ملخص أطروحة الدكتوراه بعنوان

تحسين أداء شبكات الحسّاسات اللاسلكية اعتماداً على الشبكات المعرّفة برمجياً

اسم الطالب

المهندس أحمد لؤي الابراهيم

المشرف

الأستاذ الدكتور المهندس عبد الرزاق البدوية

القسم والاختصاص

قسم هندسة الإلكترونيات والاتصالات

هندسة الاتصالات المتقدمة

الملخـــــص

أصبحت شبكات الحسّاسات اللاسلكية WSNs شائعة بشكل متزايد لمجموعة متنوعة من التطبيقات مثل المراقبة البيئية والرعاية الصحية وتطبيقات إنترنت الأشياء IoT، كما أنّها تواجه عدداً من التحدّيات والتهديدات بما في ذلك هجمات حجب الخدمة DoS. ومن أهم الحلول التي انبثقت لمعالجة التحدّيات المتأصّلة لها هي الشبكات المعرّفة برمجيّاً SDNs، التي فتحت الأفق لتطوير شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSNs التي تتيح تنفيذ سياسات وإجراءات معتمدة على تعلّم الآلة ML في كشف هذه الهجمات والتخفيف من أثرها مما ينعكس على أداء شبكات WSNs.

تبحث هذه الأطروحة استخدام نموذج شبكات SDNs لتحسين أداء شبكات WSNs ضد هجمات DoS وهجمات DDoS، باقتراح خوارزميّة لكشف ومنع هذه الهجمات بالاعتماد على خوارزميات تعلّم الآلة في شبكات SDWSNs، ودراسة أداء هذه الخوارزميّة في تحسين أداء الشبكة.

تعتمد هذه الأطروحة على استخراج سِمات مجموعة المعطيات لنموذج تعلّم الآلة التي يمكن استخدامها في كشف هذه الهجمات، وتصميم خوارزميّة لكشف ومنع هجمات DoS وهجمات DDoS بالاعتماد على خوارزميات تعلّم الآلة المعتمدة على التصنيف، ومضاهاة أداء الخوارزميّة المقترحة باستخدام البرنامج Mininet-Wifi ومتحّكم من النوع Ryu-Manager لشبكة SDWSN.

أظهرت نتائج دراسة متوسط استهلاك الطاقة ونسبة تسليم الرزم ومتوسط التأخير من نهاية إلى نهاية أنّه يمكن للخوارزميّة المقترحة أن تحسّن أداء هذه الشبكات ذات الموارد المحدودة، كما أنّها تحقّق معدّل كشف مرتفع للهجمات بلغت 99.86%.

تشير النتائج إلى أنّ الخوارزميّة المقترحة يمكن أن تكون حلاً فعالاً لتحسين أداء شبكات WSNs ضد هجمات DoS وهجمات DDoS في الزمن الحقيقي.

PhD dissertation summary

Improving the Performance of Wireless Sensor Networks Based on Software-Defined Networks

Student Name

Eng. Ahmad Al Ebrahim

Supervisor

Prof. Dr. Abdelrazak Badawieh

Department

Department of Electronics and Communications Engineering

Advanced Communication Engineering

Abstract

Wireless Sensor Networks (WSNs) become increasingly popular for a variety of applications such as environmental monitoring, healthcare, and Internet of Things (IoT) applications. However, they face a number of challenges and security threats, including Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. One of the most promising solutions to address the inherent challenges is Software-Defined Networks (SDN), which opened up the develop of Software-Defined Wireless Sensor Networks (SDWSNs), which enables the implementation of Machine Learning (ML) based policies and procedures to detect and mitigate DoS and DDoS attacks, and improve WSNs performance.

This thesis examines the use of the SDN network model to improve the performance of WSNs against DoS and DDoS attacks, by proposes an algorithm to detect and prevent these attacks based on machine learning algorithms in SDWSN, and studies the effect of this algorithm in improve network performance.

This thesis is based on extract the dataset features of the ML model that can be used to detect these attacks, then design an algorithm to detect and prevent DoS and DDoS attacks based on classification-based ML algorithms, and emulate the performance of the proposed algorithm using the Mininet-Wifi program and a Ryu-Manager controller for SDWSN.

The results of the study of average energy consumption, Packet Delivery Ratio (PDR), and average End-to-End delay showed that the proposed algorithm can improve the performance of these limited resources networks, while also achieves a high attack detection rate of 99.86%.

The results indicate that the proposed algorithm can be an effective solution to improve the performance of WSNs against real-time DoS and DDoS attacks.