مجلة جامعة دمشق للعلوم الهندسية
المجلد 42 العدد (2): 236-252

Damascus University Journal for Engineering Sciences
V42 No(2): 236-252

دراسة أثر هجمات حجب الخدمة DoS على أداء شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN

أحمد لؤي الابراهيم*[1] عبد الرزّاق البدويّة[2]

[1*]. طالب دراسات عليا، دكتوراه في هندسة الاتصالات المتقّدمة، قسم هندسة الإلكترونيات والاتصالات، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق.
(ahmad.alebrahim@damascusuniversity.edu.sy)

[2]. أستاذ، دكتور في قسم هندسة الإلكترونيات والاتصالات، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق.
gbadawil@damascusuniversity.edu.sy.

الملخّص:

تعدّ شبكات الحسّاسات اللاسلكية المعرفة برمجيّاً SDWSN تقنية واعدة لمجموعة متنوعة من التطبيقات، مثل المراقبة البيئية والتحكم الصناعي والرعاية الصحية وغيرها من تطبيقات انترنت الأشياء IoT. ومع ذلك، فإن هذه الشبكات معرّضة لهجمات أمنية عديدة كونها لا تأخذ دائماً في الاعتبار القيود الموجودة في شبكات الحسّاسات اللاسلكية WSN مثل التعقيد الحسابي وقيود الطاقة. ومن أخطر هذه الهجمات هي هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS التي قد تؤدّي إلى تعطيل التشغيل العادي للشبكة عن طريق إغراقها بحركة مرور ضارة أو استهلاك مواردها أو منع حركة المرور المشروعة من الوصول إلى وجهتها.

تدرس هذه الورقة البحثية تأثير هجمات حجب الخدمة DoS على شبكات SDWSN، حيث تلقي نظرة عامّة على الأنواع المختلفة لهذه الهجمات، ثمّ إجراء مضاهاة لشبكة حسّاسات لاسلكية معرّفة برمجيّاً SDWSN، وإجراء عملية تبادل للمعطيات بين العقد والمتحكّم لدراسة وتقييم تأثير هذه الهجمات على أداء شبكات SDWSN. تظهر نتائج الدراسة أنّ هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS يمكن أن يكون لها تأثير كبير على أداء شبكات SDWSN، ويمكنها أن تؤدّي إلى انخفاض معدّل التسليم وزيادة زمن الوصول واستهلاك الطاقة وفقدان الرزم. تقدم هذه الدراسة رؤى جديدة حول تأثير هجمات DoS على شبكات SDWSN، ونعتقد أنّ النتائج التي توصلنا إليها ستكون مفيدة لتصميم ونشر شبكات SDWSN الآمنة.

الكلمات المفتاحية: شبكات الحسّاسات اللاسلكية المعرفة برمجيّاً (SDWSN)، شبكات الحسّاسات اللاسلكية (WSN)، إنترنت الأشياء IoT، هجمات حجب الخدمة (DoS)، هجمات حجب الخدمة الموزّع (DDoS)، الأمان، تأثير الأداء.

تاريخ الإيداع: 2023/8/8
تاريخ القبول: 2023/10/8

http://journal.damascusuniversity.edu.sy/index.php/index/index
ISSN (online): 2789-6854

Study The Impact of DoS Attacks on The Performance of Software-Defined Wireless Sensor Network

Ahmad Al Ebrahim[*1] Abdelrazak Badawieh[2]

[*1.] Postgraduate Student, Department of Electronics and Communications Engineering, Faculty of Mechanical and Electrical Engineering, Damascus University. (ahmad.alebrahim@damascusuniversity.edu.sy)

[2.] Professor, Department of Electronics and Communications Engineering, Faculty of Mechanical and Electrical Engineering, Damascus University. gbadawil@damascusuniversity.edu.sy.

Received: 8/8/2023
Accepted: 8/10/2023

Abstract:

Software-Defined Wireless Sensor Networks (SDWSNs) are a promising technology for a variety of applications, such as environmental monitoring, industrial control, healthcare, and other IoT applications. However, SDWSNs are vulnerable to many security attacks because they do not always take consideration to the restrictions in traditional Wireless Sensor Networks (WSNs) such as computational complexity and power constraints. The most dangerous of these at-tacks are Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks that can disrupt the normal operation of an SDWSN by flooding the network with malicious traffic, consuming network resources, or preventing legitimate traffic from reaching its destination.

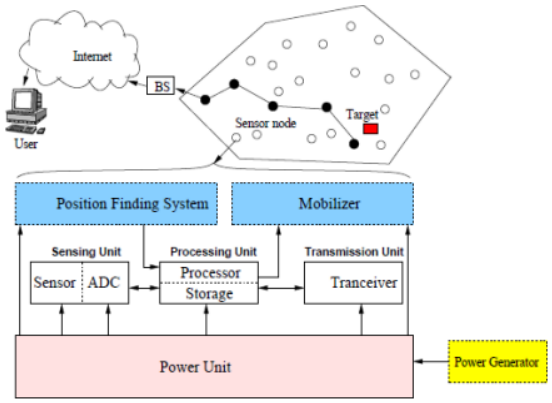
This paper examines the impact of DoS and DDoS attacks on SDWSNs, as it takes an overview of the different types of these attacks, then conducts an emulation for SDWSN network, and execute a data exchange between sensing nodes and the controller to study and evaluate the impact of these attacks on the performance of SDWSNs. The results of the study show that DoS and DDoS attacks can have a significant impact on the performance of SDWSNs, and can lead to reduced Packet Delivery Rate, increased End to End Delay, power consumption, and Packet Loss Rate. This study provides new insights into the impact of DoS attacks on SDWSNs. We believe that our findings will be useful for the design and deployment of secure SDWSNs.

Keywords: Software-Defined Wireless Sensor Network (SDWSN), Wireless Sensor Network (WSN), Internet of Things (IoT), Denial of Service (DoS), Distributed Denial of Service (DDoS), Attacks, Security, Performance Impact.

المقدمة:

تعدّ شبكات الحسّاسات اللاسلكية Wireless Sensor Network (WSN) مكوّنا رئيساً في شبكات الاتصالات الحديثة، وحظيت باهتمام متزايد بسبب كثرة التطبيقات المستفادة منها، وتتكوّن من مئات أو آلاف عقد تحسّس ذات قدرات اتصال وحوسبة واستشعار كما تحتوي هذه العقد على بطاريات تحد من عمرها، وتتواصل مع بعضها البعض أو بشكل مباشر مع محطة قاعدية وتتفاعل مع البيئة المحيطة بها لغرض التحسّس في الموسطات الفيزيائية المتعلقة بالبيئة المحيطة وتحوّلها إلى إشارة كهربائية مثل درجة الحرارة والرطوبة ومستوى الضغط والاهتزازات والحركات والأحداث الزلزالية وغيره(Dludla et al., 2013, 2) ، وتكشف معالجة مثل هذه الإشارات عن بعض الخصائص حول الكائنات الموجودة أو الأحداث التي تحدث في محيط أجهزة التحسّس. وغالباً ما يتم نشر هذه العقد بشكل عشوائي على مساحة كبيرة لأغراض المراقبة مما يتطلب التحكّم في نطاقات الاتصال والتحسّس لضمان الاتصال بالعقد الأخرى ولتغطية المنطقة بأكملها بالتطبيق المطلوب(Mostafaei et al., 2018) .

يبيّن الشكل (1) الرسم التخطيطي لمكوّنات عقدة التحسّس وحقل التحسّس، كما يوضّح كذلك بنية النقل والإرسال في شبكة WSN، حيث أنّ كل عقدة ليست مسؤولة فقط عن جمع المعطيات، بل تعتمد في قراراتها على نوعها ومهمتها والمعطيات التي لديها، ومعرفتها وحسابها، وطرائق اتصالها، وموارد الطاقة. ولكل من هذه العقد القدرة على جمع المعطيات وتوجيهها إما إلى عقد أخرى أو العودة إلى المحطّة القاعدية. وقد تكون هذه المحطة عقدة ثابتة أو عقدة متنقلة قادرة على توصيل شبكة الحسّاسات مع بنية اتصالات قائمة أو بالإنترنت حيث يمكن للمستخدم الوصول إلى المعطيات المبلّغ عنها .(Mallick et al., 2018, 42)



الشكل (1) مكوّنات عقدة التحسّس وحقل التحسّس (Mallick et al., 2018)

إن سهولة النشر والتكلفة المنخفضة لشبكات WSN جعلت استخدامها أكثر شيوعاً، فأصبحنا نجدها في مجموعة متنوعة من تطبيقات انترنت الأشياء IoT، تتراوح من المجالات الصناعية والأمنية مثل أتمتة العمليات وتطبيقات المراقبة بالفيديو، وصولاً إلى تطبيقات الاستخدام الشخصي مثل التشغيل الآلي للمنزل والإشراف الطبي. ومع ذلك فقد اشتهرت شبكات WSN بمجال التطبيقات الرئيسية لإنترنت الأشياء للمدن الذكية، واشتهرت بشكل متزايد بتطبيقات مثل النقل ومراقبة البيئة وقياس المياه والغاز ومواقف السيارات الذكية وغيرها (Zanella et al., 2014, 22).

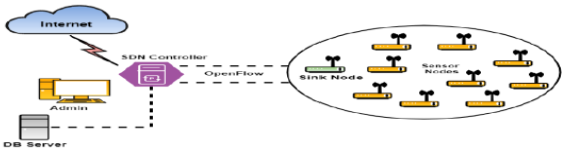
في حين أنّ الشبكات المعرّفة برمجيّاً Software Defined Network (SDN) هي بنية شبكات تمنح الفرصة للتغلب على القيود الحالية للبنية التحتية في الشبكات التقليدية، وذلك بفصل مستوي التحكّم Control Plane في الشبكة عن مستوي البيانات Data Plane. وهذا يعني أن وحدة التحكّم الذكية تقوم بتكوين عناصر إعادة التوجيه مع قواعد مخصّصة لرزم البيانات ذات التدفّقات المختلفة، عن طريق حصولها على معلومات كافية لتنفيذ هذه المهمة بحيث لم تعد هناك حاجة إلى بروتوكولات التحكّم الموزعة بين عناصر إعادة التوجيه. بالإضافة إلى تحسين أداء الشبكة عن طريق تفاعلها مع التطبيقات في مستوي التطبيقات (Mostafaei et al., 2018).

ISSN (online): 2789-6854
https://journal.damascusuniversity.edu.sy/index.php/engj/index

ومن الممكن أن تتسبب عملية التحكّم هذه في حدوث مشكلات خطيرة عند وجود طلبات مفرطة من مستوي البيانات إلى مستوي التحكّم، فإذا تلقّى مستوي البيانات العديد من الطلبات في فترة زمنية قصيرة، يمكنه إغراق الرسائل في مستوي التحكّم، كما يمكنه أيضاً إغراق جدول التدفّق في مستوي البيانات المقيدة بقواعد معالجة الطلبات (Fawcett et al., 2018, 2805).

تمّ اقتراح شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً Software Defined Wireless Sensor Network (SDWSN) بهدف أن تتمكن شبكات WSN من الاستفادة بشكل خاص من نموذج شبكات SDN وذلك عن طريق تبسيط تشغيل عقد التحسّس لتوفير الطاقة وإدارة كامل الشبكة من خلال وحدة تحكّم قوية لها رؤية على الشبكة بأكملها بدلاً من بروتوكولات التحكّم الموزّعة (Mostafaei et al., 2018)، بالإضافة إلى معالجة التحديات المتأصلة لأداء شبكات WSN، والمتمثّلة في قيود الموارد التي تؤدي إلى عدم القدرة على تنفيذ تدابير الأمان، كما تواجه شبكات SDN أيضاً مشاكلها الخاصة مثل المفاضلة بين الوظيفة والأداء (خاصّة على مستوي البيانات)، مما يؤدّي إلى نقاط ضعف أمنية.

يوضّح الشكل (2) نظرة عامّة على نموذج شبكات SDWSN، حيث تنفّذ عقد التحسّس وظائف إعادة التوجيه فقط ويكون ذكاء الشبكة في وحدة تحكّم نموذج شبكات SDN، كما ستكون المهام الحسابية المكثّفة والمستهلكة للطاقة مثل إدارة حركة المرور وإدارة جودة الخدمة وتخصيص الموارد وإحصائيات الشبكة وقياس مستويات الطاقة وحساب المسارات وغيرها من المهام التي تنفّذ من وحدة التحكّم (Letswamotse et al., 2018, 1306).



الشكل (2) نظرة عامة على نموذج شبكات SDWSN (Letswamotse et al., 2018)

1- المشكلة:

دخلت شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN العديد من التطبيقات المدنية والعسكرية، وأصبح للمعطيات التي تنتقل عبرها أهمية في إجرائيات اتخاذ القرار، كما أن الاستخدام الكبير لهذه الشبكات في تطبيقات انترنت الأشياء IoT أدى إلى تزايد الطلب عليها، لذا غدا أمن هذه المعطيات وحمايتها من أي مؤثر خارجي قد يمنع إيصالها أو يغير محتواها من الأولويات الواجب أخذها بالحسبان عند استخدام هذا النوع من الشبكات، بما في ذلك هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS التي تشكّل حجر الأساس للتحديات الأمنية في شبكات SDWSN، والتي تؤثّر على أداء هذه الشبكات عبر إغراقها بحركة المرور أو إرسال بيانات ضارة أو استهلاك مواردها.

سيتناول البحث الأنواع المختلفة لهجمات DoS التي يمكن أن تستهدف شبكات SDWSN وتأثيرها على أداء الشبكة.

2- الأسس النظرية للبحث:

2-1- الدراسات المرجعية:

أوضح (Sarkunavathi et al., 2021) هجمات حجب الخدمة DoS المختلفة في طبقات شبكات WSN والإجراءات المضادة الحالية واستراتيجيات الدفاع للحفاظ على السرّية والمتاحية والسلامة ضد الهجمات اللاسلكية الخبيثة، كما أوضحوا كيفية مساعدة ميّزات نموذج شبكات SDN في التخفيف من أثر هذه الهجمات من أجل إنشاء تدفّقات حركة المرور التي تقلل من استهلاك الطاقة للشبكة، حيث يمكن لوحدة تحكم SDN اتخاذ قرارات توجيه أفضل ويمكن استخدامها بشكل ملائم في شبكات WSN الحديثة.

بينما اقترح (Ahmad et al., 2015) طرق متعددة لتأمين مستوي التحكّم في نموذج شبكات SDN، مثل الحماية ضد التطبيقات الخبيثة أو الخاطئة، والحماية من قابلية التوسع المستهدفة لمستوي التحكّم، كذلك منع حجب الخدمة DoS وحجب الخدمة الموزّع DDoS وضمان الأمن من خلال وضع

متحكّم موثوق به، عن طريق تنفيذ آلية لتخفيف حجب الخدمة DoS وحجب الخدمة الموزّع DDoS من خلال مراقبة إحصائيات التدفّق المخزنة في مبدّلات التدفّق المفتوح OpenFlow Switches.

في حين قام (Yin et al., 2018) باقتراح كاشف لهجمات حجب الخدمة الموزّع DDoS لمراقبة اختلاف الرزم التي تتلقاها وحدة التحكّم باستخدام تشابه جيب التمام عبر تطوير إطار عمل SD-IoT، حيث يعتمد هذا الاقتراح فقط على وجهة نظر وحدة التحكّم مما قد يحد من أنواع الهجوم التي يمكنه اكتشافها. تم تصميم هذه الآلية للشبكات حيث يكون لجميع العقد اتصال دوري مع وحدة التحكّم، والتي قد لا تكون مثالية للشبكات المقيدة للغاية ذات العقد المنخفضة. اختبر المؤلفون اقتراحهم من خلال عمليات المحاكاة باستخدام برنامج المضاهاة Mininet ولم يتم تحديد حجم الشبكة بشكل صريح، ولكن يُستدل على أنه يتراوح بين 50 إلى 60 عقدة.

كما قام (Segura et al., 2019) بإجراء تحليل لحركة مرور بيانات شبكة SDWSN من أجل فهم أداء الشبكة عندما تكون تحت أنواع معينة من هجمات حجب الخدمة DoS، حيث أظهرت النتائج حدوث تغييرات مهمّة في كل من متوسط القيمة والتباين في معدل تسليم الرزم PDR والنفقات العامة الأخرى مثل زمن التأخير واستهلاك الطاقة، وذلك في حالة وجود مهاجم واحد أو أكثر من مهاجم.

بينما قام (Segura et al., 2020) بإجراء دراسة لأثر هجمات حجب الخدمة الموزّع DDoS في شبكات SDWSN وتقديم مقترح لاكتشاف هذا الهجوم من خلال مراقبة التغييرات في القيم المتوسطة لكل من معدل تسليم رزم بيانات الشبكة ورزم التحكّم باستخدام خوارزمية نقطة التغيير Change Point (CP) بهدف تقدير وجود التغييرات وعددها وحجمها واتجاهها في الوقت الفعلي في سلسلة زمنية، لاكتشاف تغيير في أي من المقياسين بسبب هجوم DDoS، حيث تعتمد هذه الطريقة على البحث عن نقاط التغير في سلسلة البيانات من خلال مقارنة قيم السلسلة مع المتوسط أو الانحراف المعياري، عبر تحليل سلسلة البيانات لتحديد وجود نقاط التغير المحتملة، وتحديد نقاط التغير المحتملة بناءً على نتائج التحليل، ثمّ تقييم نقاط التغير المحتملة لتحديد ما إذا كانت نقاط تغير فعلية. والتي تمّ تطبيقها في طوبولوجيا مكونة من 36 و100 عقدة، وبأعداد متفاوتة من المهاجمين، وأوجد الباحثون علاقة ما بين ارتفاع معدّل الكشف مع زيادة شدّة الهجوم حيث وصلت إلى 100%.

في حين قام (Jurado-Lasso et al.,2022) بإجراء مراجعة شاملة لأعمال أبحاث شبكات SDWSN وتقنيات تعلّم الآلة لأداء إدارة الشبكة وإعادة تشكيلها. كما أكّدوا في بحثهم أن شبكات SDWSN هي حل فعّال لتحسين أداء شبكات WSN وإدارتها عبر استخدام خوارزميات تعلّم الآلة Machine Learning (ML)، والتي أصبحت حلّاً شائعاً وتظهر أداءً جيداً في معالجة المشكلات الرئيسية، ويمكن لهذا الاستخدام أن يساعد في اتخاذ قرارات أكثر ذكاءً وقوة، كما أن لهذه الخوارزميات دوراً هاماً في إنشاء تطبيقات وبروتوكولات جديدة في شبكات SDWSN.

في دراسة مماثلة، قام (Ahmed et al., 2022) بمناقشة مناهج مختلفة تستند إلى التقنيات الكلاسيكية لاكتشاف الهجمات في نموذج شبكات SDN والتي يمكن استخدامها في شبكات SDWSN، حيث تضمّنت الدراسة شرحاً حول نقاط الضعف في الأساليب التقليدية وضعف أدائها، والتأكيد على إمكانية الكشف عن الثغرات الأمنية ورصد الشبكة باستخدام أساليب تعلّم الآلة ML والتعلّم العميق Deep Learning (DL). وأظهروا أن استخدام هذه المنهجيات تحسّن فعالية أجهزة الكشف وأدائها من حيث زيادة دقة الكشف.

كما قام (Liu et al., 2023) باقتراح طريقة كشف فعّالة لهجمات Low-Rate Denial of Service (LDoS) مع سمات الإشارات الصغيرة، حيث تُحلّل الإشارات الصغيرة الناتجة عن الهجمات باستخدام طريقة تحليل الوقت والتردد

بناءً على تحويل هيلبرت–هوانغ Hilbert–Huang Transform (HHT) عبر تحويل سمات تدفّق البيانات أحادية البعد إلى سمات زمنية طيفية ثنائية الأبعاد، والتي يتم إدخالها بشكل إضافي في الشبكة العصبونية التلافيفية Convolutional Neural Network (CNN) لاكتشاف هجمات LDoS. كما قاموا بتقييم الأداء بمحاكاة هجمات LDoS المختلفة في بيئة محاكاة NS-3 وأظهرت النتائج التجريبية أن الطريقة لديها دقة الكشف بنسبة 99.8٪ مع الحفاظ على معدلات منخفضة إيجابية كاذبة وسلبية كاذبة لهجمات LDoS المعقّدة والمتنوعة.

نجد في ضوء الدراسات المرجعية السابقة أنّ الأبحاث التي تناولت هذا موضوع دراسة أثر هجمات حجب الخدمة DoS على أداء شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN قديمة نسبيّاً، وأنّ الأبحاث الحديثة المتاحة في المجلات والمراجع العالمية تعالج موضوع الكشف عن هذه الهجمات دون دراسة أثرها على أداء الشبكة، كما أنّها تدرس معدّلات الكشف عن هذه الهجمات باستخدام خوارزميات تعلّم الآلة والتعلّم العميق دون انعكاسها على الأداء الإجمالي للشبكة.

2-2- هجمات حجب الخدمة في شبكات SDWSN:

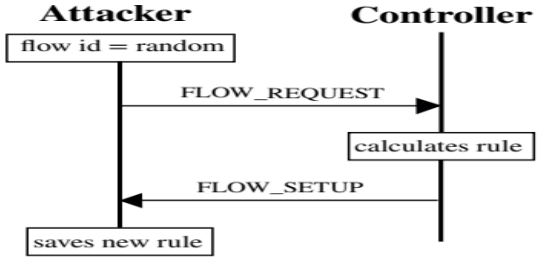
حجب الخدمة يعني إما عدم توافر الشبكة أو تغيير المعطيات المنقولة عبرها، وذلك بإرسال رزم إضافية غير ضرورية قبل أن يقرأها المستخدم المطلوب بالفعل. وينتج هذا الهجوم من عمل ضار أو فشل مقصود في العقد المستهدفة واستهلاك مواردها ومنع المستخدمين الشرعيين من الوصول إلى الموارد التي يحق لهم الحصول عليها (Sharma et al., 2017, 388)، كما يمكن تصعيد هذه الهجمات من داخل أو من خارج الشبكة عن طريق إرسال طلب وهمي نيابة عن أعضاء آخرين.

ويعد هجوم حجب الخدمة DoS أحد أكثر الهجمات الأمنية المحتملة في نموذج شبكات SDWSN، كما يمكن للمهاجمين الوصول إلى كامل الشبكة والتحكّم فيها بسبب الواجهات المفتوحة والبروتوكولات المعروفة المستخدمة فيها. وعلاوة على ذلك فإن الشبكة تعاني أيضاً من مخاطر هجوم حجب الخدمة الموزّع DDoS الذي يشن على كفاءة لاستهلاك الموارد ويستهلكها بشكل كبير (Kgogo et al., 2017).

2-3- آلية عمل هجمات حجب الخدمة:

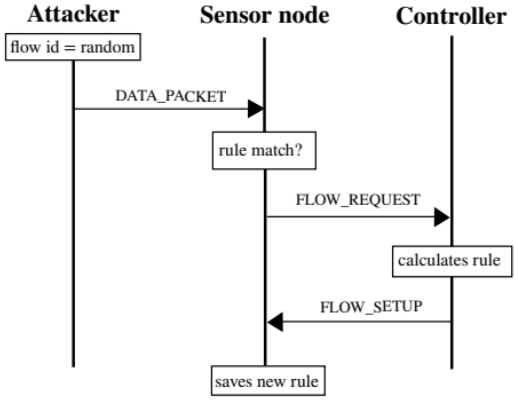
يستهدف هذا الهجوم كلاً من مستوي التحكم ومستوي البيانات في شبكات SDWSN نظراً للعدد الكبير من رسائل التدفّق الجديدة التي تؤدي إلى تدهور أداء الشبكة، فعندما تتلقى العقدة رسالة لا مثيل لها في جدول التدفّق، يتوجّب على هذه العقدة عندها، إرسال رسالة تحكم بالتدفّق الجديد إلى وحدة التحكم للحصول على قاعدة توجيه جديدة. ويمكن للمهاجمين استغلال هذه الميزة لشن هجوم حجب الخدمة في كل من مستويات البيانات والتحكم، كما يمكن شن الهجوم باستخدام بيانات مزورة أو التحكم في الرسائل بواسطة عقدة ضارة. يمكن تقسيم أنواع هذا الهجوم إلى ثلاث أقسام رئيسية وهي:

1) جوم طلب التدفّق الخاطئ False Flow Request (FFR): يستهدف هذا الهجوم وحدة التحكم وتتمثل أهدافه الرئيسية في زيادة عبء معالجة وحدة التحكم وحركة مرور الرزمة من أجل زيادة عدد التصادمات، حيث يرسل المهاجم طلبات قواعد تدفّق متعددة إلى وحدة التحكم لتدفّقات مختلفة لتحقيق هذه الأهداف. تعالج وحدة التحكم الرزم وتحسب القواعد وترسل الردود إلى المهاجم (Segura et al., 2019). ويوضّح الشكل (3) تبادل الرزم لهذا الهجوم.



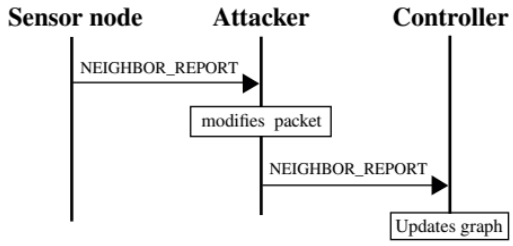
الشكل (3) تبادل الرزم في هجوم طلب التدفّق الخاطئ (Segura et al., 2019)

2) هجوم توجيه تدفّق البيانات الخاطئة False Data Flow Forwarding (FDFF): وهو هجوم مشابه للهجوم السابق لأنه يستهدف وحدة التحكم، ومع ذلك يختلف تنفيذه حيث يتم تحقيق ذلك عبر أجهزة الشبكة. حيث يرسل المهاجم في هذه الحالة رزمة بيانات ذات تدفّق غير معروف إلى الجوار، ونظراً لأن الجوار لا يعرفون التدفّق، فسوف يطلبون قاعدة تدفّق من وحدة التحكم. تتمثل الأهداف الرئيسية للهجوم في زيادة أعباء معالجة وحدة التحكم والجوار وزيادة حركة مرور رزم الشبكة، كما يمكن أن يؤدي هذا الهجوم إلى تعويم جدول تدفّق الجوار كونها أجهزة مقيدة ذات سعة تخزين محدودة (Segura et al., 2019)، ويوضّح الشكل (4) تبادل الرزم لهذا الهجوم.



الشكل (4) تبادل الرزم في هجوم توجيه تدفّق البيانات الخاطئة (Segura et al., 2019)

1) هجوم معلومات الجوار الخاطئة False Neighbor Information (FNI): يقوم هذا الهجوم بتعديل الرزم التي تحتوي على معلومات الجوار، وستعمل وحدة التحكم بهذه الطريقة على التعامل مع المعلومات الخاطئة على أنها صحيحة وسترسل قواعد توجيه خاطئة إلى العقد. الهدف الرئيسي من هذا الهجوم هو تقليل معدل توصيل الشبكة (Segura et al., 2019)، ويوضّح الشكل (5) تبادل الرزم لهذا الهجوم



الشكل (5) تبادل الرزم في هجوم معلومات الجوار الخاطئة (Segura et al., 2019)

3- التطبيق العملي والنتائج والمناقشة:

يشمل التطبيق العملي إجراء مضاهاة Emulation لشبكة حساسات لاسلكية معرّفة برمجياً SDWSN باستخدام البرنامج Mininet-WiFi وهو برنامج مفتوح المصدر يمكن من خلاله تعديل مواصفات البيئة وتغييرها، وباستخدام المتحكّم من النوع Ryu-Manager Controller وهو متحكّم مفتوح المصدر.

يهدف التطبيق العملي إلى دراسة أثر هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS في شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN، وتوضّح الفقرات التالية معاملات بيئة العمل وعملية المضاهاة التي تمّت لإجراء هذه الدراسة، بالإضافة إلى نتائج تحليل أداء الشبكة وفق مقاييس خصائص الأداء للشبكة من نسبة توصيل الرزم ومتوسط التأخير من نهاية إلى نهاية ومتوسط استهلاك الطاقة وتحليل مقاييس زمن الرحلة.

3-1- معاملات بيئة العمل:

تبيّن الجداول (1) و (2) و (3) المعاملات الأساسية في بيئة العمل المقترحة لسيناريوهات المضاهاة المختلفة، وهي: معاملات البيئة العامة ومعاملات القناة اللاسلكية والهوائيات ومعاملات الطاقة على الترتيب.

الجدول (1) معاملات البيئة العامة

المعامل	القيمة
حجم الحقل	500 X 500 [m]
نوع المتحكّم	Ryu-Manager Controller
عدد المتحكّمات	1
عدد عقد التحسس	24
عدد نقاط النفاذ	2
عدد محطات الهجمات	4
حركية العقد وإمكانية التنقل	ثابت
توزيع العقد	OpenFlow1.3
بروتوكولات التبديل	ICMP – TCP – UDP

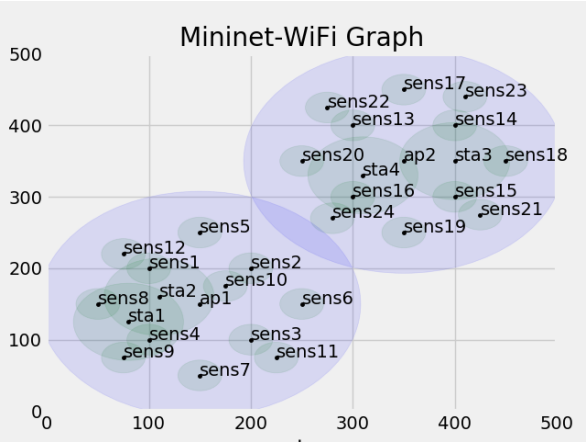
الجدول (2) معاملات القناة اللاسلكية والهوائيات

المعامل	القيمة
نوع قناة الاتصال	Wireless
نوع واجهة الربط للشبكة	Wireless Phy
بروتوكول الاتصال اللاسلكي	802.11
نمط قناة البروتوكول	n
التردد	2.4 [GHz]
رقم قناة الاتصال	1 and 6
ربح هوائي عقد التحسّس	3 [dBi]
ربح هوائي نقاط الوصول	9 [dBi]
ربح هوائي محطّات الهجمات	6 [dBi]
مجال الاتصال لعقد التحسّس	≈ 25 [m]
مجال الاتصال لنقاط الوصول	≈ 158 [m]
مجال الاتصال لمحطّات الهجمات	≈ 54 [m]
نموذج الانتشار الراديوي	Log-Distance Path Loss Model

الجدول (3) معاملات الطاقة

المعامل	القيمة
الجهد الابتدائي لعقد التحسّس	10 [Volt]
الجهد الابتدائي لنقاط الوصول	10 [Volt]
الجهد الابتدائي لمحطّات الهجمات	10 [Volt]
استطاعة الإرسال لعقد التحسّس	3 [dBm]
استطاعة الإرسال لنقاط الوصول	30 [dBm]
استطاعة الإرسال لمحطّات الهجمات	15 [dBm]

كما يوضّح الشكل (6) التوزيع الثابت للعقد ضمن بيئة العمل، حيث جرى إسناد أرقام تسلسلية لعقد التحسس من sens1 وحتى sens24 وإسناد أرقام تسلسلية لمحطات الهجمات من sta1 وحتى sta4 وإسناد أرقام تسلسلية لنقاط الوصول من ap1 وحتى ap2، لتسهيل عملية الترميز لغرض المحاكاة.



الشكل (6) التوزيع الثابت للعقد ضمن بيئة العمل

2-3- مقاييس خصائص الأداء للشبكة:

ثمّة العديد من مقاييس خصائص الأداء المتاحة والمستخدمة في تقييم أداء الشبكة ولدراسة أثر هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS، وقد استخدمنا في هذا البحث عدة مقاييس للتقييم والمقارنة، وفيما يأتي أهم هذه المقاييس.

نسبة تسليم الرزم Packet Delivery Ratio (PDR):
يعد معدل التسليم ومعدّل فقدان الرزم مقياس أداء مهم للشبكة، وهي النسبة المئوية لعدد الرزم التي تستقبلها العقدة الوجهة إلى عدد الرزم التي ترسلها العقدة المصدر (العلاقة 1) وعندما تكون هذه النسبة عالية يمكن القول أنّ الأداء أفضل.

$$\text{PDR}\,[\%] = \frac{\text{TRP}}{\text{TTP}} * 100 \qquad (1)$$

حيث أنّ:

PDR (Packet Delivery Ratio): يعبّر عن نسبة تسليم الرزم.

TRP (Total Received Packets): يعبّر عن مجموع الرزم المستقبلة.

(Total Transmitted Packets) TTP: يعبّر عن مجموع الرزم المرسلة.

نسبة فقد الرزم (Packet Loss Ratio (PLR: فقد الرزم يعني عدد الرزم التي لا يمكن استلامها عند الوجهة، أو التي لم تصل أبداً إلى الوجهة بعد أن أرسلت من المصدر، وهي النسبة المئوية لعدد العقد التي تفشل بالوصول إلى العقدة الوجهة أو المتحكّم، إلى عدد الرزم التي ترسلها العقدة المصدر (العلاقة 2)، ويكون الأداء أفضل عندما تكون هذه النسبة منخفضة.

$$PLR\ [\%] = \frac{TLP}{TTP} * 100 \qquad (2)$$

حيث أنّ:

(Packet Loss Ratio) PLR: يعبّر عن نسبة فقد أو خسارة الرزم.

(Total Lost Packets) TLP: يعبّر عن مجموع الرزم المفقودة.

(Total Transmitted Packets) TTP: يعبّر عن مجموع الرزم المرسلة.

متوسط التأخير من نهاية إلى نهاية Average End to End delay: يتم حساب التأخير من نهاية إلى نهاية عن طريق أخذ الفرق بين الوقت الذي تم فيه إرسال الرزم من العقدة المصدر، والوقت الذي تم فيه استلام هذه الرزمة عند المستقبل أو الوجهة المقابلة. يتم حساب متوسط التأخير من طرف إلى طرف بحساب متوسط كل تأخير الرزم التي تم إنشاؤها بواسطة شبكة العقد بأكملها (العلاقة 3) ويقاس بالميلي ثانية.

$$E2EAD\ [ms] = \frac{TRPT - TSPT}{TRPN} \qquad (3)$$

حيث أنّ:

(End to End Average Delay) E2EAD: يعبّر عن متوسّط التأخير من نهاية إلى نهاية.

(Total Received Packet Time) TRPT: يعبّر عن مجموع أزمنة وصول الرزم المستقبلة.

(Total Sent Packets Time) TSPT: يعبّر عن مجموع أزمنة إرسال الرزم المرسلة.

(Total Received Packets Number) TRPN: يعبّر عن مجموع عدد الرزم المستقبلة.

استهلاك الطاقة Energy Consumption: يعبّر عن استهلاك الطاقة لعقدة أو محطة ما من العقد أو المحطّات المستخدمة في المضاهاة، وتزداد هذه القيمة بازدياد استهلاك الطاقة ويتم حسابه من برنامج المضاهاة Mininet-WiFi (العلاقة 4) ويقاس بالميلي جول، ويكون أداء الشبكة جيد في حال استخدام كمية أقل من الطاقة أثناء فترة المضاهاة.

$$EC\ [mJ] = T * V * I * F \qquad (4)$$

حيث أنّ:

(Energy Consumption) EC: يعبّر عن استهلاك الطاقة.

(Time) T: يعبّر عن زمن التشغيل.

(Voltage) V: يعبّر عن الجهد.

(Current Intensity) I: يعبّر عن التيار المار في العقدة.

(Factor) F: معامل خاص ببرنامج المضاهاة Mininet-WiFi، ويستخدم في حساب الطاقة المستهلكة في العقد، كما يختلف باختلاف حالة عمل كل عقدة أو مكوّن للشبكة (حالة الإرسال – حالة الاستقبال – حالة الخمول – حالة التوقف عن العمل) وفقاً للجدول (4).

الجدول (4) قيم المعامل F

المعامل	القيمة
معامل الاستطاعة F في حالة الخمول	0.273
معامل الاستطاعة F في حالة الارسال	0.380
معامل الاستطاعة F في حالة الاستقبال	0.313
معامل الاستطاعة F في حالة النوم (التوقف)	0.033

مقاييس زمن الرحلة Round-Trip Time (RTT): تستخدم مقاييس زمن الرحلة ذهاباً وإياباً RTT لحساب الوقت الذي تستغرقه الرزمة للانتقال إلى وحدة التحكم والعودة، كما يقيس الانحراف المعياري (تباين الوقت) أو التأخير عبر جميع الرزم المسجلة خلال فترة التقييم، كما يساعد في حساب معدل الخطأ

ومعدّل تسليم ومعدّل فقد الرزم. وتمّ الاستفادة من أداة ping المستخدمة في هذه الورقة البحثية والتي تقوم بدوها تلقائياً بحساب هذه الأزمنة عبر يتم إرسال رزمة بيانات من المصدر إلى الوجهة وقياس الوقت الذي تستغرقه هذه الرزمة للوصول إلى الوجهة والعودة إلى المصدر، حيث تكرّر هذه العملية على عدد الرزم المرسلة للحصول على متوسط زمن الرحلة والإحصائيات الأخرى.

3-3- عملية المضاهاة:

تمّ إجراء المضاهاة بهدف دراسة أثر هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS في حال عدم وجود الهجمات ومع وجود الهجمات التي يتم شنّها من محطّات الهجمات. ذلك في زمن تشغيل 300.0 Sec لتخزين الطاقة، ضمن حقل أبعاده [m] 500 X 500 وتوزع ثابت للعقد غير المتحركة، مع وجود أربع وعشرون عقدة تحسّس تتصل مع المتحكّم عبر نقطتي وصول وتتبادل معطيات من نوع رسائل بروتوكول التحكم برسائل الإنترنت Internet Control Message Protocol (ICMP)، كما تمّ شن الهجمات من محطتي هجمات وأيضاً من أربع محطّات.

تمّ تخزين معلمات الدراسة والتحليل في حال عدم وجود الهجمات عبر إجراء عملية تبادل للمعطيات بين عقد التحسّس عقد والمتحكّم على الشكل التالي:

التحسّس (Sens1 to Sens12) تتبادل المعطيات مع نقطة الوصول الأولى (AP1) باستخدام أداة ping.

عقد التحسّس (Sens13 to Sens24) تتبادل المعطيات مع نقطة الوصول الثانية (AP2) باستخدام أداة ping.

نقطة الوصول الأولى والثانية (AP1 and AP2) تتصلان بشكل مباشر مع مبدّل التدفّق المفتوح OpenFlow Switch، الذي يتّصل بدوره بالمتحكّم.

ثمّ تمّ تخزين معلمات الدراسة والتحليل في حال وجود هجومين اثنين عبر إعادة نفس عملية المضاهاة السابقة مع إضافة الاتصالات التالية:

محطة الهجوم الأولى (Sta1) تقوم بمهاجمة نقطة الوصول الأولى (AP1) باستخدام أداة hping3.

محطة الهجوم الثالثة (Sta3) تقوم بمهاجمة نقطة الوصول الثانية (AP2) باستخدام أداة hping3.

ثمّ تمّ تخزين معلمات الدراسة والتحليل في حال وجود أربع هجمات عبر إعادة نفس عملية المضاهاة السابقة مع إضافة الاتصالات التالية:

محطة الهجوم الثانية (Sta2) تقوم بمهاجمة نقطة الوصول الأولى (AP1) باستخدام أداة hping3.

-

حطة الهجوم الرابعة (Sta4) تقوم بمهاجمة نقطة الوصول الثانية (AP2) باستخدام أداة hping3.

حيث تشن محطّات الهجمات هجوم تعويم رسائل بروتوكول التحكم برسائل الإنترنت ICMP Flood Attack.

4-3- تحليل النتائج:

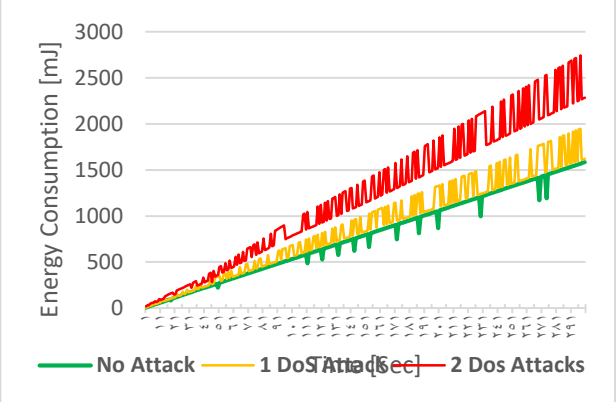
أُجريت المقارنة بين حالة عدم وجود الهجمات وحالة وجود الهجمات باستخدام الرسوم البيانية لمقاييس خصائص الأداء للشبكة، ويوضّح الشكل (7) والشكل (8) استهلاك الطاقة لنقطة الوصول الأولى AP1 ونقطة الوصول الثانية AP2 في حال عدم وجود هجمات حجب الخدمة وفي حالة وجود هجوم من محطة هجوم واحدة وفي حالة وجود هجمتين من محطتي هجمات على الترتيب خلال زمن 300 ثانية. حيث يُلاحظ من الشكل (7) أن مقدار استهلاك الطاقة في نقطة الوصول الأولى AP1 قد وصل إلى قيمة تقارب 1949 ميلي جول عند وجود هجوم واحد من محطة هجوم، وبلغ استهلاك الطاقة إلى ما يقارب 2746 ميلي جول عند وجود هجمتين من محطتي هجمات، وذلك مقارنةً بقيمة الاستهلاك التي تقارب 1585 ميلي جول عند عدم وجود الهجمات.

كما يُلاحظ من الشكل (8) أن مقدار استهلاك الطاقة في نقطة الوصول الثانية AP2 قد وصل إلى قيمة تقارب 1949 ميلي جول عند وجود هجوم واحد من محطة هجوم، وبلغ

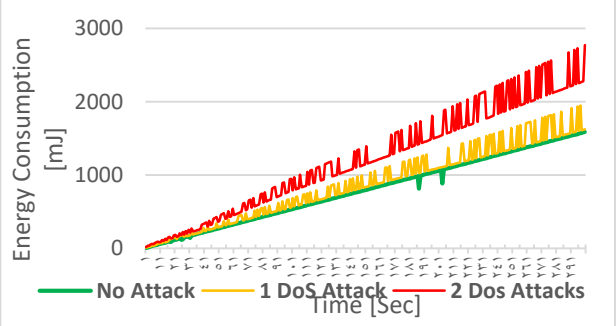
استهلاك الطاقة إلى ما يقارب 2773 ميلي جول عند وجود هجمتين من محطتي هجمات، وذلك مقارنةً بقيمة الاستهلاك التي تقارب 1585 ميلي جول عند عدم وجود الهجمات.

بالتالي نجد من الشكلين (7) و (8) أن هجمات حجب الخدمة أدت إلى زيادة في مقدار استهلاك الطاقة لنقطة الوصول الأولى AP1 ونقطة الوصول الثانية AP2 مما ينعكس سلباً على أداء الشبكة والعمر التشغيلي لها، ويجعل أداء الشبكة أسوأ.

يبيّن كذلك الجدول (5) متوسط استهلاك الطاقة لعقد التحسّس خلال زمن التشغيل البالغ 300 ثانية في حالة عدم وجود هجمات حجب الخدمة DoS وفي حالة وجود هجوم واحد على كل نقطة وصول وفي حالة وجود هجمتين من محطتي هجمات.



الشكل (7) استهلاك الطاقة لنقطة الوصول الأولى AP1 مع وبدون وجود هجوم حجب الخدمة DoS



الشكل (8) استهلاك الطاقة لنقطة الوصول الثانية AP2 مع وبدون وجود هجوم حجب الخدمة DoS

الجدول (5) متوسط استهلاك الطاقة لعقد التحسّس

المعامل	المتوسط [mJ]
عدم وجود هجمات	795.921
وجود هجوم واحد على كل نقطة وصول	962.867
وجود هجومين على كل نقطة وصول	1005.973

كذلك أُجريت المقارنة بين حالة عدم وجود الهجمات وحالة وجود الهجمات باستخدام مقاييس زمن الرحلة RTT للرزم المرسلة من عقد التحسّس إلى نقاط الوصول وحساب الاحصائيات لها، ويبيّن الجدول (6) نتائج تحليل هذه الاحصائيات.

الجدول (6) نتائج تحليل إحصائيات مقاييس زمن الرحلة

المتوسط / المعامل	حالة عدم وجود هجمات	حالة وجود هجومين	حالة وجود أربع هجمات
عدد الرزم المرسلة	800	800	800
عدد الرزم المستقبلة	791	294	12
عدد الرزم الضائعة	9	506	788
نسبة تسليم الرزم PDR	99%	36.74%	1.45%
نسبة فقد الرزم PLR	%1	63.26%	98.55%
متوسط التأخير من نهاية إلى نهاية [ms]	7.099	135.296	12016.059

5-3- الاستنتاجات والمقارنة:

نجد من الشكل (7) والشكل (8) السابقين، أن وجود عقدة مهاجمة واحدة بهجوم حجب الخدمة DoS قد أدّت إلى زيادة في استهلاك الطاقة في نقطة الوصول التي تتصل معها، وازداد استهلاك الطاقة بشكل أكبر في حال وجود عقدتي هجوم، وفي حال زيادة عدد عقد الهجمات من محطّات الهجمات أو من عقد التحسّس ذاتها بإجراء هجمات حجب الخدمة الموزّع DDoS سيؤدي إلى استهلاك أكبر بالطاقة

لنقاط الوصول حتى تفريغ كامل طاقتها وتوقفها عن العمل ونتيجةً لذلك توقف كامل الشبكة عن العمل.

كما نجد من الجدول (6) السابق أن هجمات حجب الخدمة DoS في حال حصول هجومين في نفس الوقت، قد تسببت بخسارة ما يقارب 62% من حجم المعطيات التي تمر خلال الشبكة مقارنةً بحالة الاتصال الطبيعية. وأنّ الخسارة وصلت إلى ما يقارب 98% من حجم المعطيات التي تمر خلال الشبكة في حال حصول أربع هجمات في نفس الوقت أي شن هجمات حجب الخدمة الموزّع DDoS.

كما نجد حصول زيادة كبيرة في متوسط زمن وصول الرزم من العقدة المصدر إلى نقطة الوصول أو المتحكّم (متوسط التأخير من نهاية إلى نهاية) من زمن يقدّر بحوالي 7 ميلي ثانية في حالة الاتصال الطبيعية، إلى 12016 ميلي ثانية في حال وجود أربع هجمات، كما أن الشبكة قد تتوقّف على العمل عند زيادة عدد الهجمات أو زيادة حجم الهجوم الواحد بتنفيذ هجوم حجب الخدمة الموزّع DDoS.

جرت مقارنة النتائج مع (Segura et al., 2019) ; (Segura et al., 2020) حيث وجدنا تقارب في نتائج أثر وجود هجمات حجب الخدمة في شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN، والتي تسبّب زيادة كبيرة في نسبة فقد الرزم وزيادة كبيرة في التأخيرات الزمنية لوصولها، بالإضافة إلى زيادة استهلاك الطاقة لعقد التحسّس. ويبيّن الجدول (7) نتائج هذه المقارنة.

4- الخاتمة والآفاق المستقبلية:

تتعرض شبكات SDWSN لتهديدات أمنية جديدة تؤثر بشكل مباشر على أداء شبكات WSN التقليدية، حيث قمنا بدراسة أثر هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS في هذه الشبكة، وفي نهاية هذا البحث وبعد إجراء هذه الهجمات وتحليل الرسوم البيانية لمقاييس خصائص الأداء للشبكة وإحصائيات مقاييس زمن الرحلة RTT للرزم المرسلة من عقد التحسّس إلى نقاط الوصول، توصّلنا إلى أنّ وجود عقدة مهاجمة واحدة بهجوم حجب الخدمة DoS قد أدّت إلى زيادة في استهلاك الطاقة في نقطة الوصول التي تتصل معها، وازداد استهلاك الطاقة بشكل أكبر في حال وجود عقدتي هجوم، وفي حال زيادة عدد عقد الهجمات من محطّات الهجمات أو من عقد التحسّس ذاتها بإجراء هجمات حجب الخدمة الموزّع DDoS سيؤدي إلى استهلاك أكبر بالطاقة لنقاط الوصول APs حتى تفريغ كامل طاقتها وتوقفها عن العمل، كما أوضحت النتائج زيادة كبيرة في معدّل خسارة الرزم PLR وزمن وصول الرزم من نهاية إلى نهاية، ونتيجةً لذلك توقف كامل الشبكة عن العمل.

نقترح في العمل المستقبلي استخدام نهج أكثر عدوانية مثل زيادة عدد الرزم في الدقيقة التي يرسلها المهاجم إلى وحدة التحكم ودراسة العلاقة بين أداء الشبكة وموضع المهاجم، حيث يكمن الهدف النهائي في تطوير خوارزميات للكشف المبكر عن هذه الأنواع من الهجمات. كما نقترح استخدام خوارزميات تعلّم الآلة Machine Learning وخوارزميّات التعلّم العميق Deep Learning في كشف هذا النوع من الهجمات والتنبؤ بها في الزمن الحقيقي Real Time Prediction. حيث تتم الاستفادة من ميّزة شبكات SDN في فصل مستوي التحكم عن مستوي البنية التحتية (مستوي البيانات) مما يسمح بالتحكم والإدارة المركزيتين للشبكة.

الجدول (7) مقارنة النتائج

البحث	نوع الهجمات	الآلية المستخدمة	نسبة تسليم الرزم PDR	نسبة فقد الرزم PLR	متوسط التأخير من نهاية إلى نهاية [ms]
(Segura et al., 2019)	FFR – FDFF – FNI	تحليل تدفق المعطيات	17%	83%	Up to 900
(Segura et al., 2020)	FDFF – FNI	اكتشاف نقطة التغيير CP	%4	96%	X
هذا البحث	FFR – FDFF – FNI	تحليل تدفق المعطيات	1.45%	98.55%	12016

الجدول (8) قائمة بأهم المصطلحات المستخدمة

الاختصار	المصطلح باللغة الإنكليزية	المصطلح باللغة العربية
WSN	Wireless Sensor Networks	شبكات الحساسات اللاسلكية
SDN	Software-Defined Networks	الشبكات المعرّفة برمجيّاً
SDWSN	Software-Defined Wireless Sensor Networks	شبكات الحساسات اللاسلكية المعرّفة برمجيّاً
IoT	Internet of Things	إنترنت الأشياء
DoS Attack	Denial of Service Attack	هجوم حجب الخدمة
DDoS Attack	Distributed Denial of Service Attack	هجوم حجب الخدمة الموزّع
CP	Change point	نقطة التغيير
HHT	Hilbert–Huang Transform	تحويل هيلبرت-هوانغ
CNN	Convolutional Neural Network	الشبكة العصبونية التلافيفية
ML	Machine Learning	تعلّم الآلة
DL	Deep Learning	التعلّم العميق
FFR	False Flow Request	طلب التدفّق الخاطئ
FDFF	False Data Flow Forwarding	توجيه تدفّق البيانات الخاطئة
FNI	False Neighbor Information	معلومات الجوار الخاطئة
ICMP	Internet Control Message Protocol	بروتوكول التحكم برسائل الإنترنت
TCP	Transmission Control Protocol	بروتوكول التحكم بالإرسال
UDP	User Datagram Protocol	بروتوكول برقية معطيات المستخدم
PDR	Packet Delivery Ratio	نسبة تسليم الرزم
PLR	Packet Loss Ratio	نسبة فقد الرزم
E2EAD	Average End to End delay	متوسط التأخير من نهاية إلى نهاية
RTT	Round-Trip Time	مقاييس زمن الرحلة
AP	Access Point	نقطة الوصول

التمويل: هذا البحث ممول من جامعة دمشق وفق رقم التمويل (501100020595).

References:

1. Ahmad, I., Namal, S., Ylianttila, M., and Gurtov, A. (2015). Security in Software Defined Networks: A Survey. IEEE Communications Surveys & Tutorials, 17(4), 2317–2346. DOI: https://doi.org/10.1109/comst.2015.2474118

2. Ahmed, N., Ngadi, A., Sharif, J. M., Hussain, S., Uddin, M., Rathore, M. S., Iqbal, J., Abdelhaq, M., Alsaqour, R., Sajid Ullah, S., and Tul Zuhra, F. (2022, October, 17). 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. DOI: https://doi.org/10.3390/s22207896

3. Dludla, A. G., Abu-Mahfouz, A. M., Kruger, C. P., and Isaac, J. S. (2013, May). Wireless sensor networks testbed: ASNTbed. Proceedings of the 2013 IEEE IST-Africa Conference and Exhibition (IST-Africa), Nairobi, Kenya, 1–10.

4. Fawcett, L., Scott-Hayward, S., Broadbent, M., Wright, A., and Race, N. (2018). Tennison: A Distributed SDN Framework for Scalable Network Security. IEEE Journal on Selected Areas in Communications, 36(12), 2805-2818. DOI: https://doi.org/10.1109/jsac.2018.2871313

5. Jurado-Lasso, F. F., Marchegiani, L., Jurado, J. F., Abu-Mahfouz, A. M., and Fafoutis, X. (2022, February, 22). A Survey on Machine Learning Software-Defined Wireless Sensor Networks (ML-SDWSNs): Current Status and Major Challenges. IEEE Access, 10, 23560-23592, DOI: https://doi.org/10.1109/ACCESS.2022.3153521

6. Kgogo, T., Isong, B., and Abu-Mahfouz, A. M. (2017). Software defined wireless sensor networks security challenges. 2017 IEEE AFRICON, Cape Town, South Africa. DOI: https://doi.org/10.1109/afrcon.2017.8095705

7. Letswamotse, B. B., Malekian, R., Chen, C. Y., and Modieginyane, K. M. (2018, September). Software Defined Wireless Sensor Networks (SDWSN): A Review on Efficient Resources, Applications and Technologies. Journal of Internet Technology, 19(5), 1303-1313. DOI: https://doi.org/10.3966/160792642018091905003

8. Liu, Y., Sun, D., Zhang, R., and Li, W. (2023, May, 14). A Method for Detecting LDoS Attacks in SDWSN Based on Compressed Hilbert–Huang Transform and Convolutional Neural Networks. Sensors Journal 2023, 23(10), 4745. DOI: https://doi.org/10.3390/s23104745

9. Mallick, C., and Satpathy, C. (2018). Challenges and Design Goals of Wireless Sensor Networks: A Sate-of-the-art Review. International Journal of Computer Applications, 179(28), 42-47. DOI: https://doi.org/10.5120/ijca2018916667

10. Mostafaei, H., and Menth, M. (2018, June). Software-Defined Wireless Sensor Networks A Survey. Journal of Network and Computer Applications, 119(C), 42–56. DOI: https://doi.org/10.1016/j.jnca.2018.06.016

11. Sarkunavathi, A., and Srinivasan, V. (2021). A Scrutinized study on DoS attacks in Wireless Sensor Networks and need of SDN in Mitigating DoS attacks. 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India. DOI: https://doi.org/10.1109/iccci50826.2021.9402459

12. Segura, G. A. N., Margi, C. B., and Chorti, A. (2019). Understanding the Performance of Software Defined Wireless Sensor Networks under Denial of Service Attack. Open Journal of Internet of Things (OJIOT), 5(1), 58-68.

13. Segura, G. A. N., Skaperas, S., Chorti, A., Mamatas, L., and Margi, C. B. (2020). Denial of Service Attacks Detection in Software-Defined Wireless Sensor Networks. 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland. DOI: https://doi.org/10.1109/iccworkshops49005.2020.9145136

14. Sharma, U. and Bahl, N. (2017, May). A Review on Security Issues and Attacks in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science (IJARCS), 8(4), 387-391. DOI: https://doi.org/10.26483/ijarcs.v8i4.3784

15. Yin, D., Zhang, L., and Yang, K. (2018). A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework. IEEE Access, 6, 24694–24705. DOI: https://doi.org/10.1109/access.2018.2831284

16. Zanella, A., Bui, N., Castellani, A., Vangelista, L., and Zorzi, M. (2014). Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1(1), 22–32. DOI: https://doi.org/10.1109/jiot.2014.2306328