند غیرفعال باقی می ماند. بعد از تغییر وضعیت، کلید فعال می شود و فرمانی را به لامپ می فرستد، و پیامی مبنی بر دریافت دستور دریافت می کند و بعد دوباره به حالت غیرفعال باز می گردد. در چنین شبکه ای گره لامپ اگر هماهنگ کننده Zigbee نباشد حداقل یک روتر ZigBee خواهد بود. گره کلید معمولا یک پایانه ZigBee خواهد بود.

در شبکه های Beacon دار، گره های خاص شبکه که به آن ها ZigBee Routers گفته می شود به طور تناوبی سیگنال هایی تولید می کنند تا حضور خود را به سایر گره های موجود در شبکه اعلام کنند. گره ها ممکن است بین این سیگنال ها به حالت غیرفعال درآیند. این کار باعث کم شدن سیکل کاری و افزایش عمر باتری خواهد شد. بازه زمانی بین سیگنال ها به نرخ انتقال داده ها بستگی دارد. این بازه می تواند بین 15.36

میلی ثانیه تا 251.6 ثانیه با نرخ انتقال 250 کیلوبیت بر ثانیه تغییر کند. در نرخ انتقال 40 کیلوبیت بر ثانیه این بازه بین 24 میلی ثانیه تا 393.21 ثانیه و در نرخ انتقال 20 کیلوبیت بر ثانیه بین 48 میلی ثانیه تا 786 ثانیه تغییر خواهد کرد. با این وجود عملیات با سیکل کاری و بازه های زمانی طولانی به زمان بندی دقیق نیاز دارد که با کم کردن هزینه های تولید در تضاد است.

به طور کلی، پروتکل های ZigBee زمانی که فرستنده رادیویی فعال است را به کمترین مقدار ممکن می رسانند و به این ترتیب مصرف انرژی سیستم کم می شود. در شبکه های Beacon دار، گره ها تنها باید در زمانی که سیگنالی در حال انتقال است فعال باشند. در شبکه های بدون Beacon مصرف توان نامتقارن است. برخی دستگاه ها همواره فعال هستند در حالی که برخی دیگر بیشتر اوقات غیرفعال هستند.

به جز برای پروفایل انرژی هوشمند 2، دستگاه های ZigBee باید از استاندارد IEEE 802.15.4-2003 برای شبکه های LR-WPAN تبعیت کنند. این استاندارد لایه های پایینی پروتکل را مشخص می کند. این لایه ها شامل لایه فیزیکی و بخش دسترسی کنترل رسانه از لایه پیوند داده ای (DLL)می باشند. حالت پایه دسترسی کانال CSMA/CAنمی باشد. این مطلب به این معناست که گره ها به گونه ای مشابه انسان ها با یکدیگر صحبت می کنند. ابتدا به طور مختصر بررسی می کنند که شخص دیگری در حال صحبت کردن نباشد و سپس شروع به صحبت می کند. البته 3 استثنای قابل ذکر وجود دارد. سیگنال ها بر طبق یک برنامه زمانی ثابت ارسال می شوند و از CSMA استفاده نمی کنند. پیام های تاییدی نیز از CSMA استفاده نمی کنند. در نهایت این که در شبکه های Beacon دار، دستگاه هایی که نیازی به زمان های تاخیر فوق العاده کم ندارند می توانند از Guaranteed Time Slotsاستفاده کنند که این مورد نیز طبق تعریف از CSMA استفاده نمی کنند.

نرم افزار تکنولوژیZigBee

نرم افزار این سیستم به گونه ای طراحی شده که توسعه آن بر روی ریزپردازنده های کوچک و نه چندان گران راحت باشد.

لایه شبکه درZigBee

وظایف اصلی لایه شبکه فراهم آوردن امکان استفاده صحیح از زیر لایه MAC و فراهم آوردن رابطی مناسب برای استفاده توسط لایه های بالایی- به خصوص لایه کاربرد- می باشد. توانایی ها و ساختار این لایه عمدتا همان هایی است که به این نوع از لایه های شبکه اختصاص داده می شود که به عنوان مثال می توان به تعیین مسیر (routing)اشاره کرد.

در یک طرف، موجودیت داده، واحد های داده لایه شبکه را ایجاد کرده و مدیریت می کند و همچنین با توجه به توپولوژی فعلی، عملیات تعیین مسیر را نیز انجام می دهد. در طرف دیگر، لایه ای به نام کنترل وجود دارد که تنظیم دستگاه های جدید و احداث شبکه های جدید را بر عهده می گیرد. این لایه می تواند تعیین کند ایا یک دستگاه همسایه به شبکه تعلق دارد یا خیر و همچنین می تواند دستگاه ها و روتر های جدید نزدیک به خود را نیز پیدا کند. همچنین لایه کنترل می تواند وجود یک گیرنده در شبکه را تشخیص دهد که این کار اجازه برقراری ارتباط مستقیم و همگام سازی MAC را نیز می دهد.

پروتکل تعیین مسیری که توسط لایه شبکه استفاده می شود AODV می باشد. برای پیدا کردن دستگاه مقصد، این پروتکل یک در خواست مسیر برای تمامی دستگاه های همسایه خود ارسال می کند. دستگاه های همسایه نیز این درخواست را به دستگاه های همسایه خود منتقل می کنند و به همین ترتیب این کار تا زمان رسیدن به مقصد نهایی تکرار می شود. وقتی این درخواست به مقصد نهایی رسید، پاسخ در خواست مسیر طی شده توسط یک انتقال تک پخشی و از مسیری که کمترین هزینه را در بر خواهد داشت به منبع باز می گردد. وقتی منبع این پاسخ را دریافت کرد، مقادیر گره های موجود در مسیر و هزینه مسیر را در جدول روتینگ خود را برای آدرس مقصد به روز خواهد کرد

لایه کاربرد درZigBee

لایه کاربرد سطح ، بالاترین لایه ای است که توسط این مشخصات تعریف می شود و رابطی موثر بین سیستم ZigBeeو کاربران این سیستم به شمار می رود. این لایه شامل اکثریت اجزایی است که توسط مشخصات ZigBeeاضافه شده اند. هر دوی ZDO و روش های مدیریت آن به همراه اشیا کاربرد که توسط تولید کننده تعریف شده اند به عنوان بخشی از این لایه در نظر گفته می شوند.

اجزا اصلیZigBee

ZDO (ZigBee Device Object)یک پروتکل در پروتکل پشته ای ZigBee به شمار می رود که مسئول مدیریت کلی دستگاه، کلید های امنیتی و دستورات می باشد. این پروتکل مسئولیت تعیین نقش یک دستگاه به عنوان هماهنگ کننده یا پایانه و همچنین پیدا کردن دستگاه های جدید در شبکه و شناسایی سرویس هایی که ارائه می دهند را نیز بر عهده دارد. در ادامه ممکن است این پروتکل لینک های امنی را با دستگاه های خارجی برقرار کرده و به درخواست های اتصال به طور مقتضی پاسخ دهد.

زیرلایه پشتیبانی کاربرد APS جز استاندارد دیگر این لایه به شمار می رود و به همین ترتیب، یک رابط به خوبی تعریف شده و خدمات کنترلی را ارائه می دهد. این زیرلایه به عنوان پلی بین لایه شبکه و اجزا دیگر لایه کاربرد عمل می کند. این زیرلایه جدول های اتصالات به روز شده را به شکل یک بانک اطلاعاتی نگهداری می کند که می توان از آن برای پیدا کردن دستگاه های مختلف بسته به خدماتی که مورد نیاز هستند و خدماتی که دستگاه های مختلف ارائه می دهند، استفاده کرد. همچنین به عنوان ارتباطی بین دو لایه ذکر شده، این زیرلایه پیام هایی را نیز بین لایه های مختلف پروتکل پشته ای منتقل می کند.

مدل های ارتباطیZigBee

یک کاربرد مشخص ممکن است از اشیایی تشکیل شده باشد که از طریق برقراری ارتباط با یکدیگر همکاری کرده و وظایف مورد نظر را انجام دهند. هدف ZigBee این است که کار را بین دستگاه های مختلف زیادی که در گره های- ZigBee که خودشان یک شبکه هستند- قرار گرفته اند توزیع کند(کار ذکر شده برای هر دستگاه عمدتا به صورت محلی خواهد بود. برای مثال می توان به کنترل هر کدام از وسایل خانه اشاره کرد).

مجموعه اشیایی که شبکه را تشکیل می دهند با استفاده از امکاناتی که توسط APS فراهم شده و تحت نظارت ZDOمی باشد با یکدیگر ارتباط برقرار می کنند. سرویس های داده لایه کاربرد به دنبال یک ساختار متداول درخواست-تایید یا نشانه-پاسخ فعال می شوند. تنها در داخل یک دستگاه، تا 240 اشیا کاربرد، می توانند وجود داشته باشند که در بازه 1 تا 240 شماره گذاری شده اند. عدد صفر برای رابط داده ZDO و 255 نیز برای پخش داده ها کنار گذاشته شده است. بازه 241 تا 254 در حال حاضر مورد استفاده قرار نمی گیرد اما در آینده ممکن است از این بازه نیز بهره برداری شود.

برای اشیا کاربرد، دو سرویسِ قابل استفاده وجود دارد) در:(ZigBee 1.0

- سرویس key-value pair(KVP) برای هدف تنظیم در نظر گرفته شده است. این سرویس امکان مشاهده شرح، ارسال درخواست و یا اصلاح ویژگی های شی را با استفاده از یک رابط ساده بر پایه دریافت و تعیین شکل های اولیه رویداد امکان پذیر می کند. برخی از انواع آن اجازه صدور یک درخواست برای پاسخ را نیز می دهند. تنظیمات از XML فشرده استفاده می کند) می توان از XML کامل نیز استفاده کرد (تا راه حلی سازگار با شرایط مختلف ارائه کند.
- سرویس پیام برای ارائه روند عمومی برخورد با اطلاعات طراحی شده و نیاز به سازگار کردن پروتکل های کاربرد و سربار احتمالی که توسط KVP ایجاد می شود را از بین می برد. این سرویس همچنین امکان انتقال بار کاری را از طریق فریم های APS فراهم می کند.

دادن آدرس نیز بخشی از لایه کاربرد به شمار می رود. یک گره شبکه از یک فرستنده-گیرنده رادیویی 802.15.4و یک یا چند شرح دستگاه (در واقع مجموعه ای از خصوصیات که می توان آن را تنظیم کرد یا می توان آن ها را در جریان رویداد های مختلف مورد نظارت قرار داد) تشکیل شده است. فرستنده-گیرنده مبنای آدرس دهی به شمار می رود و دستگاه های درون یک گره با یک شناساگر نقطه انتهایی در بازه 1- 240 مشخص می شوند.

ارتباط و پیدا کردن دستگاه ها

برای این که کاربرد ها بتوانند با یکدیگر ارتباط برقرار کنند دستگاه های تشکیل دهنده آن ها باید از یک پروتکل کاربرد مشترک (از نوع پیام ها، فرمت ها و...) استفاده کنند. این مجموعه از قرارداد ها در دسته پروفایل ها قرار می گیرند. همچنین برقراری اتصال توسط شناساگر های ورودی و خروجی مشابه تصمیم گیری می شود. این شناساگر ها برای هر پروفایل به طور منحصر به فرد تعریف می شوند و به جریان داده های ورودی و خروجی به یک دستگاه مرتبط می شوند. در جداول اتصال نیز زوج های منبع و مقصد موجود هستند.

بسته به اطلاعات موجود، پیدا کردن دستگاه ها ممکن است از روش های مختلفی انجام شود. زمانی که آدرس شبکه معلوم است می توان آدرس IEEE را با استفاده از ارتباط تک پشتی درخواست نمود. در صورتی که این گونه نباشد درخواست ها پخش می شوند)آدرس IEEE بخشی از بسته پاسخ به شمار می رود .(دستگاه های انتهایی شبکه به سادگی پاسخ درخواست دریافت شده را ارسال می کنند و همچنین هماهنگ کننده شبکه یا یک روتر آدرس تمامی دستگاه هایی که به آن مرتبط هستند را ارسال می کند. این پروتکل تمدید شده ی جستجو به دستگاه های خارجی اجازه می دهد تا اطلاعاتی را در مورد دستگاه های موجود در شبکه و سرویس هایی که ارائه می دهند به دست آورد. پایانه های این دستگاه ها وقتی توسط دستگاه جستجو کننده(که احتمالا آدرس آن ها را به دست آورده است) مورد پرسش قرار می گیرند می توانند این اتفاق را گزارش دهند. ممکن است از سرویس های مشابه نیز استفاده شود.

استفاده از شناساگر های خوشه ای اتصال اشیا مکمل با استفاده از جداول اتصال را به شبکه تحمیل می کند. این جدول ها توسط هماهنگ کننده ZigBee نگهداری می شوند. علت این امر آن است که جدول ها باید همواره در

داخل شبکه در دسترس باشند و هماهنگ کننده های شبکه بیشترین احتمال را برای داشتن منبع تغذیه دائمی دارند. نسخه های پشتیبان که توسط لایه های با سطوح بالاتر مدیریت می شوند ممکن است در برخی از کاربرد ها مورد نیاز باشند. اتصال به یک لینک که ارتباط آن برقرار شده است نیاز دارد. بعد از این که این ارتباط به وجود آمد، با توجه به کاربرد و سیاست های امنیتی در مورد این که آیا گره جدید به شبکه اضافه شود یا نه تصمیم گیری می شود.

ارتباط ممکن است بلافاصله بعد از اتصال برقرار شود. آدرس دهی مستقیم از هر دو گزینه آدرس های رادیویی و شناساگر های نقاط انتهایی استفاده می کند در حالی که آدرس دهی غیر مستقیم از هر نوع اطلاعات مرتبط(آدرس، پایانه، خوشه و خاصیت) استفاده می کند و لازم است تا اطلاعات به هماهنگ کننده شبکه فرستاده شوند. هماهنگ کننده از اتصالات فعلی نگهداری می کند و درخواست های برقراری ارتباط را منتقل می کند. آدرس دهی غیر مستقیم به خصوص برای ساده نگه داشتن برخی قطعات و کمینه کردن نیاز آن ها به فضای ذخیره سازی بسیار مفید است. در کنار این دو روش، پخش به تمامی نقاط انتهایی در یک دستگاه نیز امکان پذیر است و آدرس دهی گروهی نیز برای برقراری ارتباط با گروه هایی از نقاط انتهایی، متعلق به مجموعه ای از دستگاه ها نیز امکان پذیر است.

خدمات امنیتیZigBee

به عنوان یکی از ویژگی های اصلی، ZigBeeامکاناتی را فراهم می کند تا ارتباطات به صورت امن برقرار شوند ZigBee .از ایجاد و انتقال کلید های رمزنگاری، چارچوب های رمزنگاری و دستگاه های کنترل کننده آن محافظت می کند. این تکنولوژی از چارچوب تعریف شده در IEEE 802.15.4 استفاده می کند. این بخش از معماری شبکه، بر مدیریت صحیح کلید های متقارن و اجرای صحیح روش ها و قوانین امنیتی تکیه می کند.

مدل ارتباط سطح بالا

مدل امنیتی پایهZigBee

مکانیزم پایه برای اطمینان یافتن از محرمانه بودن اطلاعات، محافظت کافی از تمامی عوامل تولید کلید های امنیتی می باشد. در مرحله نصب اولیه کلید ها و همچنین پردازش اطلاعات امنیتی اعتماد به سیستم باید به عنوان فرض اولیه در نظر گرفته شود.برای این که یک عملیات اجرایی در سطح کلی عمل کند، انطباق عمومی آن به رفتار های مشخص نیز مفروض است.

کلید ها، اساس معماری امنیتی را تشکیل می دهند، در نتیجه محافظت از آن ها از بالاترین اهمیت برخوردار می باشد و این کلید ها هرگز نباید از طریق یک کانال غیرامن منتقل شوند. یک استثنا جزئی در مورد این قانون در فاز اولیه اضافه شدن یک دستگاه قبلا تنظیم نشده به شبکه رخ می دهد. مدل شبکه ZigBee باید به مسائل امنیتی اهمیت زیادی بدهد زیرا شبکه های ادهاک ممکن است به صورت فیزیکی در دسترس دستگاه های خارجی باشند. علاوه بر این، وضعیت محیط کار سیستم را نیز نمی توان پیش بینی کرد.

درون پروتکل پشته ای، لایه های مختلف شبکه از نظر رمزنگاری از یکدیگر جدا نشده اند در نتیجه به قوانین دسترسی نیاز است و فرض می شود که از طراحی متداول استفاده می شود. مدل اطمینانِ باز در یک دستگاه امکان به اشتراک گذاری کلید را فراهم می کند که باعث کاهش چشمگیر هزینه های احتمالی می شود. با این وجود، لایه ای که یک چارچوب می سازد مسئول ایمنی آن نیز به شمار می رود. اگر امکان وجود دستگاه های مخرب وجود داشته باشد هر بسته از لایه های شبکه باید رمزنگاری شود تا بتوان انتقال داده غیرمجاز را بلافاصله قطع کرد. در این مورد هم حالت استثنا، انتقال کلید شبکه می باشد که یک لایه امنیتی یکپارچه در گرید و دستگاه در حال اتصال جدید به وجود می آورد.

معماری امنیتیZigBee

ZigBeeاز کلید های 128 بیتی برای اجرای مکانیزم های امنیتی خود استفاده می کند. یک کلید ممکن است متعلق به یک شبکه باشد که در این صورت می تواند هم توسط لایه های ZigBee و هم توسط زیرلایه MAC مورد استفاده قرار گیرد و یا به یک لینک که از طریق مراحل پیش نصب،توافق و یا انتقال به دست آمده باشد مربوط باشد. ایجاد کلید های امنیتی برای لینک ها بر مبنای یک شاه کلید طراحی شده که تطابق کلید لینک ها را کنترل می کند. در بدترین حالت حداقل شاه کلید اولیه باید از طریق یک واسطه امن (انتقال یا پیش نصب) به دست بیاید زیرا امنیت کل شبکه به آن بستگی دارد. لینک و شاه کلید ها تنها برای لایه کاربرد قابل مشاهده هستند. سرویس های مختلف از تغییرات یک طرفه (با استفاده از یک تابع یک طرفه) کلید لینک استفاده می کنند تا از درز اطلاعات و خطرات امنیتی جلوگیری کنند.

توزیع کلید یکی از اقدامات امنیتی بسیار مهم شبکه است. یک شبکه امن، یک دستگاه مخصوص را که سایر دستگاه های موجود در شبکه به آن اعتماد دارند تعیین می کند تا کلید های امنیتی را توزیع کند که به این دستگاه مخصوص مرکز اطمینان (trust center)گفته می شود. در حالت ایده ال، دستگاه ها آدرس مرکز اطمینان را می دانند و شاه کلید اولیه نیز در آن ها پیش بارگذاری شده است. اگر به شبکه یک آسیب لحظه ای وارد شود مشابه انچه در بالا شرح داده شد، فرستاده می شود. کاربرد های معمولی بدون نیاز به اقدامات امنیتی خاص، از یک کلید شبکه که توسط مرکز اطمینان(از طریق یک کانال که در ابتدا ناامن است) ارائه می شود برای برقراری ارتباط استفاده می کنند.

در نتیجه مرکز اطمینان، هم از کلید شبکه نگهداری می کند و هم امنیت نقطه به نقطه را تامین می کند. دستگاه ها به جز برای شاه کلید اولیه، تنها ارتباطاتی را قبول می کنند که از یک کلید که توسط مرکز اطمینان ارائه شده باشد استفاده کنند. معماری امنیتی به شرح ذیل بین لایه های شبکه توزیع شده است:

- زیر لایه MAC توانایی برقراری ارتباطات تک هاپه قابل اطمینان را دارا می باشد. به عنوان یک قانون، سطح امنیتی که این لایه موظف به استفاده از آن است توسط لایه های بالایی تعیین می شود.
- لایه شبکه مدیریت مسیریابی، پردازش پیام های دریافت شده و توانایی پخش درخواست ها را بر عهده دارد. خروجی ها در صورت امکان از کلید لینک مناسب که بسته به مسیریابی تعیین می شود استفاده می کنند در غیر این صورت از کلید شبکه برای حفظ امنیت اطلاعات در برابر دستگاه های خارجی استفاده می شود.
- لایه کاربرد، ایجاد کلید و خدمات انتقال را در اختیار ZDO و کاربرد های مختلف می گذارد.

زیرساخت های سطوح امنیتی بر مبنای CCM* می باشند که نسبت به CCM دارای ویژگی های بیشتری می باشد. بنا بر وب سایت یک مجله کامپیوتر آلمانی، اتوماسیون خانگی ZigBee 1.2 از کلید های اضطراری برای مذاکرات رمزنگاری استفاده می کند. این کلید ها معلوم هستند و نمی توان آن ها را تغییر داد. این ویژگی باعث می شود تا سیستم رمزنگاری به شدت آسیب پذیر باشد.

حال در ادامه برای بررسی بیشتر توسط نرم افزار XCTU و یک محصول از ORBIVO ، کنترل کننده عبور از در

همانطور که در شکل زیر مشاهده میکنید این قطعه را در بر روی در نصب کرده و قطعه اهنربایی را در سمت دیگر (لنگه ی در) قرار میدهیم و حال میبایست این قطعه را به hub متصل کنیم و اطلاعات آن را جمع آوری کنیم.

برای اهداف آموزشی و بررسی دقیق پروتکل zigbee ، فرایندی که در hub قرار است اتفاق بیوفتد را خودمان پیاده سازی کردیم برای همین منظور یک ماژول zigbee را با پروتروکل HA1.2 کانفیگ کرده و در برد رادیویی این قطعه قرار میدهیم

پیش از این که به بررسی بسته های تبادل شده بپردازیم سخت افزار و نرم افزار و محیط کار را به اختصار شرح میدهم

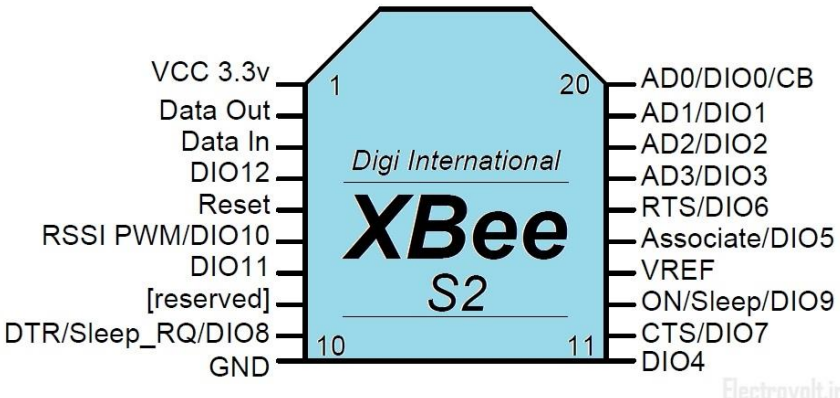
ماژول Xbee S2

این ماژول ساخت شرکت digi است که مانند یک میکرو کنترلر از از پروتکل zigbee استفاده میکند

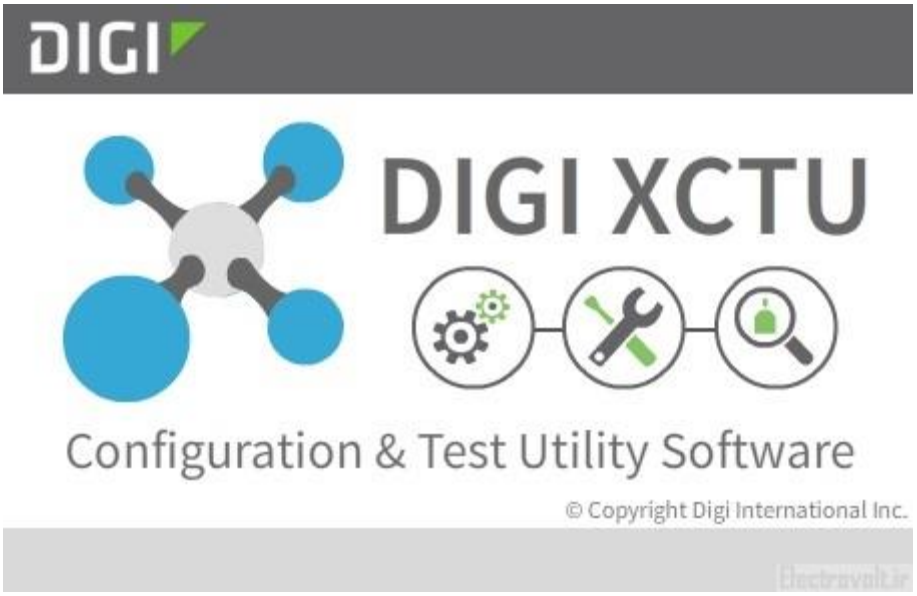
در جدول زیر میتوان سه مدل از ماژول های شرکت digi را مقایسه کرد

Specification	XBee	XBee-PRO (S2)	XBee-PRO (S2B)
Performance			
Indoor/Urban Range	up to 133 ft. (40 m)	Up to 300 ft. (90 m), up to 200 ft (60 m) international variant	Up to 300 ft. (90 m), up to 200 ft (60 m) international variant
Outdoor RF line-of-sight Range	up to 400 ft. (120 m)	Up to 2 miles (3200 m), up to 5000 ft (1500 m) international variant	Up to 2 miles (3200 m), up to 5000 ft (1500 m) international variant
Transmit Power Output	2mW (+3dBm), boost mode enabled 1.25mW (+1dBm), boost mode disabled	50mW (+17 dBm) 10mW (+10 dBm) for International variant	63mW (+18 dBm) 10mW (+10 dBm) for International variant
RF Data Rate	250,000 bps	250,000 bps	250,000 bps
Data Throughput	up to 35000 bps (see chapter 4)	up to 35000 bps (see chapter 4)	up to 35000 bps (see chapter 4)
Serial Interface Data Rate (software selectable)	1200 bps - 1 Mbps (non-standard baud rates also supported)	1200 bps - 1 Mbps (non-standard baud rates also supported)	1200 bps - 1 Mbps (non-standard baud rates also supported)
Receiver Sensitivity	-96 dBm, boost mode enabled -95 dBm, boost mode disabled	-102 dBm	-102 dBm
Power Requirements			
Supply Voltage	2.1 - 3.6 V	3.0 - 3.4 V	2.7 - 3.6 V
Operating Current (Transmit, max output power)	40mA (@ 3.3 V, boost mode enabled) 35mA (@ 3.3 V, boost mode disabled)	295mA (@3.3 V) 170mA (@3.3 V) international variant	205mA, up to 220 mA with programmable variant (@3.3 V) 217mA, up to 232 mA with programmable variant (@3.3 V), International variant
Operating Current (Receive))	40mA (@ 3.3 V, boost mode enabled) 38mA (@ 3.3 V, boost mode disabled)	45 mA (@3.3 V)	47 mA, up to 62 mA with programmable variant (@3.3 V)
Idle Current (Receiver off)	15mA	15mA	15mA
Power-down Current	< 1 uA @ 25ºC	3.5 µA typical @ 25ºC	3.5 µA typical @ 25ºC

که پایه های آن به شرح زیر است :



این ماژول را از طریق پورت سریال و به کمک یه مدل به کامپیوتر متصل میکنیم و نرم افزار XCTU را نصب کرده و باز میکنیم



سپس discover radio madule را انتخاب کرده تا قطعه به نرم افزار متصل شود. حال باید تنظمات مربوط به HA را انجام دهیم پس از داکیومنت detail-HomeAutomation Profile-ZigBee که درضمیه قرار گرفته تنظیمات را به طور کامل انجام میدهیم.

با وصل کردن قطعات ، دو دیوایس بهم متصل میشوند.

حال به بررسی دستورات و کامند هایی که در این بین اتفاق میوفتد میپردازیم

اولین فریم فعال سازی در کوردینتور

Modem Status (API 1)

7E 00 02 8A 06 6F

Start delimiter: 7E

Length: 00 02 (2)

Frame type: 8A (Modem Status)

Status: 06 (The coordinator started)

Checksum: 6F

که به معنای ریست شدن میکرو است

اولین فریم ارسال شده از سنسور هنگام اتصال

Explicit RX Indicator (API 1)

7E 00 1E 91 00 12 4B 00 09 43 E2 4D 70 F0 00 00 00 13 00 00 42 00 F0 70 4D E2 43 09 00 4B 12 00 80 29

Start delimiter: 7E

Length: 00 1E (30)

Frame type: 91 (Explicit RX Indicator)

64-bit source address: 00 12 4B 00 09 43 E2 4D

16-bit source address: 70 F0

Source endpoint: 00

Destination endpoint: 00

Cluster ID: 00 13

Profile ID: 00 00

Receive options: 42

RF data: 00 F0 70 4D E2 43 09 00 4B 12 00 80

Checksum: 29

Cluster ID	Cluster Name	Description
0x0013	Multistate Output (Basic)	An interface for setting the value of a multistate output (typically to the environment) and accessing various characteristics of that value.

00: Transaction sequence number

F0 70 : 16 bit addr

4D E2 43 09 00 4B 12 00 80 : 64 bit address

ادرس خود را معرفی میکند

در بخشZDO

دومین فریم ارسال شده از سنسور هنگام اتصال

Explicit RX Indicator (API 1)

7E 00 20 91 00 12 4B 00 09 43 E2 4D 70 F0 01 0A 00 03 01 04 41 18 00 0A C5 07 F0 4D E2 43 09 00 4B 12 00 2C

Start delimiter: 7E

Length: 00 20 (32)

Frame type: 91 (Explicit RX Indicator)

64-bit source address: 00 12 4B 00 09 43 E2 4D

16-bit source address: 70 F0

Source endpoint: 01

Destination endpoint: 0A

Cluster ID: 00 03

Profile ID: 01 04

Receive options: 41

RF data: 18 00 0A C5 07 F0 4D E2 43 09 00 4B 12 00

Checksum: 2C

0x0003	Identify	Attributes and commands for putting a device into Identification mode (e.g. flashing a light)

Bits: 0-1	2	3	4	5-7
Frame type	Manufacturer specific	Direction	Disable default response	Reserved

18=00 01 00 10 :

00 : Command acts across the entire profile

0: dose not have manufacture specific

1: direction is from node to coordinator

0 : dose not have ACK 010 :meaningless

00: Transaction sequence number

0A: Command identifier

0x0a	Report attributes

C5 07: 16 bit address

F0 4D E2 43 09 00 4B 12 00: 64 bit adrr

ZCL در

فریمی از سمت اند دیوایس برای اعلام میزان پاور باقی مانده

Explicit RX Indicator (API 1)

7E 00 19 91 00 12 4B 00 09 43 E2 4D 70 F0 01 0A 00 01 01 04 41 18 00 0A 21 00 20 A0 E1

Start delimiter: 7E

Length: 00 19 (25)

Frame type: 91 (Explicit RX Indicator)

64-bit source address: 00 12 4B 00 09 43 E2 4D

16-bit source address: 70 F0

Source endpoint: 01

Destination endpoint: 0A

Cluster ID: 00 01

Profile ID: 01 04

Receive options: 41

RF data: 18 00 0A 21 00 20 A0

Checksum: E1

0x0001	Power configuration	Attributes for determining more detailed information about a device's power source(s), and for configuring under/over voltage alarms.

Bits: 0-1	2	3	4	5-7
Frame type	Manufacturer specific	Direction	Disable default response	Reserved

18=00 01 00 10 :

00 : Command acts across the entire profile

0: dose not have manufacture specific

1: direction is from node to coordinator

0 : dose not have ACK 010 :meaningless

00: Transaction sequence number

0A: Command identifier

0x0a	Report attributes

حال به کلاستر Power configuration را بررسی میکنیم :

Table 3.16 Power Configuration Attribute Sets

Attribute Set Identifier	Description
0x000	Mains Information
0x001	Mains Settings
0x002	Battery Information
0x003	Battery Settings
0x004 – 0xfff	Reserved

Table 3.20 Attributes of the Battery Information Attribute Set

Identifier	Name	Type	Range	Access	Default	Mandatory / Optional
0x0020	*BatteryVoltage*	Unsigned 8-bit integer	0x00 – 0xff	Read only	-	O

00 20 : identifier

A0:

که نتیجه گزارش اعلام میکند که ولتاژ باتری به میزان A0/FF است (60 درصد یا 160/255) است

فریم ارسال اطلاعات از سنسور

Explicit RX Indicator (API 1)

7E 00 1B 91 00 12 4B 00 09 43 E2 4D 9F 2D 01 0A 05 00 01 04 41 19 03 00 21 01 00 00 00 00 36

Start delimiter: 7E

Length: 00 1B (27)

Frame type: 91 (Explicit RX Indicator)

64-bit source address: 00 12 4B 00 09 43 E2 4D

16-bit source address: 9F 2D

Source endpoint: 01

Destination endpoint: 0A

Cluster ID: 05 00

Profile ID: 01 04

Receive options: 41

RF data: 19 03 00 21 00 10 00 00 00

Checksum: 36

Cluster ID: 05 00 → Security and Safety - IAS Zone

Bits: 0-1	2	3	4	5-7
Frame type	Manufacturer specific	Direction	Disable default response	Reserved

19=00 01 00 11 :

00 : Command acts across the entire profile

0: dose not have manufacture specific

1: direction is from node to coordinator

0 : dose not have ACK 011 :meaningless

03: Transaction sequence number

00 21 : unsigned 32 bit integer

0x0021	*ElapsedActive Time*	Unsigned 32-bit integer	-	R*W	0xffffffff	O

Table 8.3 Attributes of the Zone Information Attribute Set

Identifier	Name	Type	Range	Access	Default	Mandatory / Optional
0x0000	*ZoneState*	8-bit enumeration	All	Read only	0x00	M
0x0001	*ZoneType*	16-bit enumeration	All	Read only	-	M
0x0002	*ZoneStatus*	16-bit bitmap	All	Read only	0x00	M

00 01 : zone type

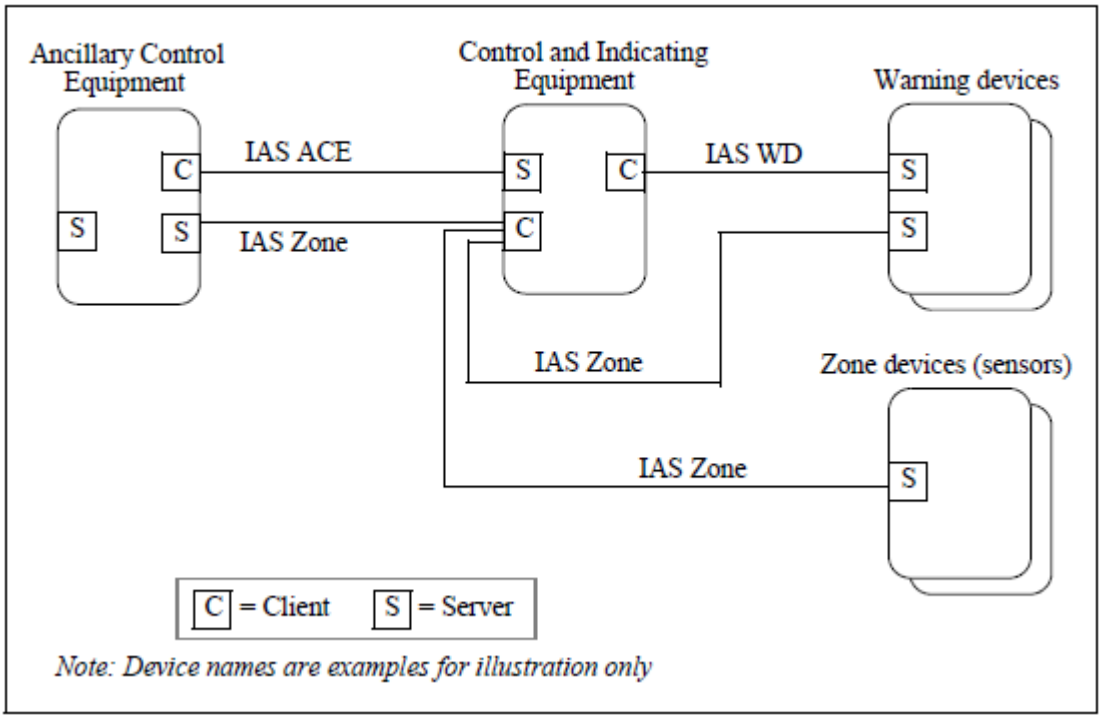
Table 8.5 Values of the *ZoneType* Attribute

Attribute Value	Zone Type	Alarm1	Alarm2
0x0000	Standard CIE	System Alarm	-

0000 : standard CIE است

که به معنای تغییر حالت در ، در است

لازم به ذکر است با رسیدن این بسته System Alarm در لایه امنیت فعال میشود.



اگر شبکه کامل باشد ، بسته ای از کلاستر IAS WD توسط control and indicatin به سایر نقاط منتقل میشود وگزارش میکند.

در ادامه دستگاه دیگری را بررسی میکنیم که عملگر نیز داشته باشد :

و بتوانیم با کامند زدن آن را بررسی کنیم ، برای این کار از دستگاه جا به جایی پرده استفاده میکینیم ، و با کامند دادن همه مسائل آن را تفسیر میکنیم:

دستور اول

ZDO-Network Address Request

Explicit Addressing Command Frame (API 1)

E 00 1E 11 00 00 12 4B 00 13 56 8F 89 FF FE 00 00 00 00 00 00 00 00 01 13 56 8F 89 00 12 4B 00 00 347

Start delimiter: 7E

(30) Length: 00 1E

Frame type: 11 (Explicit Addressing Command Frame)

(0) Frame ID: 00

bit dest. address: 00 12 4B 00 13 56 8F 89-64

bit dest. address: FF FE-16

Source endpoint: 00

Dest. endpoint: 00

Cluster ID: 00 00

Profile ID: 00 00

(0) Broadcast radius: 00

Transmit options: 00

RF data: 01 13 56 8F 89 00 12 4B 00 00

Checksum: 34

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose 64-bit (network) address is being discovered
Request Type	1	0x00 – Single device response. (Only the device with a matching IEEE address responds.) 0x01 – Extended response. (The device with a matching IEEE address responds AND sends a list of the 16-bit addresses of devices in its associated device list starting at 'Start Index' until the next entry won't fit in the data payload.
Start Index	1	Indicates the starting index in the associated device list to return 16-bit addresses. Only used if extended response is requested.

و در جواب:

Explicit RX Indicator (API 1)

E 00 1E 91 00 12 4B 00 13 56 8F 89 A7 AB 00 00 80 00 00 00 01 01 81 13 56 8F 89 00 12 4B 00 AB A7 0B7

Start delimiter: 7E

(30) Length: 00 1E

Frame type: 91 (Explicit RX Indicator)

bit source address: 00 12 4B 00 13 56 8F 89-64

bit source address: A7 AB-16

Source endpoint: 00

Destination endpoint: 00

Cluster ID: 80 00

Profile ID: 00 00

Receive options: 01

RF data: 01 81 13 56 8F 89 00 12 4B 00 AB A7

Checksum: 0B

Field Name	Size (bytes)	Description
Status	1	
IEEE Address	8	Indicates the 64-bit address of the responding device
Network Address	2	Indicates the 16-bit address of the responding device

در ادامه دستور :

ZDO-Node Descriptor Request

Explicit Addressing Command Frame (API 1)

E 00 17 11 01 00 12 4B 00 13 56 8F 89 A7 AB 00 00 00 02 00 00 00 00 01 AB A7 687

Start delimiter: 7E

(23) Length: 00 17

Frame type: 11 (Explicit Addressing Command Frame)

(1) Frame ID: 01

bit dest. address: 00 12 4B 00 13 56 8F 89-64

bit dest. address: A7 AB-16

Source endpoint: 00

Dest. endpoint: 00

Cluster ID: 00 02

Profile ID: 00 00

(0) Broadcast radius: 00

Transmit options: 00

RF data: 01 AB A7

Checksum: 68

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose node descriptor is being requested.

و در پاسخ اطاعاتی کلی در مورد نوع گره نهایی میدهد که به شرح زیر است :

Explicit RX Indicator (API 1)

E 00 23 91 00 12 4B 00 13 56 8F 89 A7 AB 00 00 80 02 00 00 01 01 00 AB A7 01 40 8E 00 00 50 A0 00 00 7 00 A0 00 00 09

Start delimiter: 7E

(35) Length: 00 23

Frame type: 91 (Explicit RX Indicator)

bit source address: 00 12 4B 00 13 56 8F 89-64

bit source address: A7 AB-16

Source endpoint: 00

Destination endpoint: 00

Cluster ID: 80 02

Profile ID: 00 00

Receive options: 01

RF data: 01 00 AB A7 01 40 8E 00 00 50 A0 00 00 00 A0 00 00

Checksum: 09

Field Name	Size (bytes)	Description
Status	1	
Network Address	2	Indicates the 16-bit address of the responding device
Node Descriptor	Variable	See node descriptor below.

Node Descriptor

Name	Size (bits)	Description
Logical Type	3	Indicates the logical device type: 000 – Coordinator 001 – Router 010 – End device
Complex Descriptor Available	1	0 – Complex descriptor not supported 1 – Complex descriptor supported
User Descriptor Available	1	0 – User descriptor not supported 1 – User descriptor supported
Reserved	3	
APS flags	3	Not supported. Set to 0
Frequency Band	5	bit0 – 868 MHz bit1 – Reserved bit2 – 900 MHz bit3 – 2.4 GHz bit4 – Reserved
MAC capability flags	8	Bit0 – Alternate PAN coordinator Bit1 – Device Type Bit2 – Power source Bit3 – Receiver on when idle Bit4-5 – Reserved Bit6 – Security capability Bit7 – Allocate address
Manufacturer Code	16	Indicates the manufacturer's code assigned by the ZigBee Alliance.
Maximum Buffer Size	8	Maximum size in bytes, of a data transmission (including APS bytes)
Maximum incoming transfer size	16	Maximum number of bytes that can be received by the node.
Server mask	16	
Maximum outgoing transfer size	16	Maximum number of bytes that can be transmitted by this device, including fragmentation.
Descriptor capability field	8	Bit0 – Extended active endpoint list available Bit1 – Extended simple descriptor list available

حال باید end point های سمت مقابل را بدست آوریم که با دستور زیر حاصل میشود :

ZDO-Active Endpoints Request

Explicit Addressing Command Frame (API 1)

E 00 17 11 01 00 12 4B 00 13 56 8F 89 A7 AB 00 00 00 05 00 00 00 00 01 AB A7 657

Start delimiter: 7E

(23) Length: 00 17

Frame type: 11 (Explicit Addressing Command Frame)

(1) Frame ID: 01

bit dest. address: 00 12 4B 00 13 56 8F 89-64

bit dest. address: A7 AB-16

Source endpoint: 00

Dest. endpoint: 00

Cluster ID: 00 05

Profile ID: 00 00

(0) Broadcast radius: 00

Transmit options: 00

RF data: 01 AB A7

Checksum: 65

Active Endpoints Request

Cluster ID: 0x0005

Description: Transmission used to discover the active endpoints on a device with a matching 16-bit address.

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose active endpoint list being requested.

و جواب زیر حاصل میشود :

Explicit RX Indicator (API 1)

E 00 18 91 00 12 4B 00 13 56 8F 89 A7 AB 00 00 80 05 00 00 01 01 00 AB A7 01 01 637

Start delimiter: 7E

(24) Length: 00 18

Frame type: 91 (Explicit RX Indicator)

bit source address: 00 12 4B 00 13 56 8F 89-64

bit source address: A7 AB-16

Source endpoint: 00

Destination endpoint: 00

Cluster ID: 80 05

Profile ID: 00 00

Receive options: 01

RF data: 01 00 AB A7 01 01

Checksum: 63

Field Name	Size (bytes)	Description
Status	1	
Network Address	2	Indicates the 16-bit address of the responding device
Active Endpoint Count	1	Number of endpoints in the following endpoint list
Active Endpoint List	Variable	List of endpoints supported on the destination device. One byte per endpoint.

حال میبایست محتوای endpoint 01 را بررسی کنیم ، برای همین منظور دستور زیر را اجرا میکنیم:

ZDO-Simple Descriptor Request

Explicit Addressing Command Frame (API 1)

E 00 18 11 01 00 12 4B 00 13 56 8F 89 A7 AB 00 00 00 04 00 00 00 00 01 AB A7 01 657

Start delimiter: 7E

(24) Length: 00 18

Frame type: 11 (Explicit Addressing Command Frame)

(1) Frame ID: 01

bit dest. address: 00 12 4B 00 13 56 8F 89-64

bit dest. address: A7 AB-16

Source endpoint: 00

Dest. endpoint: 00

Cluster ID: 00 04

Profile ID: 00 00

(0) Broadcast radius: 00

Transmit options: 00

RF data: 01 AB A7 01

Checksum: 65

Field Name	Size (bytes)	Description
Network Address	2	16-bit address of a device in the network whose simple descriptor is being requested.
Endpoint	1	The endpoint on the destination from which to obtain the simple descriptor.

و جواب به شرح زیر است :

Explicit RX Indicator (API 1)

E 00 2B 91 00 12 4B 00 13 56 8F 89 A7 AB 00 00 80 04 00 00 01 01 00 AB A7 14 01 04 01 03 02 00 05 00 7 00 02 01 05 00 04 00 06 00 01 00 00 2F

Start delimiter: 7E

(43) Length: 00 2B

Frame type: 91 (Explicit RX Indicator)

bit source address: 00 12 4B 00 13 56 8F 89-64

bit source address: A7 AB-16

Source endpoint: 00

Destination endpoint: 00

Cluster ID: 80 04

Profile ID: 00 00

Receive options: 01

RF data: 01 00 AB A7 14 01 04 01 03 02 00 05 00 00 02 01 05 00 04 00 06 00 01 00 00

Checksum: 2F

به طور کامل شرح میدهیم :

01: seq num

00: status

Network addr: A7AB

Length : 14(hex)-> 20

Field Name	Size (bytes)	Description
Status	1	
Network Address	2	Indicates the 16-bit address of the responding device
Length	1	Length of the simple descriptor
Simple Descriptor	Variable	See simple descriptor below.

ادامه بسته:

01 04 01 03 02 00 05 00 00 02 01 05 00 04 00 06 00 01 00 00

Name	Size (bits)	Description
Endpoint	8	The endpoint on the node to which this descriptor refers.
Application profile ID	16	The profile ID supported on this endpoint.
Application device ID	16	Specifies the device description identifier supported on the device
Application device version	4	The version of the device description supported on this endpoint.
Reserved	4	
Input cluster count	8	The number of input clusters supported on this endpoint.
Input cluster list	Variable	The list of input clusters supported on this endpoint. Each cluster is 2 bytes in size. This field is not included if the input cluster count is 0.
Output cluster count	8	The number of output clusters supported on this endpoint.
Output cluster list	Variable	The list of output clusters supported on this endpoint. Each cluster is 2 bytes in size. This field is not included if the output cluster count is 0.

01:endpoint

04 01 : application profile = 01 04 HA v1.2

03 02 :Application device id : = 02 03 : window covering controller

00: application device version + Reserved

05: Input cluster coint -00 00

-01 02---> کلاستر مربوط به پرده ، توابع در این کلاستر واقع شده

-00 05

-00 04

-00 06

01 : out cluster count -00 00

7.4.1.3 Cluster Identifiers

Identifier	Name
0x0102	Window Covering

توابع کلاستر window covering

Table 7-45. Commands Received by the Window Covering Server Cluster

Command ID	Description	M/O
0x00	Up / Open	M
0x01	Down / Close	M
0x02	Stop	M
0x04	Go To Lift Value	O
0x05	Go to Lift Percentage	O
0x07	Go to Tilt Value	O
0x08	Go to Tilt Percentage	O

حال به پیاده سازی این سه تابع اول که حتما میبایست در سخت افزار پیاده شده باشد ، میپردازیم ، نکته قابل توجه در پیام های ZCL این است که باید پیام ها از فرمت زیر تبعیت کنند :

Bits: 8	0/16	8	8	Variable
Frame control	Manufacturer code	Transaction sequence number	Command identifier	Frame payload
ZCL header				ZCL payload

که جزیات فریم کنترل به شرح زیر است :

Bits: 0-1	2	3	4	5-7
Frame type	Manufacturer specific	Direction	Disable Default Response	Reserved

Frame Type Value b1b0	Description
00	Command is global for all clusters, including manufacturer specific clusters[2]
01	Command is specific or local to a cluster

از ان جایی که window covering , generic نیست ، 01 باید باشد ، ddr=0 , 0=direction manufac=0

در ادامه command identifire را از توابع کلاس انتخاب کرده و شماره بسته را مشخص میکنیم و سه بسته زیر را میسازیم :

Explicit Addressing Command Frame (API 1)

E 00 17 11 01 00 12 4B 00 13 56 8F 89 A7 AB 00 01 01 02 01 04 00 00 01 02 00 B17

Start delimiter: 7E

(23) Length: 00 17

Frame type: 11 (Explicit Addressing Command Frame)

(1) Frame ID: 01

bit dest. address: 00 12 4B 00 13 56 8F 89-64

bit dest. address: A7 AB-16

Source endpoint: 00

Dest. endpoint: 01

Cluster ID: 01 02

Profile ID: 01 04

(0) Broadcast radius: 00

Transmit options: 00

RF data: 01 02 00

Checksum: B1

Explicit Addressing Command Frame (API 1)

E 00 17 11 01 00 12 4B 00 13 56 8F 89 A7 AB 00 01 01 02 01 04 00 00 01 03 01 AF7

Start delimiter: 7E

(23) Length: 00 17

Frame type: 11 (Explicit Addressing Command Frame)

(1) Frame ID: 01

bit dest. address: 00 12 4B 00 13 56 8F 89-64

bit dest. address: A7 AB-16

Source endpoint: 00

Dest. endpoint: 01

Cluster ID: 01 02

Profile ID: 01 04

(0) Broadcast radius: 00

Transmit options: 00

RF data: 01 03 01

Checksum: AF

Explicit Addressing Command Frame (API 1)

E 00 17 11 01 00 12 4B 00 13 56 8F 89 A7 AB 00 01 01 02 01 04 00 00 01 04 02 AD7

Start delimiter: 7E

(23) Length: 00 17

Frame type: 11 (Explicit Addressing Command Frame)

(1) Frame ID: 01

bit dest. address: 00 12 4B 00 13 56 8F 89-64

bit dest. address: A7 AB-16

Source endpoint: 00

Dest. endpoint: 01

Cluster ID: 01 02

Profile ID: 01 04

(0) Broadcast radius: 00

Transmit options: 00

RF data: 01 04 02

Checksum: AD