سومین کنفرانس بین المللی نوآوری و تحقیق در علوم مهندسی
گرجستان - تفلیس (۳۰ تیرماه ۱۳۹۸) آکادمی بین المللی علوم گرجستان
ICIRES 21 July 2019
www.icires.ir
info@icires.ir
CIU
NEW VISION UNIVERSITY NVU
Eco energy
GIAS

# بررسی مسیریابی امن در شبکه اینترنت اشیا

اکرم گل محمدی[۱] ، سید دانیال علیزاده جواهری[۲] و رضا قائمی [۳]
[۱] دانشجوی دکتری ،گروه کامپیوتر،واحد نیشابور،دانشگاه آزاد اسلامی ،نیشابور،ایران
golmohammadi.akram@gmail.com
[۲] دانشجوی دکتری ،گروه کامپیوتر،واحد نیشابور،دانشگاه آزاد اسلامی ،نیشابور،ایران
itcjavaherii@gmail.com
[۳] استادیارگروه کامپیوتر،واحد قوچان،دانشگاه آزاد اسلامی ،قوچان،ایران
r.ghaemi@iauq.ac.ir

**چکیده- اینترنت اشیاء بر استقرار شبکه‌های پر اتلاف و کم توان تاکید می‌کند تا از روابط بین اشیا و اتصال آنان با اینترنت حمایت و پشتیبانی کند. شناسایی و تجزیه و تحلیل حملات امنیتی امری ضروری می‌باشد. حملات علیه توپولوژی شبکه باعث می‌شود که تنظیمات شبکه بهم بریزد و باعث تنزل کارایی شبکه و کناره‌گیری گره‌ها شود. در نهایت حملات علیه ترافیک شبکه بیشتر می‌شود. گره مخرب این اجازه را می‌یابد که به بخش عمده ای از ترافیک دسترسی پیدا کند و آن را تجزیه و تحلیل نماید و اهداف حمله به مسیریابی را عملی کند. شبکه‌های اینترنت اشیاء می‌توانند برای کاربردهای بسیاری در حوزه‌های مختلف صنعتی از جمله نظارت بر زیرساخت، خدمات شهری، کاربردهای نظارتی و امنیتی و غیره مورد استفاده قرار بگیرند. با این حال، جمع‌آوری مقادیر زیادی از داده‌ها از چنین شبکه‌هایی اغلب باعث تراکم ترافیک در ناحیه شبکه مرکزی می‌شود و موجب به خطر افتادن امنیت داده‌ها می‌شود. روش‌های مسیریابی امن مشکلات امنیتی را تاحد زیادی برطرف می‌کنند. در این تحقیق، روش‌های مسیریابی امن و تشخیص نفوذ پیشنهاد می‌شود که می‌توانند حمله گره‌های مجاور را در پروتکل‌های مختلف شناسایی کنند و یک فرایند امن برای جلوگیری از تاثیر حملات به پروتکل‌ها ارائه دهند که باتوجه به اطلاعات مکان و قدرت سیگنال دریافتی شناسایی گره مخرب انجام می‌شود. همچنین الگوریتم‌های بررسی شده در این تحقیق سعی دارند با معیارهای اعتماد در میان گره‌های اینترنت اشیاء، حملات و لینک‌های مخرب و جعلی منتهی به گره‌های مخرب تا حد ممکن انتخاب نمی‌شود. به علاوه طول عمر شبکه افزایش می‌یابد و با سوء رفتار در شبکه مقابله می‌کنند. این موضوع برای جلوگیری از حملات مختلف استفاده می‌شود.**

**واژگان کلیدی:**اینترنت اشیا- گره جعلی- مسیریابی امن- اعتبار گره- پروتکل ***RPL***

## ۱- مقدمه

اینترنت اشیا[۱] شامل اتصال اشیاء ایستا یا پویا و دستگاه‌های مجهز به ارتباطات، سنسورها و ماژول‌های راه انداز از طریق اینترنت می‌باشد[1]. تبادل داده‌ها و مسیریابی با کیفیت سرویس[۲] و امنیت موضوع اصلی در اینترنت اشیا است. در شبکه‌های اینترنت اشیا اگر مسیریابی امن به درستی صورت نگیرد آنگاه این امر به حملات چندگانه منجر می‌شود که در آن یک گره مخرب می‌تواند محتویات بسته‌ها را دستکاری کند تا بر عملکرد شبکه تاثیر بگذارد. چنین حملاتی می‌تواند کنترل، پیاده‌سازی، جعل، اصلاح، پاسخ و ایجاد پیام‌های کنترل را به اختیار خود درآورد و به این ترتیب باتری‌های گره را تخلیه کند[2]. حملات برای پروتکل‌های مسیریابی بسیار خطرناک است زیرا حملات دیگر مانند سینکول، سیاه چاله، حلقه‌ها و غیره را انجام

[1] Internet fo thing

2Quality of service