«بسم الله الرحمن الرحیم»

موسسه آموزش عالی صنعتی مازندران
گروه مهندسی کامپیوتر

پایان نامه برای دریافت درجه کارشناسی ارشد
در رشته مهندسی فناوری اطلاعات گرایش شبکه های کامپیوتری

«ارائه یک پروتکل مسیریابی RPL ارتقاء یافته مبتنی بر اعتماد برای اینترنت اشیاء »

استاد راهنما:
دکتر پیام محمودی نصر

استاد مشاور:
دکتر میثم یداله زاده طبری

تهیه شده توسط:
یداله حسین زاده سرخ

زمستان ۱۴۰۰

اینترنت اشیاء یا IOT چیست؟

- ✓ شبکه ای از اشیاء متصل به اینترنت و قابل مدیریت و کنترل از راه دور
- ✓ اشیاء متصل به اینترنت دارای قابلیت ارسال و دریافت اطلاعات مابین خودشان.
- ✓ ارتباط سنسورها و دستگاه ها با شبکه

هدف کلی اینترنت اشیاء چیست؟

ایجاد اتصال ماشین به ماشین (M2M)
انسان به انسان (H2H)
انسان به ماشین (H2M)

چالش مهم و حیاتی: دسترسی به اطلاعات و نابودی آن توسط مهاجم

موضوع پژوهش

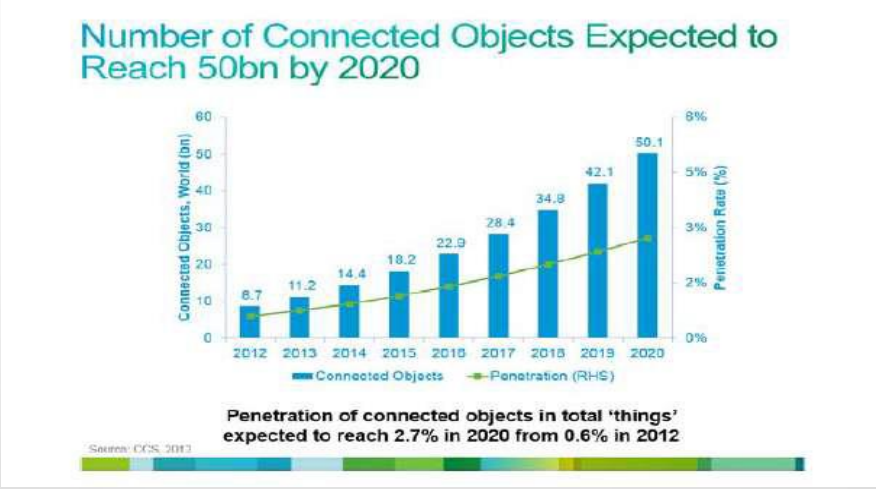
«توسعه ی پروتکل مسیریابی RPL ارتقا یافته مبتنی بر اعتماد برای اینترنت اشیاء»

ضرورت پژوهش

افزایش روز افزون تعداد اشیاء متصل

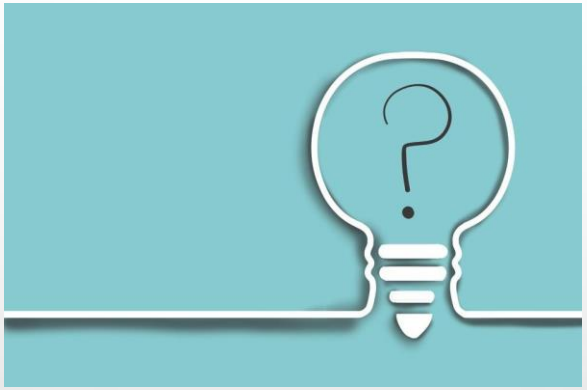
افزایش اهمیت امنیت شبکه ها در اینترنت اشیاء

ارایه ی روش امنیتی کارآمد برای توقف یا به حداقل رساندن تاثیر حملات



پرسش های پژوهش

- کدام حملات مسیریابی هستند که به یکپارچگی و دسترس پذیری اطلاعات مسیریابی در میان گره های حسگر IOT صدمه و آسیب می زنند؟
- چه سیستمی را می توان به کار برد تا مسیریابی امن شبکه در میان گره های حسگر IOT را به روش مؤثر و کارآمد حفظ نماید؟
- چگونه می توان سیستمی طراحی نمود که سطح امنیتی به سطح اعتماد گره ها وابسته باشد؟
- سیستم جدید در حالی که حملات مسیریابی را مورد توجه قرار می دهد چگونه می تواند تأثیر مخرب بر عملکرد اجرایی شبکه را کاهش و به حداقل میزان خود برساند؟



اهداف پژوهش

- ایجاد یک مسیر امن در شبکه با استفاده از پروتکل مسیریابی RPL
- شناسایی و حذف نقاط مورد تهدید
- طراحی یک چارچوب مسیریابی امن به نام SR-Framework بر اساس مقیاس بندی اندازه اینترنت اشیاء

این چارچوب سیستمی را برای شناسایی و جداسازی گره های بدخواه و دارای سوء نیت فراهم می سازد. هر گره، قابلیت اعتماد همسایه های مستقیمش را بر مبنای ارزش اعتماد محاسبه و با ارزش اعتماد پیشنهاد شده مقایسه می کند.

یافتن همسایه های بدخواه یا آسیب زننده دارای ارزش های اعتماد پایین.

گره های دارای ارزش اعتماد بالا (مقادیر اعتماد زیاد) برای مسیریابی امن انتخاب می شوند.

محدودیت های پژوهش

- محدودیت های ذاتی نرم افزار متلب
- تفاوت عملکردی متفاوت با محیط واقعی
- پیشرفته نبودن حملات به دلیل ایزوله بودن محیط شبیه سازی

مزایا و معایب اینترنت اشیاء

مزایا:
کمک به افراد در کارهای روزمره
مفید بودن در سیستم ایمنی بدن
امکان بررسی علائم حیاتی بیمار
کمک به امنیت شخصی افراد
آگاهی افراد از مکان و شرایط یکدیگر
قابلیت ردیابی مشتریان

معایب:
نقض حریم شخصی
اتکای بیش از اندازه بر فناوری
فقدان شغل

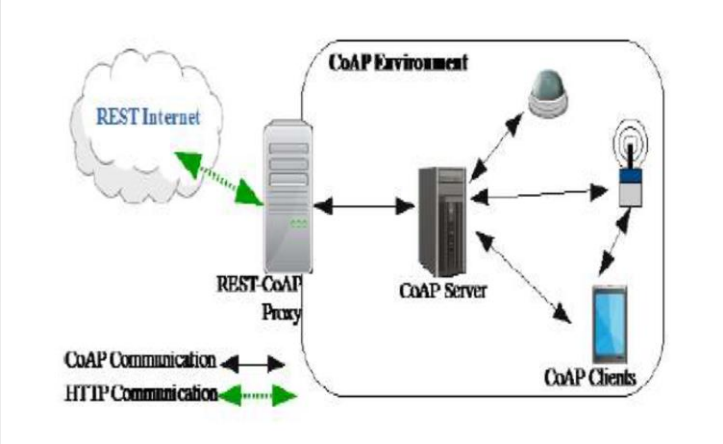
کاربردهای اینترنت اشیاء

شهر هوشمند
نظارت بر محیط زیست
مدیریت انرژی
اتوماسیون خانگی
مدیریت زیر ساخت
حمل و نقل هوشمند
پزشکی و مراقبت های بهداشتی

پروتکل های مسیریابی اینترنت اشیاء

پروتکل های لایه کاربرد:

- **پروتکل COAP**



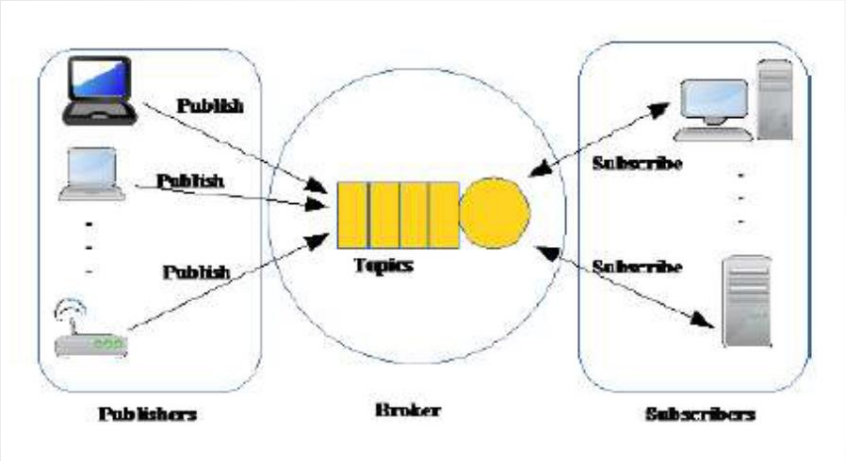
پروتکل COAP از متدهایی مانند GET (برای دریافت و خواندن اطلاعات)، POST (برای ساخت و ارسال اطلاعات)، PUT (برای تغییر و جایگزین کردن اطلاعات) و DELETE (برای حذف اطلاعات) استفاده می کند تا بتوان عملیات CRUD را انجام دهد.

ویژگی ها:

- مشاهده و نظارت بر منابع
- انتقال منابع به صورت بلوکی
- کشف منابع
- قابلیت تعامل با HTPP
- امنیت

پروتکل های مسیریابی اینترنت اشیاء (ادامه)

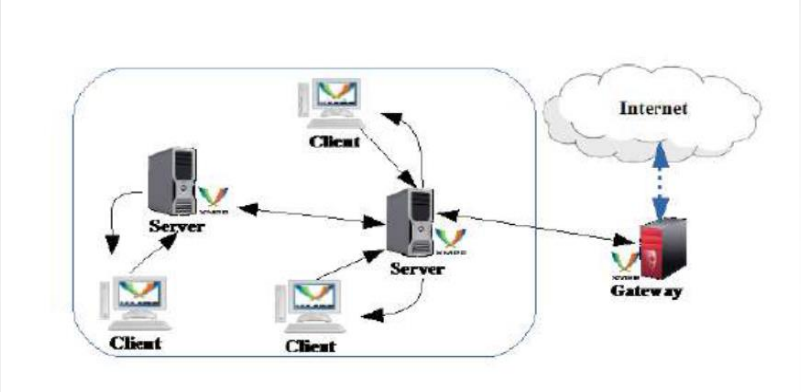
- پروتکل MQTT



یک پروتکل انتقال پیام است.
هدف اصلی پروتکل MQTT متصل کردن وسایل تو کار با شبکه ها از طریق میان افزارها و برنامه های کاربردی است به این صورت که عملکرد اتصال از یک مکانیسم مسیریابی (یک به یک، یک به چند و چند به چند) استفاده می کند.

پروتکل های مسیریابی اینترنت اشیاء (ادامه)

- پروتکل XMPP

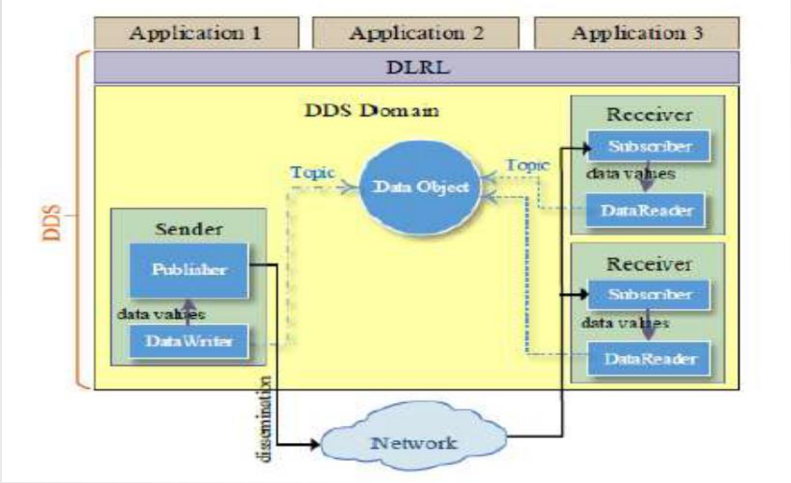


یک پروتکل پیام رسان فوری است که در نرم افزارهای پیام رسان و تماس های صوتی و تصویری کاربرد دارد.
این پروتکل این امکان را به کاربران می دهد تا بتوانند از طریق ارسال پیام در اینترنت بدون در نظر گرفتن این که در حال استفاده از چه نوع سیستم عاملی می باشند با یکدیگر ارتباط برقرار کنند. علاوه بر این، این پروتکل به نرم افزارهای پیام رسان فوری امکان احراز هویت، کنترل دسترسی، حفظ حریم شخصی و رمزنگاری را می دهد و قابلیت سازگاری با دیگر پروتکل ها را نیز دارا می باشد.

- سرویس دهنده مدیریت لینک ها و مسیریابی پیام ها را انجام می دهد.
- درگاه برای این استفاده می شود تا ارتباط پایداری بین شبکه های ناهمگن برقرار شود.
- سرویس گیرنده می تواند با پروتکل TCP/IP به سرویس دهنده متصل شده و محتویات را با پروتکل جریانی XML منتقل کند.

پروتکل های مسیریابی اینترنت اشیاء (ادامه)

- **پروتکل DDS**



پروتکل ارتباطی مبتنی بر مدار انتشار/ اشتراک بلادرنگ، برای ارتباطات ماشین با ماشین

برخلاف MQTT از مدل پخش همگانی (ارسال اطلاعات از یک کامپیوتر مرکزی به دیگر کامپیوترها) استفاده می کند.

معماری DDS دو لایه را تعریف می کند:
DCPS (Data Centric Publish/Subscribe)
DLRL (Data Local Reconstruction Layer)

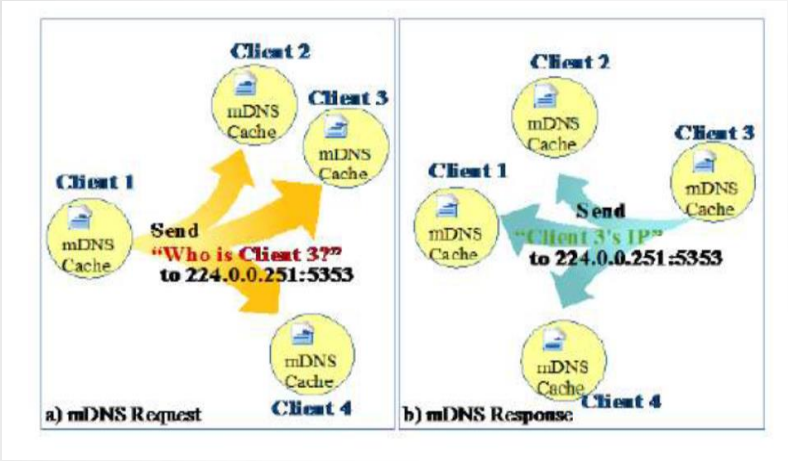
«DCPS مسئول تحویل دادن پیام به گیرنده است»

پنج موجودیت لایه DLRL
1) Publisher
2) Data Writer
3) Subscriber
4) Data Reader
5) Topic

پروتکل های مسیریابی اینترنت اشیاء (ادامه)

پروتکل های کشف سرویس:

- پروتکل MDNS



MDNS سرویسی است که می تواند وظیفه ی DNS را انجام دهد.

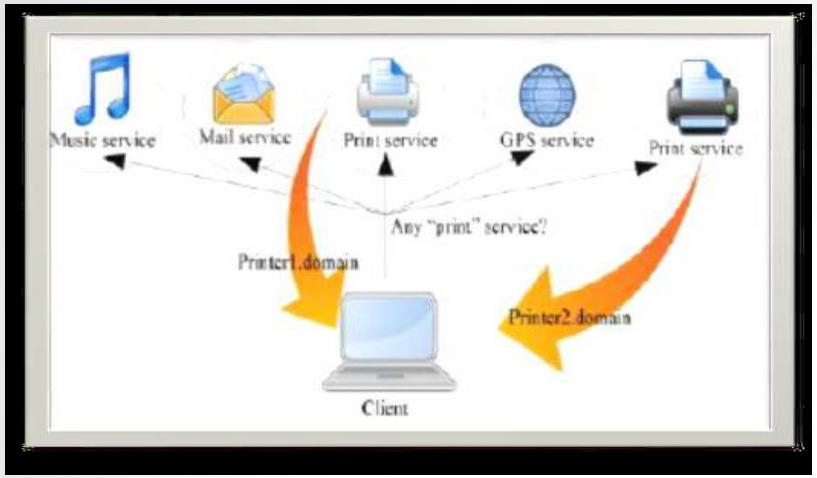
مناسب بودن MDNS برای اینترنت اشیاء به دلایل زیر:

- ✓ نیاز به هیچ گونه پیکربندی دستی و مدیریت اضافی برای مدیریت کردن وسایل ندارد.
- ✓ قابلیت اجرا شدن بدون هیچ گونه زیر ساختی را دارد.
- ✓ در صورت بروز خطا در زیر ساخت قابلیت اجرا و ادامه دادن دارد.

پروتکل های مسیریابی اینترنت اشیاء (ادامه)

- پروتکل DNS-SD

(Domain Name Service - Service Discovery)

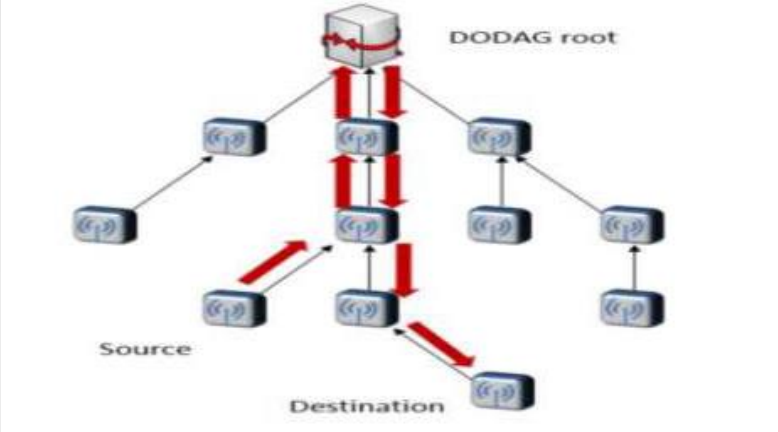


با استفاده از این پروتکل سرویس گیرنده می تواند یک مجموعه از سرویس های مورد نظر خودش را در یک شبکه با بکارگیری پیام استاندارد DNS کشف کند.

برای پردازش کشف سرویس دو گام اصلی وجود دارد:
۱. پیدا کردن نام سرویس درخواستی مثل Printer.
۲. جفت کردن نام های درخواستی یا میزبان با آدرس های IP با استفاده از MDNS

پروتکل های مسیریابی اینترنت اشیاء (ادامه)

پروتکل های زیرساخت:



- **پروتکل RPL**

(Routing Protocol for Low-Power)

یک گراف جهت دار غیر چرخشی مقصد گرا (DODAG)
Destination Oriented Directed Acyclic Graph

پروتکل مسیریابی اینترنتی بهینه شده برای شبکه های حسگر است که حداقل نیازمندی های مسیریابی را از طریق ساختن یک توپولوژی مستحکم بر روی مسیرهای بی ثبات پشتیبانی می کند.

پروتکل های مسیریابی اینترنت اشیاء (ادامه)

- **پروتکل 6LowPAN**

(IPV6 Over Low Power Wireless Personal Area Network)

این پروتکل یک شبکه بی سیم شخصی کم قدرت مبتنی بر IPV6 است.
این پروتکل شبکه، از مکانیسم های فشرده سازی سرآیند استفاده می کند و مستقل از باند فرکانسی و لایه فیزیکی است.

- **پروتکل IEEE 802.15.4**

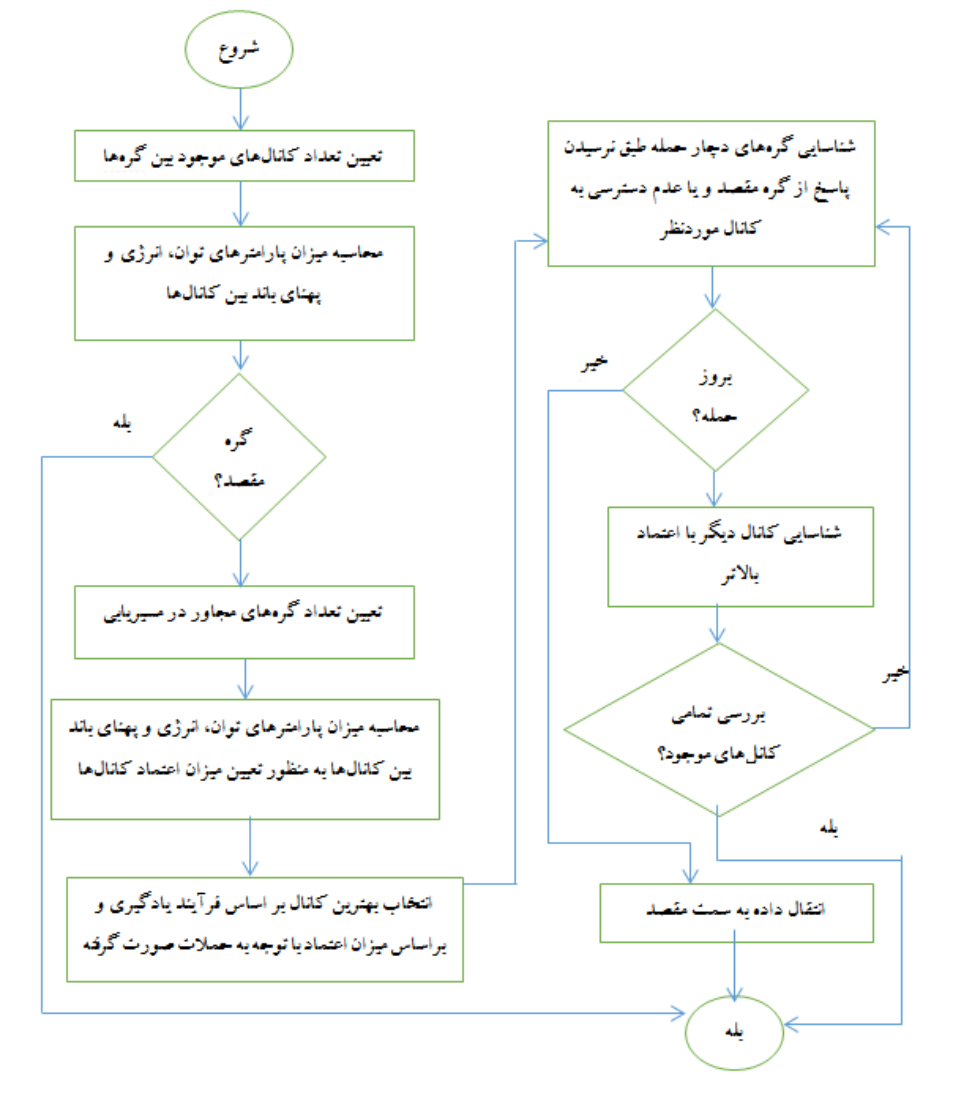
هدف از ایجاد این پروتکل اضافه کردن یک زیرلایه کنترل دسترسی رسانه و یک لایه فیزیکی به شبکه های بی سیم با نرخ کم

مقدمه
کلیات پژوهش
مروری بر ادبیات
روش پیشنهادی
ارزیابی نتایج
نتیجه گیری
پیشنهادات

مروری بر کارهای پیشین

نویسندگان مقاله	عنوان مقاله	نتایج بدست آمده
یوکینگ ژانگ و همکاران	تجزیه و تحلیل مسائل امنیتی و حفظ حریم شخصی در اینترنت اشیاء	یافتن چالش ها و تهدیداتی که این حوزه از تکنولوژی را مورد هدف قرار می دهد.
سامی یول مونیر	بررسی سیستم کنترل دسترسی برای اینترنت اشیاء	طراحی معماری متفاوتی از اینترنت اشیاء و ارائه راه حل هایی مبنی بر اطمینان از سیستم با معرفی CLOUD و دسترسی به ویژگی هایی که این امنیت را تضمین کنند.
سوگانگ و همکاران	بررسی راه حل های ابتکاری و جنبه های امنیتی معماری مختلف اینترنت اشیاء و مضرات آن ها،	شناسایی چالش های امنیتی و حریم خصوصی برای سیستم های اینترنت اشیاء و پیشنهاد یک راه حل امنیتی برای اینترنت اشیاء و همچنین معماری برای اینترنت آینده
میرزا عبدور رزاق و همکاران	بررسی مسائل و حملات امنیتی در اینترنت اشیاء و اقدامات متقابل با آن ها و تحلیل حملات مختلف و رفتارهای آن ها	ارائه یک مکانیزم امنیتی برای حفاظت از تهدیدها و راهکارهایی برای مقابله با این حملات
وانا و همکاران	تشریح مجموعه ای از پروتکل های ارتباطی اینترنت اشیاء و معماری هر یک از لایه های مختلف	ارائه چارچوبی برای ردیابی حملات DoS در اینترنت
کنزابیورو و همکاران	بررسی مسائل امنیتی سیستم اینترنت اشیاء و راه حل و روش های آن	تصویب و گسترش اینترنت اشیاء و راه حل های این نوع مسائل و همچنین از فناوری این رویکردها در جهت خدمت رسانی که توسط علوم و فناوری و نوآوری (CTIS) و توسعه نوآوری استراتژیک (SIP) و آژانس سرمایه گذاری سایبری- امنیت برای زیر ساخت بحرانی (NEDO) و شرکت های دیگر از جمله شرکت هیتاچی در بهبود بخشیدن در انجام پژوهش ها، اعتبار سنجی و در تولید محصولات جدید استفاده کردند.

فلوچارت روند کلی روش پیشنهادی



SecTrust

یک چارچوب توزیع شده اعتماد محور برای مسیریابی مطمئن درIOT

تعیین حملات مسیر

تعیین رفتار اعتماد بخش یک گره

درستی گره در SecTrust از طریق ارزشیابی گره های مجاورش مشخص می شود.

از طریق تبادل بسته موفق زمان محور بین گره های مجاور و تأیید بسته مثبت همراه با مشاهده متوالی بین گره های مجاور مرتبط

پروتکل RPL

RPL (**R**outing **P**rotocol for **L**ow-Power and **L**ossy Networks)

- پروتکل مسیریابی برای شبکه های کم قدرت و پر اتلاف
- بر مبنای IPV6
- از طریق کشف اولیه مسیر زمانی که اجرایی می شود، عمل می کند.

شروع از طریق ایجاد یک مکان درخت مانند به نام DAG
هر گره سنسور یک گره والد انتخاب می کند (مدخل بسته برای آن گره)
اگر خارج شود، فقط بسته را به گره دریافت کننده ارسال می کند.
اگر یک گره ورودی مقصد برای یک بسته در جدولش نداشته باشد، گره بسته را به والدش ارسال می کند.
این فرآیند تا زمانی ادامه می یابد که بسته به دریافت کننده گره برسد.

محاسبه مسیریابی SecTrust توسط پروتکل RPL

- مسیریابی اعتماد:

فرآیند محاسبه مسیریابی اعتماد

فرآیند رتبه بندی اعتماد

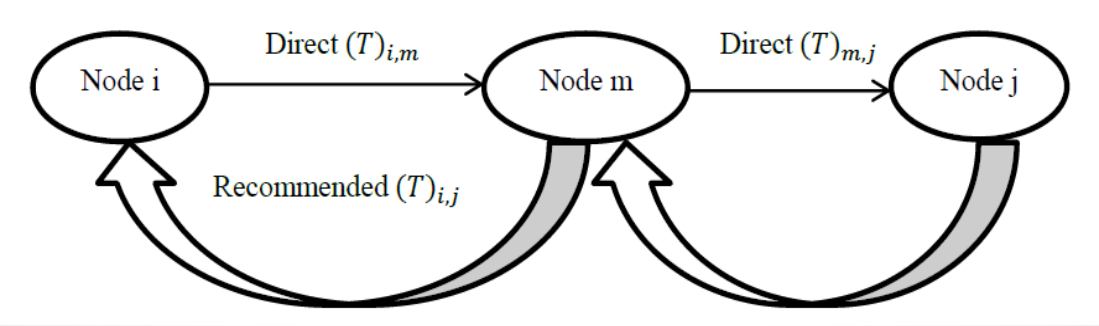
- فرآیند محاسبه اعتماد:

ارزیابی گره ی اطمینان شونده توسط یک گره اطمینان کننده

محاسبه اعتماد اعتبار، قابلیت وابستگی و صلاحیت برای عملکرد فعالیت های ارسال شده توسط گره ها از تعاملات مستقیم یا غیر مستقیم با گره های دیگر را نشان می دهد.

روش پیشنهادی

- دو نوع اعتماد در روش پیشنهادی: اعتماد **مستقیم** و اعتماد **پیشنهادی**



- رابطه ارزش اعتماد پیشنهادی در روش پیشنهادی:

$$RT(N_t, N_j) = \alpha\beta\, DT(N_t,N_m) * DT(T_{m,j})$$ رابطه ۳-۱

- سیستم رتبه بندی اعتماد برای رتبه بندی گره ها:

$v = [v_1, v_2, v_3, v_4, v_5]$

شاخص‌های توان، پهنای باند و انرژی

پیاده سازی

۱	تعداد گره حمله کننده در شبکه
۵	تعداد کانال ارتباطی بین هر ۲ دستگاه
مصرف انرژی، توان، پهنای باند	پارامترهای هر کانال

محاسبه میزان اعتماد هر کانال ارتباطی بین دو دستگاه:

پارامتر مصرف انرژی بر حسب ژول، توان بر حسب وات و پهنای باند بر حسب مگابیت است.

حذف این واحد ها = تقسیم مقدار هر پارامتر بر مقدار حداکثر که در بازه تعریف شده است.

سپس مجموع این ۳ پارامتر میزان اعتماد هر لینک در نظر گرفته می شود.

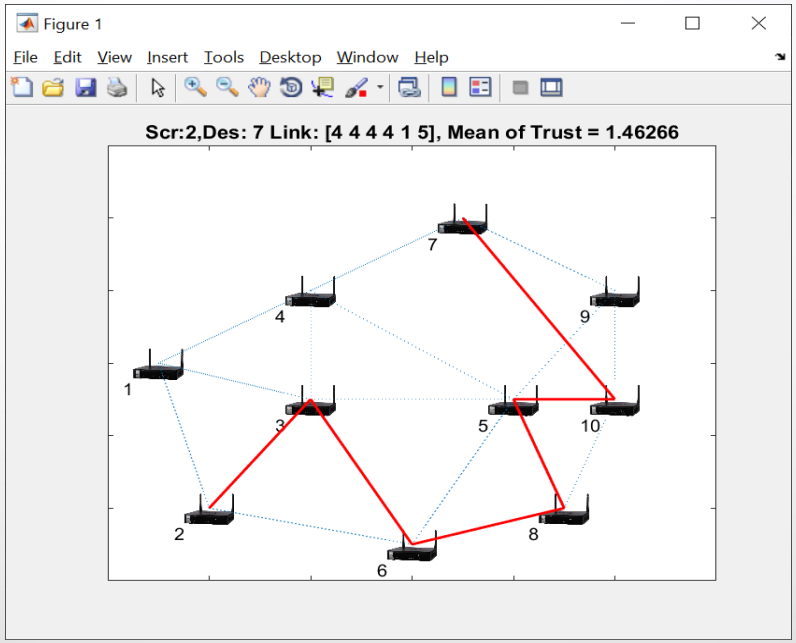
انواع ارسال حمله توسط دستگاه حمله کننده:

- ارسال حمله به دستگاه دیگر
- ارسال حمله به کانال دستگاه دیگر

پیاده سازی (ادامه)

مثالی از مسیریابی RPL ارتقا یافته بین دو دستگاه شماره ۲ و ۷ در روش پیشنهادی:

تعداد کل دستگاه ها	۱۰
گره حمله کننده در شبکه	گره شماره ۹
پهنای باند	[1 10] (Mbps)
توان	[1 100] (Watt)
مصرف انرژی	[0.1 0.9] (Jol)



مقدمه
کلیات پژوهش
مروری بر ادبیات
روش پیشنهادی
ارزیابی نتایج
نتیجه گیری
پیشنهادات

پیاده سازی (ادامه)

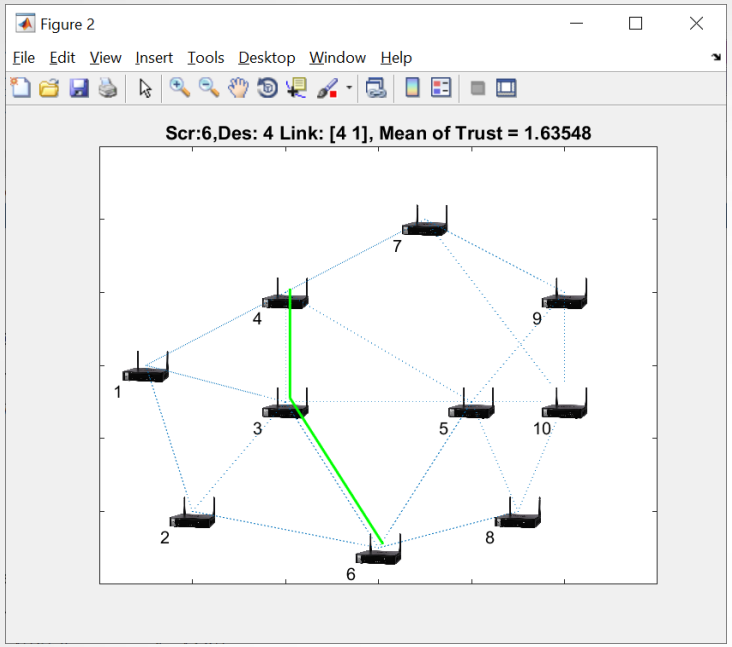
Sum Power	Sum Bandwidth	Sum Energy	Sum Trust
88/307	26	8775/2	776/8

Mean Power	Mean Bandwidth	Mean Energy	Mean Trust
313/51	3333/4	47958/0	4627/1

مقدمه
کلیات پژوهش
مروری بر ادبیات
روش پیشنهادی
ارزیابی نتایج
نتیجه گیری
پیشنهادات

پیاده سازی (ادامه)

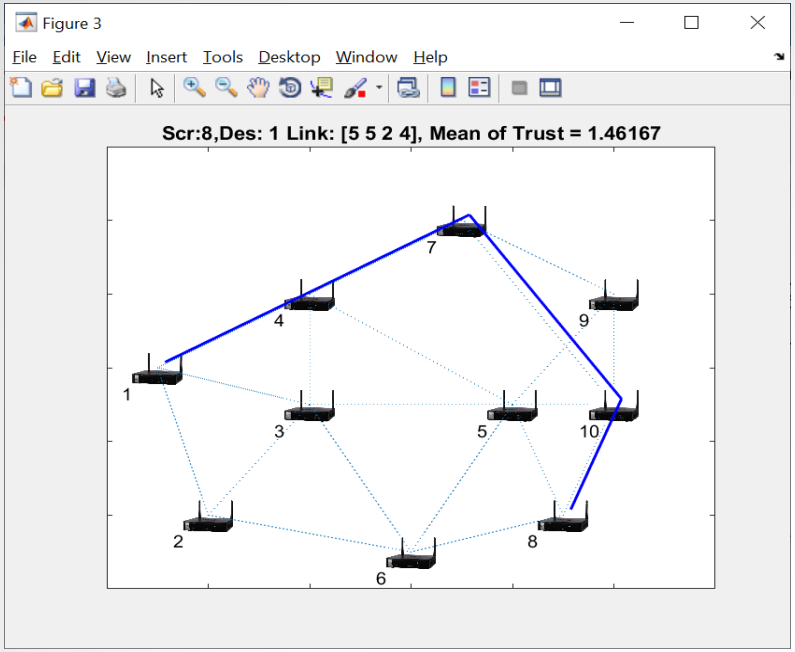
مسیریابی RPL ارتقا یافته بین دو دستگاه شماره ۶ و ۴ در روش پیشنهادی:



Sum Power	Sum Bandwidth	Sum Energy	Sum Trust
79/118	7	68402/0	271/3

Mean Power	Mean Bandwidth	Mean Energy	Mean Trust
395/59	5/3	34201/0	6355/1

پیاده سازی (ادامه)

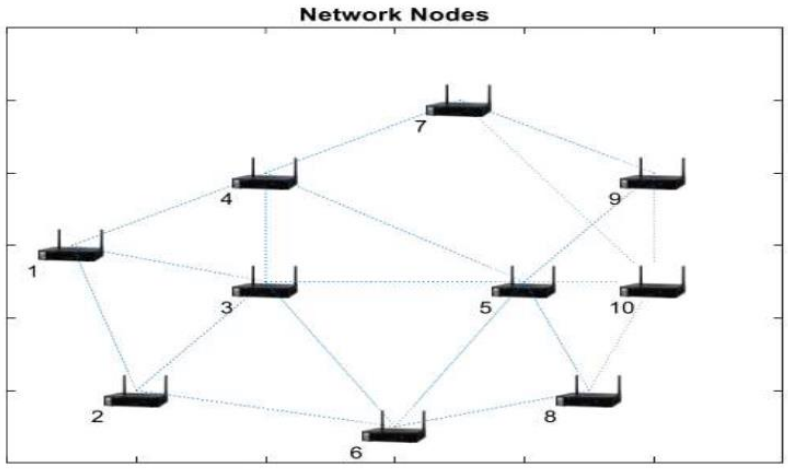


مسیریابی RPL ارتقا یافته بین دو دستگاه شماره ۸ و ۱ در روش پیشنهادی:

Sum Power	Sum Bandwidth	Sum Energy	Sum Trust
2/221	12	542/2	8467/5

Mean Power	Mean Bandwidth	Mean Energy	Mean Trust
299/55	3	63549/0	4617/1

سناریو شبیه سازی



شکل (۴-۱) طراحی شبکه RPL دارای ۱۰ گره

۰/۸	حد آستانه
۰/۳	آلفا
۰/۳	بتا

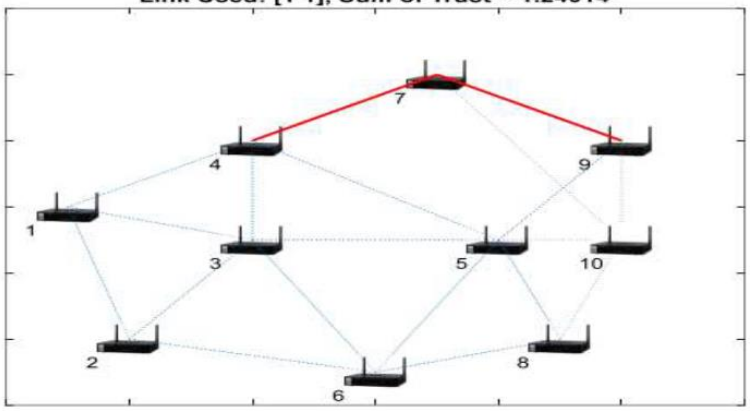
سناریو شبیه سازی (ادامه)

محاسبه رتبه بندی در SecTrust-RPL

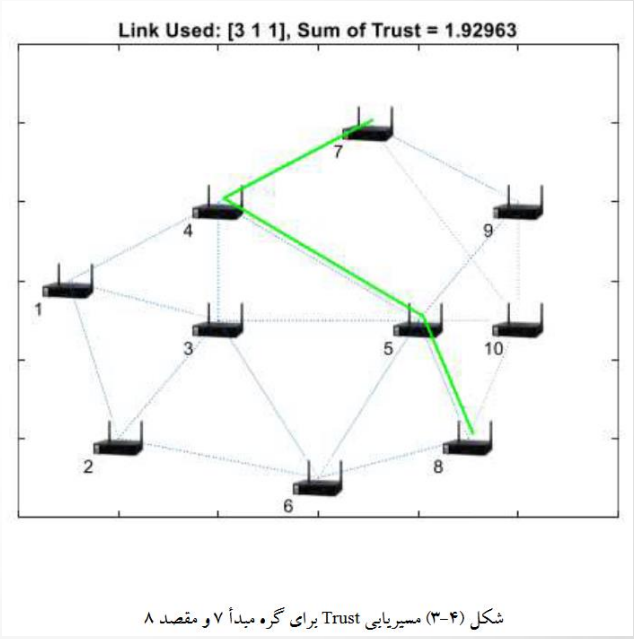
جدول (۴-۱) محاسبه Trust از اجرای مرحله اول

گره مبدأ	گره مقصد	گره کانال	مجموع Trust
۴	۹	۱	۱/۲۴۰۱۴
۷	۸	۱و ۳	۱/۹۲۹۶۳
۳	۱۰	۳	۱/۰۹۴۵۲

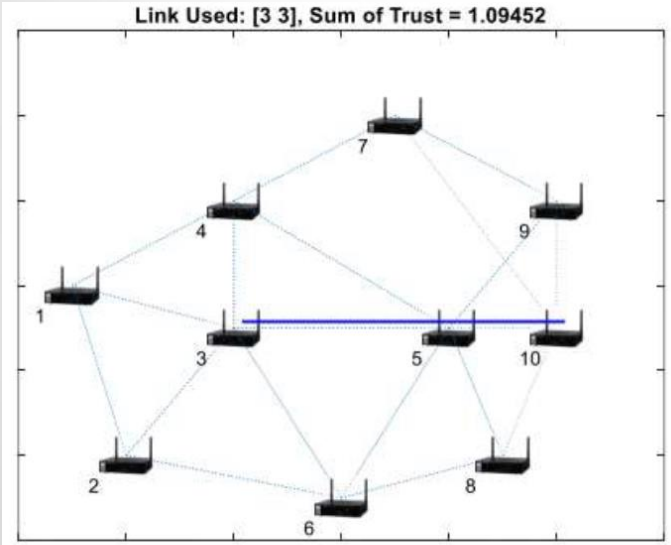
سناریو شبیه سازی (ادامه)



شکل (۴-۲) مسیریابی Trust برای گره مبدأ ۴ و مقصد ۹

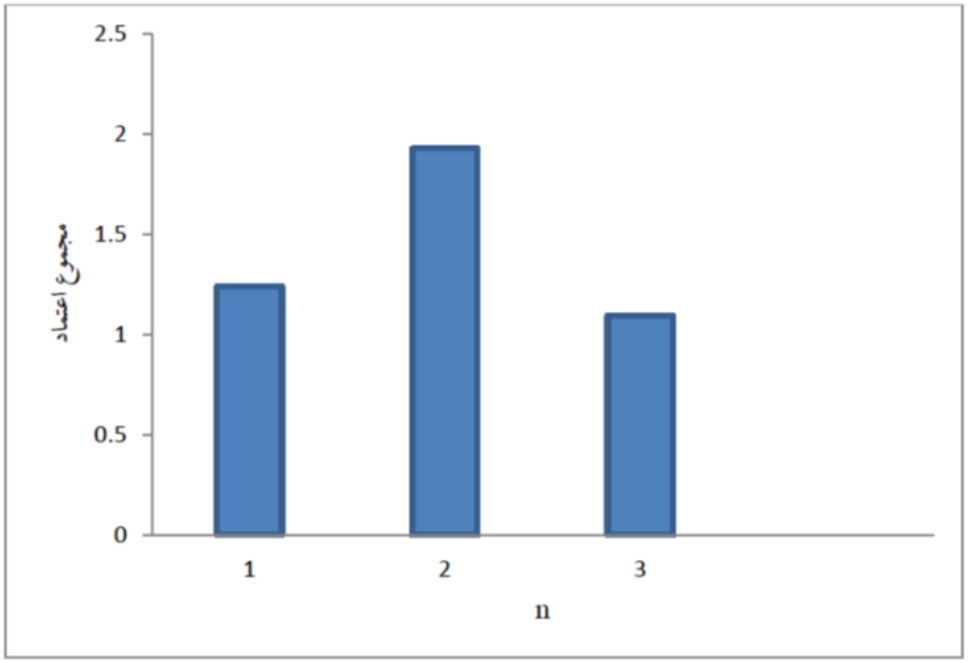


شکل (۴-۳) مسیریابی Trust برای گره مبدأ ۷ و مقصد ۸



شکل (۴-۴) مسیریابی Trust برای گره مبدأ ۳ و مقصد ۱۰

سناریو شبیه سازی (ادامه)



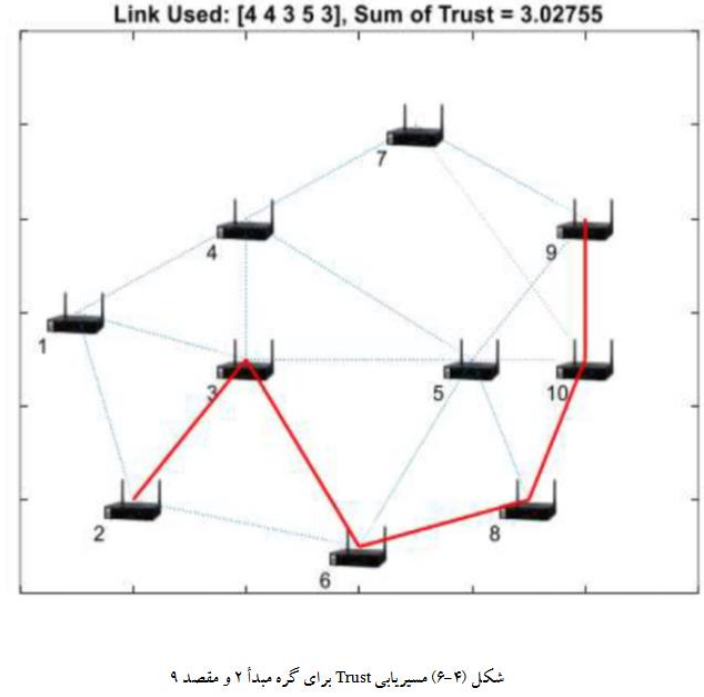
شکل (۴-۵) میزان مجموع اعتماد در اجرای مرحله اول

سناریو شبیه سازی (ادامه)

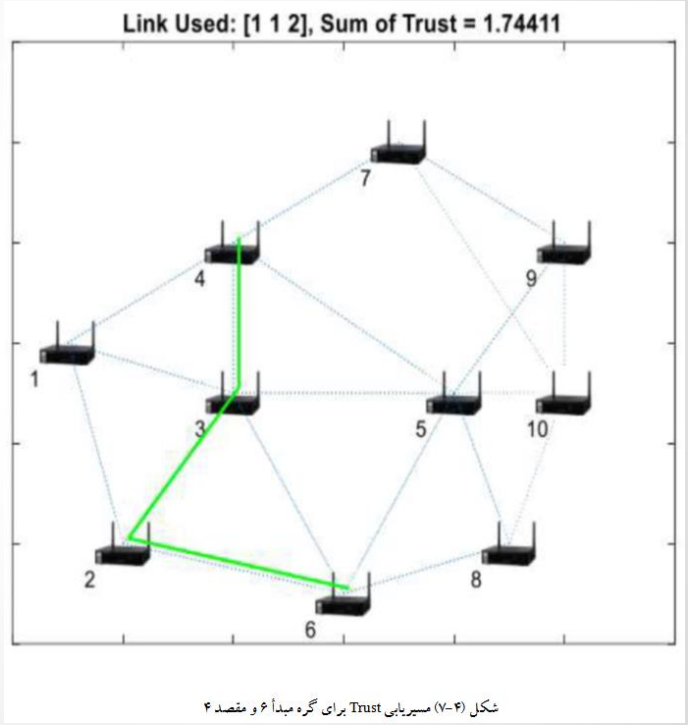
جدول (۴-۲) محاسبه Trust از اجرای مرحله دوم

گره مبدأ	گره مقصد	گره کانال	مجموع Trust
۲	۹	۳،۵،۳،۴،۴	۳/۰۲۷۵۵
۶	۴	۱،۱،۲	۱/۷۴۴۱۱
۸	۱	۱،۴،۴	۱/۷۴۹۴۹

سناریو شبیه سازی (ادامه)

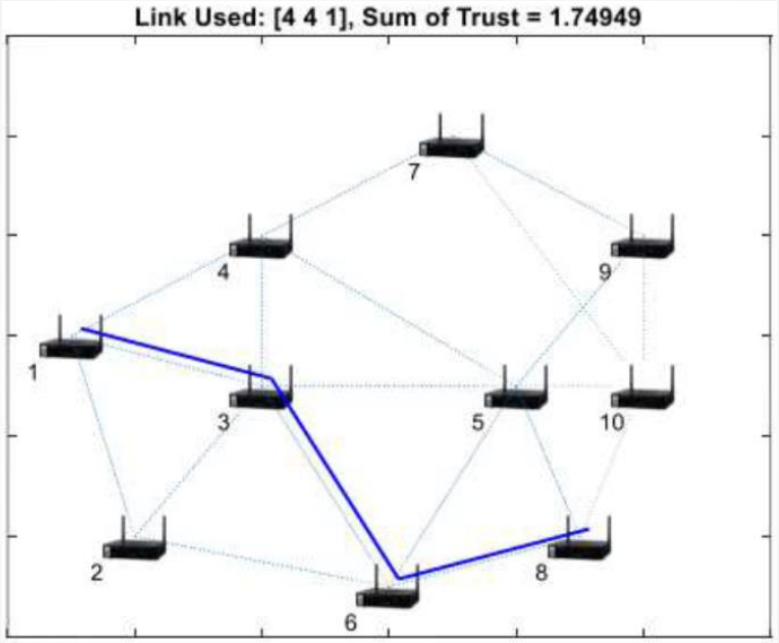


شکل (۴-۶) مسیریابی Trust برای گره مبدأ ۲ و مقصد ۹



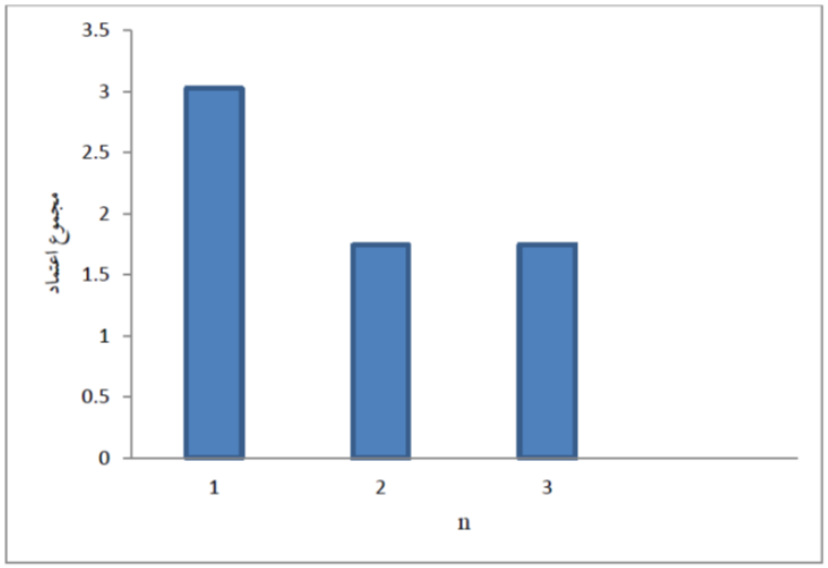
شکل (۴-۷) مسیریابی Trust برای گره مبدأ ۶ و مقصد ۴

سناریو شبیه سازی (ادامه)



شکل (۴-۸) مسیریابی Trust برای گره مبدأ ۸ و مقصد ۱

سناریو شبیه سازی (ادامه)

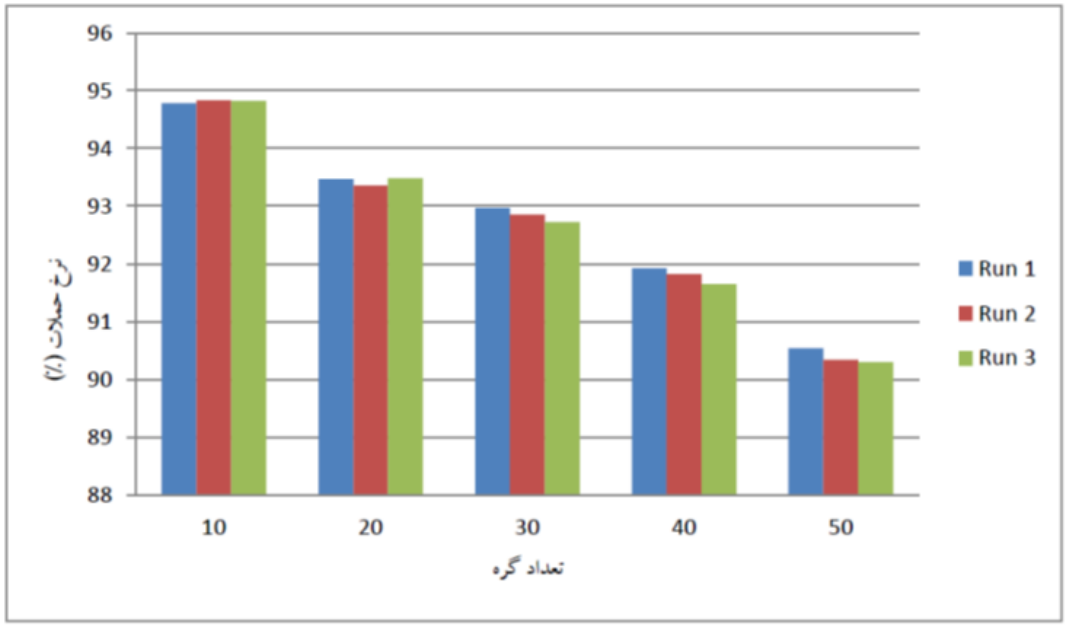


شکل (۴-۹) میزان مجموع اعتماد در اجرای مرحله دوم

ارزیابی نتایج

مقایسه درصد نرخ حملات	اجرای اول	اجرای دوم	اجرای سوم
n=۱۰	٪۹۴/۷۸۳	٪۹۴/۸۳۱	٪۹۴/۸۲۲
n=۲۰	٪۹۳/۴۷۲	٪۹۳/۳۵۸	٪۹۳/۴۸۲
n=۳۰	٪۹۲/۹۷۳	٪۹۲/۸۵۴	٪۹۲/۷۲۶
n=۴۰	٪۹۱/۹۲۳	٪۹۱/۸۲۶	٪۹۱/۶۵۲
n=۵۰	٪۹۰/۵۴۴	٪۹۰/۳۴۳	٪۹۰/۳۰۲

ارزیابی نتایج (ادامه)



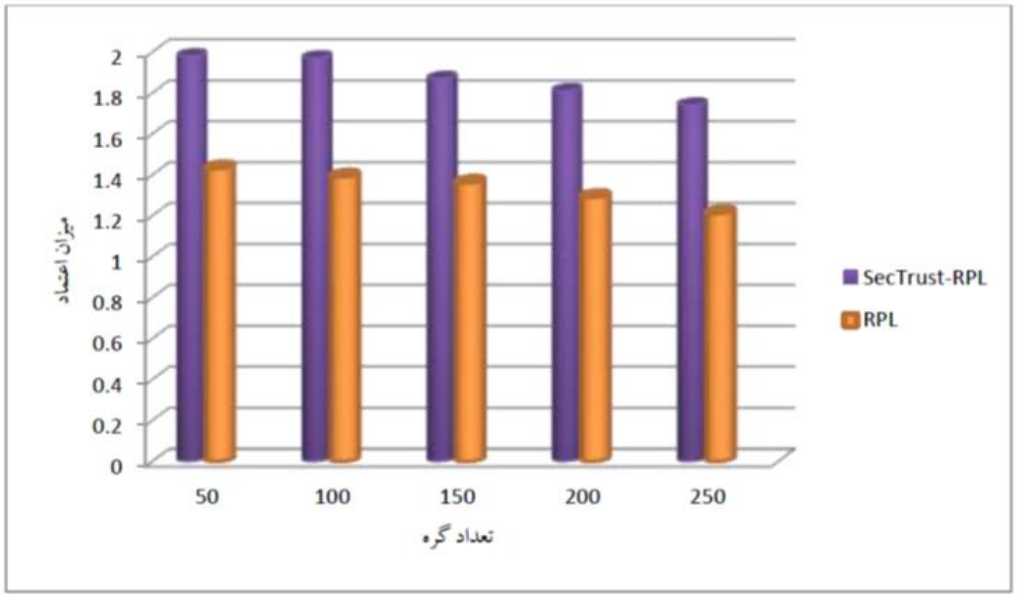
شکل (۴-۱۰) نرخ حملات شناخته شده به ازای تعداد گره های مختلف

ارزیابی نتایج (ادامه)

جدول (۴-۴) مقایسه میزان اعتماد بین secTrust-RPL و RPL

تعداد گره	SecTrust-RPL	RPL
n=۵۰	۱/۹۸	۱/۴۳
n=۱۰۰	۱/۹۷	۱/۳۹
n=۱۵۰	۱/۸۷	۱/۳۶
n=۲۰۰	۱/۸۱	۱/۲۹
n=۲۵۰	۱/۷۴	۱/۲۱

ارزیابی نتایج (ادامه)



شکل (۴-۱۱) مقایسه میزان اعتماد بین SecTrust-RPL و RPL

نتیجه گیری

- ارائه یک روش مسیریابی مبتنی بر اعتماد جهت جداسازی گره های حمله و تشخیص نوع حمله
- پروتکل SecTrust-RPL توانست با محاسبه روش های اعتمادی خود، گره های حملـه کننـده را جدا سازد.
- این پروتکل نوع حملات را نیز تشخیص می دهد.
- روش پیشنهادی دفاع خوبی در شبکه در برابر نفوذگران انجام داده است.

تحقیقات آتی

- بررسی سیستم رمزگذاری متقارن و نامتقارن با هدف انطباق آن با مشخصات محیط اینترنت اشیاء
- استفاده از رمزنگاری های بلاکی در پرداختن به مباحث محرمانه بودن برای گره های حسگر اینترنت اشیاء برای دفاع در برابر حملات
- تشخیص بهینه مبتنی بر اعتماد دستگاه های به خطر افتاده در شبکه های WSN و IOT
- بکارگیری سیستم های مبتنی بر اعتماد در مدیریت خدمات آنلاین

سپاس از توجه شما