عنوان مقاله:
سیستم تشخیص نفوذ کارآمد انرژی برای شبکه های سنسور بی سیم مبتنی بر ZigBee

محل انتشار:
هشتمین کنفرانس بین المللی راهکارهای نوین در مهندسی، علوم اطلاعات و فناوری در قرن پیش رو (سال: 1400)

تعداد صفحات اصل مقاله: 22

نویسنده:
عرفان شامحمدی حیدری - *کارشناسی ارشد مهندسی فناوری اطلاعات گرایش تجارت الکترونیک ، دانشگاه آزاد اسلامی واحد الکترونیک*

خلاصه مقاله:
امروزه ZigBee یکی از استاندارد های غالب برای شبکه های سنسور بی سیم و شبکه های اینترنت اشیا (IoT) می باشد. با اینکه استاندارد ZigBee دارای هزینه پایین در هر واحد، امنیت و انعطاف شبکه است، مکانیسم امنیتی موجود برای تامین امنیت و محافظت در مقابل حملات کرم چاله ها و حملات منع سرویس توزیع شده (DDoS) به شبکه هایی مثل WSN و IOT موثر نیست. آنها همچنین مصرف زیاد انرژی، پردازش و حافظه ذخیره سازی را نشان می دهند. در این مطالعه، سیستم تشخیص نفوذکارآمد انرژی (EE-IDS) و سیستم تشخیص نفوذ کارآمد انرژی با پیش بینی انرژی (EE-IDSEP) برای حفاظت از شبکه های سنسور بی سیم مبتنی بر ZigBee در حضور حملات کرم چاله و حملات منع سرویس توزیع شده (DDoS) پیشنهاد می شود EE-IDS توسعه می یابد و عملکرد آن با در نظر گرفتن سه پروتکل مسیریابی مختلف (STR)؛ (AODV) و (OSTR) برای بهبود امنیت در مقابل حمله کرم چاله و کاهش مصرف انرژی گره های سنسور در شبکه های سنسور بی سیم مبتنی بر ZigBee ارزیابی می گردد. EE-IDS و EE-IDSEP پیشنهادی از طریق شبیه سازی های گسترده با استفاده از NS۲ ارزیابی شدند و سپس با سیستم (EE-TSW) و سیستم (EE-TS) برای تشخیص حمله DDoS مقایسه شدند. از نتایج شبیه سازی این طور استنباط می شود که IDS پیشنهادی یعنی EE-IDS-AODV, EE-IDS-STR و EE-IDS-OSTR برای تشخیص حمله کرم چاله عملکرد بهتری نسبت به EE-TSW موجود دارد و سیستم پیشنهادی EE-IDSEP برای تشخیص حمله DDoS نسبت به EE-TS سیستم موجود از لحاظ معیارهای عملکرد مانند (PDR)، متوسط تاخیر End-to-End مصرف انرژی، سرعت تشخیص، زمان تشخیص متوسط و (FPR) عملکرد بهتری را نشان می دهد.

کلمات کلیدی:
سیستم تشخیص نفوذ کارامد انرژی، پروتکل STR، حملات DDoS، حمله کرم چاله