جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الإلكترونيات والاتصالات

تحسين أداء شبكات الحسّاسات اللاسلكية اعتماداً على الشبكات المعرّفة برمجياً

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

المهندس أحمد لؤي الابراهيم
الأستاذ الدكتور المهندس عبد الرزاق البدوية

الملخص

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. وتعتمد هذه الأطروحة على استخراج سمات 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 ومتحكّم 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%.

القسم النظري

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 الخطيرة بسبب قيود الموارد لأجهزة التحسّس مثل المعالجة والذاكرة والطاقة وقدرات الاتصال، كما تواجه التهديدات بما في ذلك هجمات حجب الخدمة DoS وحجب الخدمة الموزع DDoS.

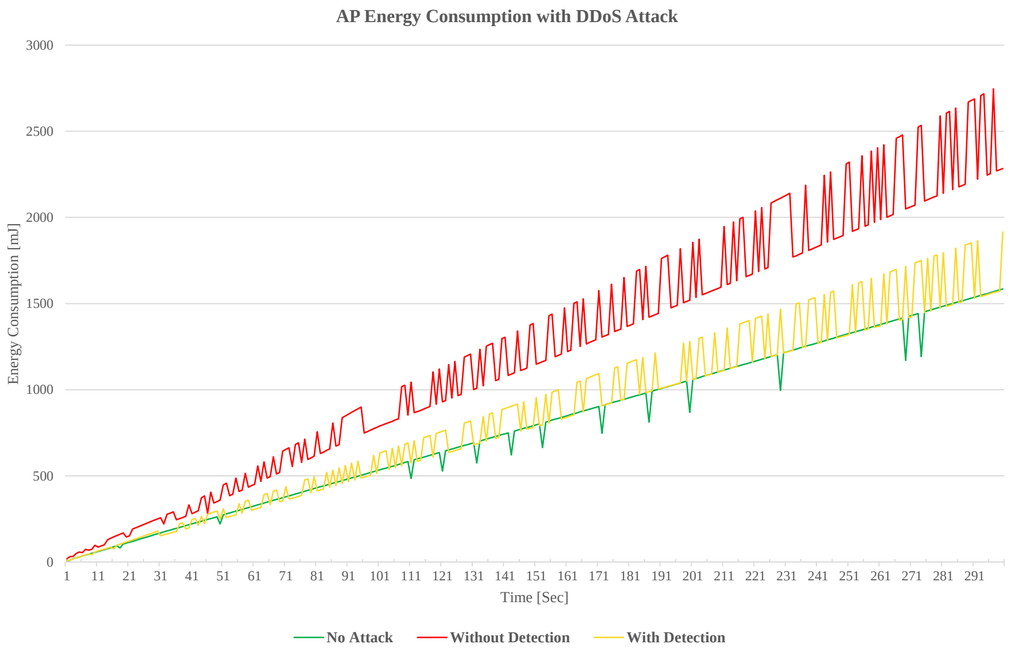
من أهم الحلول التي انبثقت لمعالجة التحدّيات المتأصّلة لها هي الشبكات المعرّفة برمجيّاً SDNs، التي تعمل على فصل مستوي التحكّم في الشبكة عن مستوي البيانات. والتي فتحت الأفق لتطوير شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSNs التي تتيح تبسيط تشغيل عقد التحسّس وتنفيذ سياسات وإجراءات معتمدة على تعلّم الآلة ML في كشف هذه الهجمات والتخفيف من أثرها مما ينعكس على أداء شبكات WSNs.

القسم العملي

جرى دراسة أثر هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS في شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSNs بناءً على مقاييس أداء الشبكة، ثم استخراج سمات مجموعة المعطيات لنموذج تعلّم الآلة التي يمكن استخدامهَا في كشف هجمات حجب الخدمة في هذه الشبكات عبر توليد ثلاث مجموعات معطيات وتطبيق خوارزميات تعلّم الآلة المعتمدة على التصنيف على هذه المجموعات ودراسة مقاييس خصائص الأداء لخوارزميات تعلّم الآلة للتحقق من كفاية السمات التي تحتويها، ثمّ اقتراح خوارزميّة لكشف ومنع هجمات حجبَ الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS المعتمدة على خوارزميات تعلّم الآلة في شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSNs في الزمن الحقيقي، ودراسة أداء هذه الخوارزميّة المقترحة في تحسين أداء الشبكة ومقارنة النتائج مع نتائج بعض الدراسات السابقة.

النتائج والمناقشة

قدّمت الخوارزميّة المقترحة تحسّناً في مقدار استهلاك الطاقة لنقاط الوصول ومتوسط استهلاك الطاقة لعقد التحسّس في شبكة WSN، وأصبحت مستويات استهلاك الطاقة أقرب إلى حالة العمل الطبيعية دون وجود الهجمات، مما يطيل عمر تشغيل الشبكة ويحسّن أداءها، كما قدّمت تحسناً كبيراً في نسبة تسليم الرزم PDR وفي متوسط زمن وصول الرزم من العقدة المصدر إلى نقطة الوصول أو المتحكّم، مما ينعكس إيجاباً على تحسين إدارة موارد الشبكة وتحسين أدائها بما يخدم استخدامها في تطبيقات إنترنت الأشياء IoT المختلفة. كما أنّ الخوارزميّة المقترحة قادرة على التنبؤ وإيقاف أي هجوم حجب الخدمة DoS أو هجوم حجب الخدمة الموزّع DDoS في الزمن الحقيقي Real Time حيث وصلت دقّة الكشف DR إلى 99.86% ومعدّل الخطأ السالب FNR إلى 0.14%، وذلك وفقاً لمقاييس خصائص الأداء لخوارزميات تعلّم الآلة.



المراجع

- Elsadig, M. A. (2023). Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach. *IEEE Access, 11*, 83537 –83552.
- Gebremariam, G. G., Indu, S., & Panda, J. (2023). Localization and Detection of Multiple Attacks in Wireless Sensor Networks Using Artificial Neural Network. *Wireless Communications and Mobile Computing*, *2023*, 2744706, 1-29.
- Liu, Y., Sun, D., Zhang, R., & Li, W. (2023). A Method for Detecting LDoS Attacks in SDWSN Based on Compressed Hilbert–Huang Transform and Convolutional Neural Networks. *Sensors Journal 2023, 23*(10), 4745, 1-14.
- Jurado-Lasso, F. F., Marchegiani, L., Jurado, J. F., Abu-Mahfouz, A. M., & Fafoutis, X. (2022). A Survey on Machine Learning Software-Defined Wireless Sensor Networks (ML-SDWSNs): Current Status and Major Challenges. *IEEE Access, 10,* 23560-23592.
- Ahmed, N., Ngadi, A., Sharif, J. M., Hussain, S., Uddin, M., Rathore, M. S., Iqbal, J., Abdelhaq, M., Alsaqour, R., Sajid Ullah, S., & Tul Zuhra, F. (2022). Network Threat Detection Using MachineDeep Learning in SDN-Based Platforms A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction. *Sensors Journal 2022, 22*(20), 7896, 1-34.
- Sood, T., Prakash, S., Sharma, S., Singh, A., & Choubey, H. (2022). Intrusion Detection System in Wireless Sensor Network Using Conditional Generative Adversarial Network. *Wireless Personal Communications, 126*, 911–931.