



عنوان

امنیت مسیریابی در اینترنت اشیا

عنوان	صفحه
چکیده	۷
فصل اول: مقدمه	
۱-۱- مقدمه	۱۰
فصل دوم: بستر تحقیق	
۱-۲- مقدمه	۱۴
۲-۲- اینترنت اشیا	۱۵
۳-۲- چشم انداز اینترنت اشیا	۱۶
۴-۲- کاربردهای اینترنت اشیا	۱۶
۱-۴-۲- انتقال و سامان‌دهی	۱۷
۱-۴-۲-۱- سامان‌دهی	۱۷
۲-۴-۲-۱- کمک به رانندگی	۱۷
۳-۴-۲-۱- نشان دادن پارامترهای محیطی	۱۸
۴-۴-۲-۱- نقشه‌های تکمیل شده	۱۸
۲-۴-۲- سلامتی	۱۸
۱-۴-۲-۱- شناسایی و تایید افراد	۱۸
۲-۴-۲-۲- اثرگذاری	۱۹
۳-۴-۲-۳- حسگر	۱۹
۳-۴-۲- محیط‌های هوشمند	۱۹
۱-۴-۲-۳- خانه‌ها و اداره‌های راحت	۱۹
۴-۴-۲- اجتماعی و شخصی	۱۹
۵-۴-۲- تله پورت	۱۹
۶-۴-۲- حمل و نقل	۲۰
۷-۴-۲- حضور مجازی	۲۰
۵-۲- خواص سیستم‌های خودکار اینترنت اشیا	۲۰
۱-۵-۲- خودسازگاری	۲۰
۲-۵-۲- خودسازماندهی	۲۰
۳-۵-۲- خود بهینه‌سازی	۲۱
۴-۵-۲- خودپیکربندی	۲۱
۵-۵-۲- خودترمیمی	۲۱

۲۱	۲-۵-۶- خودتوصیفی
۲۱	۲-۶- امنیت در اینترنت اشیا
۲۴	۲-۷- تهدیدات امنیتی خاص اینترنت اشیا
۲۵	۲-۸- چالش‌های امنیتی استانداردها و پروتکل‌های ارتباطی اینترنت اشیا
۲۵	۲-۹- تهدیدها و چالش‌های امنیتی در معماری لایه‌ای اینترنت اشیا
۲۶	۲-۱۰- نیازمندی‌های امنیتی مهم در اینترنت اشیا
۲۷	۲-۱۰-۱- امنیت شبکه
۲۷	۲-۱۰-۲- مدیریت هویت
۳۵	۲-۱۰-۳- حریم خصوصی
۲۸	۲-۱۰-۴- اعتماد
۲۹	۲-۱۰-۵- انعطاف‌پذیری

فصل سوم: پیشینه تحقیق

۳۱	۳-۱- مقدمه
۳۲	۳-۲- پروتکل‌های مسیریابی در اینترنت اشیا
۳۲	۳-۲-۱- شبکه‌های شخصی بی‌سیم کم قدرت
۳۳	۳-۲-۲- پروتکل مسیریابی برای شبکه‌های کم قدرت
۳۶	۳-۲-۳- IPv6 در طی زمان حالت نوسانی
۳۶	۳-۳- آسیب‌پذیری به مسیریابی در اینترنت اشیا
۳۶	۳-۳-۱- تهدیدهای مربوط به پروتکل‌های مسیریابی
۳۸	۳-۳-۲- پروتکل‌های مسیریابی ایمن در IoT
۳۸	۳-۳-۱- مسیریابی چندگانه امن برای ارتباطات IoT
۳۹	۳-۳-۲- TSRF یک چارچوب مسیریابی امن در شبکه‌های حسگر بی‌سیم
۳۹	۳-۳-۳- اعتماد مبتنی بر اقرار دوگانه
۳۹	۳-۳-۴- طرح مدیریت اعتماد مبتنی بر گروه
۴۰	۳-۳-۵- پروتکل مسیریابی مبتنی بر اعتماد (CLT) مشترک
۴۳	۳-۴- اعتماد در مسیریابی امن در اینترنت اشیا
۴۵	۳-۵- مسیریابی امن در IoT: مسائل و چالش‌ها
۴۵	۳-۵-۱- چالش‌های پژوهش
۴۷	۳-۵-۲- PRL: چالش‌های تحقیق

فصل چهارم: نتیجه گیری و پیشنهادات

۴-۱- نتیجه گیری و پیشنهادات ۵۱

۵۳

مراجع

فهرست شکل‌ها

- شکل ۱-۱- اتصال گره‌های اینترنت اشیا که متشکل از مسیریاب‌های لبه ۱۰
- شکل ۱-۲- پیش بینی اتصال بیش از ۵۰ میلیارد دستگاه تا سال ۲۰۲۰ ۱۱
- شکل ۲-۱- نمونه‌ای از اینترنت اشیا: یک دید کلی ۱۵
- شکل ۲-۲- دامنه‌ی کاربردها و طرح‌های مرتبط ۱۷
- شکل ۳-۲- آسیب‌پذیری امنیتی دستگاه‌های اینترنت اشیا ۲۴
- شکل ۴-۲- معماری امنیتی اینترنت اشیا و نیازمندی‌های امنیتی در هر لایه ۲۵
- شکل ۵-۲- نیازمندی‌های امنیتی اصلی و زیرمولفه‌هایشان ۲۶
- شکل ۶-۲- خاصیت اینترنت اشیا و ضریب نفوذ نیازهای امنیتی ۲۹
- شکل ۱-۳- پروتوکول‌های مربوط به دستگاه‌های IOT ۳۴
- شکل ۲-۳- یک شبکه RPL ۳۵

فهرست جدول‌ها

- جدول ۳-۱- خلاصه‌ای از حملات و اقدامات متقابل RPL ۳۸
- جدول ۳-۲- خلاصه‌ای از پروتکل‌های مسیریابی امن برای اینترنت اشیا ۴۰
- جدول ۳-۳- بررسی و مقایسه پروتکل‌های مسیریابی امن برای اینترنت اشیا ۴۲
- جدول ۳-۴- خلاصه از مدل‌های Trust برای مسیریابی امن در شبکه‌های حسگر ۴۴

چکیده

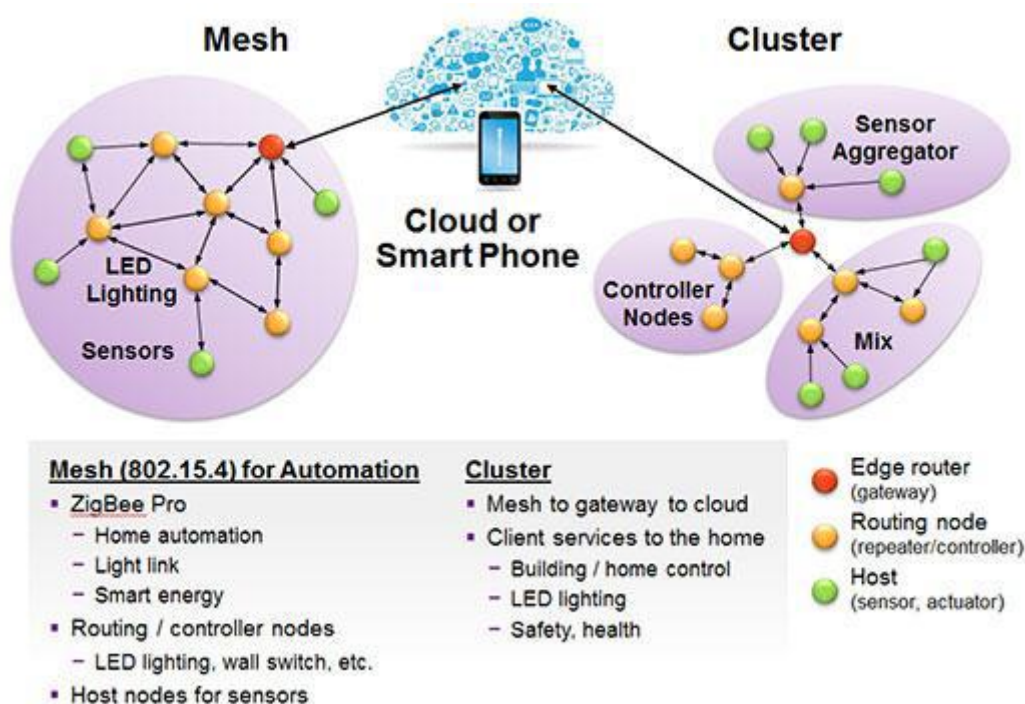
اینترنت اشیاء را می‌توان به عنوان یک شبکه فراگیر و جهانی تعریف نمود که سیستمی را برای نظارت و کنترل جهان فیزیکی از طریق جمع‌آوری، پردازش و تجزیه و تحلیل اطلاعات تولید شده توسط دستگاه‌های حسگر اینترنت اشیا فراهم می‌آورد. پیش‌بینی شده است که تا سال ۲۰۲۰ تعداد دستگاه‌های متصل به صورت نمایی تا ۵۰ بیلیون افزایش می‌یابد. عاملین اصلی این رشد، دستگاه‌هایی هستند که به طور روزمره به کار می‌روند، مانند اتومبیل‌ها، یخچال‌ها، دستگاه‌های تهویه، چراغ‌ها، تلفن‌های همراه و دیگر فن‌آوری‌هایی نظیر زیرساخت‌های تولیدی که در حال حاضر در سراسر جهان متصل هستند. واضح است که امنیت یک عامل اساسی برای گسترش موفق و استفاده از اکثر برنامه‌های کاربردی اینترنت اشیا و به ویژه در مسیریابی امن از میان گره‌های حسگر اینترنت اشیا است و در نتیجه، لازم است مکانیسم‌هایی برای ایجاد ارتباطات امن جهت دستگاه‌های فعال شده توسط فن‌آوری اینترنت اشیا، طراحی شود. در این سمینار، پروتکل‌های مسیریابی موجود و مکانیزم لازم برای تامین امنیت مسیریابی در اینترنت اشیا، به عنوان مسائل تحقیقاتی باز مورد تجزیه و تحلیل قرار می‌گیرد. همچنین بررسی می‌شود که چگونه روش‌های موجود مسیریابی امن در اینترنت اشیا را تضمین می‌کنند، نقاط ضعف آنها، تهدیدهای پیش روی مسیریابی امن در اینترنت اشیا، چالش‌ها و استراتژی‌های مربوط به کارهای تحقیقاتی آتی جهت بهبود مسیریابی امن در اینترنت اشیا نیز مورد تجزیه و تحلیل قرار می‌گیرد.

کلمات کلیدی: اینترنت اشیا، مسیریابی، امنیت، شبکه حسگر، گره.

فصل اول

مقدمه

با پیشرفت در محاسبات و ارتباطات بی‌سیم، یک پارادایم جدید تحت عنوان اینترنت اشیا شناخته شده است و به سرعت تحقیقات جالب و انقلاب صنعتی مهمی را به راه انداخته است. اینترنت اشیا^۱ را می‌توان به عنوان یک شبکه فراگیر و جهانی تعریف نمود که سیستمی را برای نظارت و کنترل جهان فیزیکی از طریق جمع‌آوری، پردازش و تجزیه و تحلیل اطلاعات تولید شده توسط دستگاه‌های حسگر اینترنت اشیا فراهم می‌آورد. این دستگاه در رابطه با سنجش و ارتباطات مانند حسگرها، دستگاه‌های شناسایی فرکانس رادیویی، دستگاه‌های موقعیت یاب جهانی، حسگرهای مادون قرمز، لیزر، اسکنرها، دیسک، شبکه‌های محلی بی‌سیم ساخته شده‌اند. در واقع "همه چیز" را می‌توان به اینترنت متصل کرد و از این رو مدیریت از راه دور کنترل و مدیریت نمود. این دستگاه‌ها می‌توانند در میان خود و (ماشین به ماشین) از طریق ارسال و دریافت اطلاعات، سنجش دمای محیط، فشار و غیره تعامل و ارتباط داشته باشند. یعنی که انتقال اطلاعات از یک دستگاه به دستگاه‌های دیگر برای پردازش و یا اقدامات بیشتر. بر اساس اتحادیه بین‌المللی مخابرات و خوشه تحقیقات اروپایی اینترنت اشیا، اینترنت از اشیا است به عنوان یک شبکه زیرساخت جهانی تعریف می‌شود که دارای قابلیت‌های پیکربندی متمرکز بر استاندارد و پروتکل‌های ارتباطی است و در آن اشیا فیزیکی و مجازی دارای هویت، ویژگی‌های فیزیکی و ویژگی‌های مجازی هستند و از طریق رابطه‌های هوشمند و پیچیده در شبکه اطلاع‌رسانی بدون مرز ارتباط برقرار می‌کنند.



شکل ۱-۱- اتصال گره‌های اینترنت اشیا که متشکل از مسیریاب‌های لبه^۲، گره‌های مسیریابی^۳ (که به عنوان گره‌های کنترلی نیز عمل می‌کنند) و حسگرهای متحرک^۴ یا گره‌های عملگر^۵ است [1].

¹ Internet of Things (IoT)

² Routers edge

³ routing nodes

⁴ mobile sensory

⁵ actuator nodes