مجلة جامعة دمشق للعلوم الهندسية
المجلد 42 العدد (3): 13-32

Damascus University Journal for Engineering Sciences
V42 (3): 13-32

تطوير خوارزميّة تعتمد على تعلّم الآلة لكشف ومنع هجمات حجب الخدمة في شبكات SDWSN

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

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

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

الملخّص:

شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN هي نموذج تم تطويره مؤخراً للتحكم الديناميكي والآمن في تطبيقات انترنت الأشياء IoT، حيث توظّف مزايا الشبكات المعرّفة برمجيّاً SDN في سهولة إدارة وتكوين الشبكة بسبب الفصل بين مستويات التحكم والبيانات، من أجل معالجة التحديات المتأصلة التي تواجهها شبكات الحسّاسات اللاسلكية WSN. ومع ذلك فإن شبكات SDWSN ليست محصّنة ضد التحديات والتهديدات الناشئة عن عمليات اقتحام الشبكة، كما أنّه لا توجد آلية نشطة لمراقبة الشبكة وجعلها في حالة تأهب استباقي في جميع الأوقات. كما تُعد هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS تهديداً كبيراً للأمن في هذه الشبكات، حيث يمكن أن تطغى على الشبكة بحركة المرور، مما يمنع المستخدمين الشرعيين من الوصول إلى الشبكة وتعطيل الخدمات الحيوية للشبكة مثل الاتصالات ونقل المعطيات والتحكّم والمراقبة، والتي تسبب خسائر مالية وتشغيلية كبيرة.

تقترح هذه الدراسة تنفيذ خوارزمية قائمة على تعلّم الآلة لاكتشاف ومنع هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS في شبكات SDWSN، حيث تستخدم الخوارزمية مجموعة متنوعة من السمات، مثل نوع الرزمة وحجم الرزمة ومعدل الرزمة ومصدر ووجهة الرزمة وعدد من السمات المحسوبة إحصائياً لتدريب المصنّف الذي يمكنه التمييز بين حركة المرور الحميدة وحركة المرور الضارّة والناتجة عن الهجمات. تظهر النتائج أنّه يمكن للخوارزمية المقترحة اكتشاف ومنع هجمات حجب الخدمة بمعدل اكتشاف مرتفع، مما ينعكس على الأداء العام للشبكة، كما أنّها قابلة للتطوير والنشر بسهولة في شبكات SDWSN مما يقدّم مساهمة كبيرة في مجال أمن هذه الشبكات.

الكلمات المفتاحية: شبكات الحسّاسات اللاسلكية المعرفة برمجيّاً (SDWSN)، الشبكات المعرّفة برمجيّا (SDN)، شبكات الحسّاسات اللاسلكية (WSN)، إنترنت الأشياء (IoT)، تعلّم الآلة، هجمات حجب الخدمة (DoS)، هجمات حجب الخدمة الموزّع (DDoS)، الأمان، الكشف، الأداء.

تاريخ الإيداع:2023/8/24
تاريخ القبول: 2023/10/11

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

Develop a Machine Learning Based Algorithm to Detect and Prevent DoS and DDoS Attacks in SDWSN

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

[*1] Postgraduate Student, Eng, 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: 24/8/2023
Accepted: 11/10/2023

Abstract:

Software Defined Wireless Sensor Network (SDWSN) is a network paradigm recently developed for dynamic and secure control for Internet of Things (IoT) applications. Where it employs the ease of network management and configuration of Software Defined Network (SDN)due to the separation between control and data planes, in order to address the inherent challenges that faced Wireless Sensor Networks (WSN). However, SDWSNs are not immune against the challenges and threats that arise from network intrusions, and there is no active mechanism in place to monitor the network and make it in proactive alert at all times. Also, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are major threats to security in SDWSN networks, as these attacks can overwhelm the network with traffic, preventing legitimate users from accessing the network and disrupt critical network services such as communications, data transmission, control, and monitoring, which cause significant financial and operational loss.

This study proposes implementation of a machine learning-based algorithm to detect and prevent DoS and DDoS attacks in SDWSNs. The algorithm uses a variety of features, such as packet size, packet rate, packet source, packet destination and a number of statistical calculated features to train a classifier that can distinguish between benign traffic and malicious traffic generated by attacks. The results show that the proposed algorithm can detect and prevent DoS and DDoS attacks with high detection rate, which is reflected in the overall performance of the network. It is also easily scalable and deployable in SDWSNs, which makes a significant contribution to the security of these networks.

Keywords: Software Defined Wireless Sensor Network (SDWSN), Software Defined Network (SDN), Wireless Sensor Network (WSN), Internet of Things (IoT), Machine Learning (ML), Denial of Service (DoS), Distributed Denial of Service (DDoS), Attacks, Security, Detection, Performance.

ومنطقها عن أجهزة إعادة التوجيه (Kreutz et al., 2013, 55)، ونظراً لوجود واجهات الربط المفتوحة بين الأجهزة والتطبيقات ووحدات التحكّم، فمن السهل شن هجمات على الشبكة مثل هجمات حجب الخدمة DoS ضد عقد أجهزة التحسّس ووحدة التحكّم التي تستهدف استهلاك مواردها (Sezer et al., 2013, 36)، كما يمكن الهجوم على أجهزة إعادة التوجيه لإسقاط أو إبطاء أو العبث بالرزم المرسلة، وبالتالي يمكن للمهاجم إضافة حركة مرور مزورة لزيادة التحميل على كل من أجهزة مستوي التحكّم مثل المتحكّم وأجهزة مستوي البيانات مثل المبدّلات والموجّهات وعقد التحسّس وما إلى ذلك في حالة عدم وجود آلية كشف (Yan et al., 2011, 810).

1- المشكلة:

أدى النمو السريع للأجهزة الذكية والتقنيات اللاسلكية إلى تطوير شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN واستخدامها على نطاق واسع في عدد من التطبيقات مثل تطبيقات انترنت الأشياء IoT، وتُعد هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS تهديداً كبيراً للأمن في هذه الشبكات، حيث يمكن أن تطغى هذه الهجمات على الشبكة عبر إغراقها بحركة المرور، مما يمنع المستخدمين الشرعيين من الوصول إلى الشبكة وتعطيل الخدمات الحيوية للشبكة مثل الاتصالات ونقل المعطيات والتحكّم والمراقبة.

تقترح هذه الدراسة خوارزمية قائمة على تعلّم الآلة Machine Learning (ML) لاكتشاف ومنع هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS في شبكات SDWSN، حيث تستخدم الخوارزمية المقترحة مجموعة متنوعة من السمات، مثل نوع الرزمة وحجم الرزمة ومعدل الرزمة ومصدر ووجهة الرزمة وعدد من السمات المحسوبة إحصائياً لتدريب المصنّف الذي يمكنه التمييز بين حركة

المقدمة:

جلب استخدام نموذج الشبكات المعرّفة برمجيّاً Software Defined Network (SDN) في شبكات الحسّاسات اللاسلكية Wireless Sensor Network (WSN) فوائد هائلة للعديد من التطبيقات والحلول مثل المحاكاة الافتراضية لوظائف الشبكة Network Functions Virtualization (NFV) ومراكز البيانات وشبكات المؤسسات والعديد من تطبيقات انترنت الأشياء IoT، مما أثار اهتمام الباحثين والشركات المطوّرة والمصنّعة في مجال شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً Software Defined Wireless Sensor Network (SDWSN) (Mathebula et al., 2019, 1288). إذ تُستخدم هذه الشبكات في بيئات مختلفة مثل شبكات الجامعة ومراكز البيانات والصناعات التحويلية ومقرات الجيش وغيرها من الأماكن الحسّاسة، وبالنظر إلى أن البيانات المنقولة بين العقد وأجهزة التحكّم في الشبكة يمكن أن تكون حسّاسة في اتخاذ القرارات، فإنّه يعد أمن هذه الشبكات مجالاً نشطاً للبحث، حيث يستخدم التشفير المتماثل والتشفير غير المتماثل والتشفير الهجين لمنع الاختراقات ضمن شبكات SDWSN في الممارسات العملية، بينما تُستخدم أنظمة كشف التسلل IDS للكشف عن الاختراقات في هذه الشبكات (Wa Umba et al., 2019, 2220). وعلى الرغم من قدرة نموذج شبكات SDWSN في التغلّب على القيود المتأصلة المرتبطة بشبكات WSN مثل القدرة الحسابية المحدودة وسعة تخزين البيانات وعرض نطاق الإرسال والتحديات التقنية المتعلقة بالمرونة والأمن، ومع الأخذ بعين الاعتبار أنّ تكوين الإطار المعماري لشبكات SDWSN من تحكّم مركزي يسمح بتنفيذ المزيد من تدابير الأمان المكثفة للموارد، إلّا أنّ هذا النموذج من الشبكات يواجه العديد من التحديات الأمنية الجديدة (Kobo et al., 2017, 1872).

إن إحدى السمات المميزة في مركزية شبكات SDWSN هي التحول الجذري لمعمارية الشبكة عن طريق فصل ذكاء الشبكة

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

العميق Deep Learning (DL) وخوارزميّة نموذج Naïve Bayes (NB). حيث تشتمل وحدة تحكّم على ثلاث وظائف رئيسية هي جمع التدفّق الذي يجمع معلومات الشبكة، وكاشف الشذوذ الذي يكتشف أي سلوك غير طبيعي في الشبكات، وعامل التخفيف من الشذوذ الذي يعمل على مواجهة الشذوذ المكتشف. تُظهر النتائج أن نهج NB هو الأنسب لتطبيقات شبكات SDWSN حيث قامت وحدة التحكّم بتقييد إمكانيات الذاكرة، كما أنها تُظهر متطلبات أقل لاستهلاك الطاقة. ومع ذلك أظهرت خوارزميّة DT أفضل أداء إجمالي لاكتشاف الحالات الشاذة وخاصّةً للتطبيقات الحسّاسة للتأخير.

بينما قام (Indira et al., 2020, 275) بتصميم نظام كشف التسلّل IDS يستفيد من مزايا خوارزميّة Salp Swarm Optimization (SSO) في اختيار السمات المثالية لكاشف التسلّل، واستخدامها لتحسين كفاءة اكتشاف مصنّف خوارزميّة الغابة العشوائية Random Forest (RF)، حيث قاموا بتحليل الأنشطة غير الطبيعية في الشبكة وتحديد الهجمات المعروفة وغير المعروفة، بالإضافة إلى تقييم موثوقية النظام المقترح من حيث التأخير ونسبة التسليم واستهلاك الطاقة ومعدّل النقل (الإنتاجية).

2-2- شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً:

تحتاج طوبولوجيا شبكات الحسّاسات اللاسلكية WSN غير المعتمدة على الشبكات المعرّفة برمجيّاً SDN إلى آليات لاستكشاف البنية التحتية للشبكة، حيث تعتمد على رسائل البث التي ترسل بشكل دوري من قبل كل عقدة ضمن نطاق إرسالها لتحديد جوارها. تضيف هذه العملية عبئاً كبيراً على الشبكة وتستهلك أيضاً الكثير من الطاقة. فبعد الحصول على طوبولوجيا الشبكة، يمكن اتخاذ العديد من القرارات ومنها على سبيل المثال قرارات توجيه حركة المرور في الشبكة، ولتنفيذ هذه القرارات تحتاج كل عقدة إلى تخزين جداول التوجيه داخل المرور المشروعة أو الحميدة وحركة المرور الناتجة عن الهجمات.

2- الأسس النظرية للبحث:

2-1- الدراسات المرجعية:

قدّم (Chen et al., 2020, 122) نظام اكتشاف هجمات حجب الخدمة الموزّع DDoS قائم على تعلّم الآلة ML في شبكة تتضمن تجهيزات انترنت الأشياء IoT، حيث قاموا بنشر العديد من نقاط التحسّس اللاسلكية في ثمانية أقطاب لجمع البيانات، ثم استخرجوا السمات بناءً على تنفيذ هجمات DDoS متعددة بما في ذلك فيضان بروتوكول ICMP وفيضان التزامن SYN لبروتوكول TCP وفيضان بروتوكول UDP مع فترات زمنية مختلفة. أظهرت النتائج أن خوارزميّة شجرة القرار Decision Tree (DT) قد حققت دقة تزيد عن 97٪.

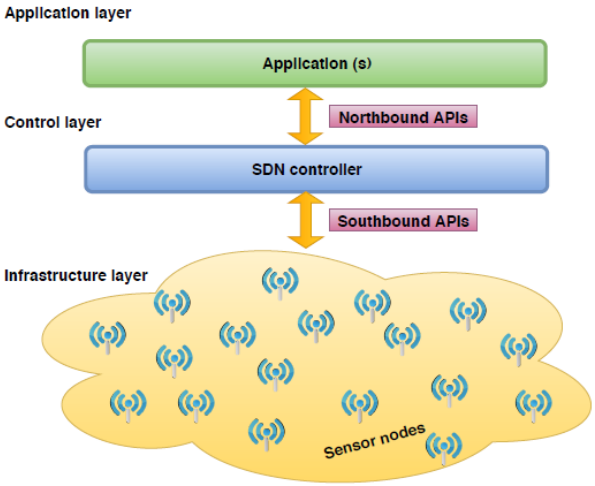
فيما اقترح (Kgogo, 2019) نظام لكشف التسلّل IDS باستخدام خوارزميات تعلّم الآلة ML لتحديد الخوارزميّة التي تعمل بشكل أفضل في اكتشاف التهديدات والهجمات في شبكات SDWSN، حيث كانت الخوارزميات المختبرة هي خوارزميّة شجرة القرار Decision Tree (DT) وخوارزميّة آلة دعم المتّجه Support Vector Machines (SVM) وخوارزميّة الانحدار اللوجستي Logistic Regression (LR). أظهرت النتائج أن نموذج SVM هو الأكثر فاعلية في اكتشاف كل من الحالات الطبيعية والشاذة يليه نموذج DT، ومع ذلك فإن نموذج DT هو الأكثر كفاءة وفعالية في الكشف عن اختراق الشبكة في الوقت الفعلي ويمكنه أن يتفاعل مع شبكات SDWSN مع أي تطفل على الفور.

وقام (Wa Umba et al., 2019, 2220) بتقديم دراسة مقارنة لثلاثة مناهج للذكاء الاصطناعي لأنظمة كشف التسلل IDS في شبكات SDWSN هي خوارزميّة شجرة القرار DT والتعلّم

الشكل (1) نظرة عامة على نموذج شبكات SDWSN [9]

3-3- بنية شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً:

يوضّح الشكل (2) البنية العامة لشبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN، والتي تتكون من المستويات المنطقية الآتية: مستوي البنية التحتية (مستوي البيانات) – مستوي التحكّم – مستوي التطبيقات.



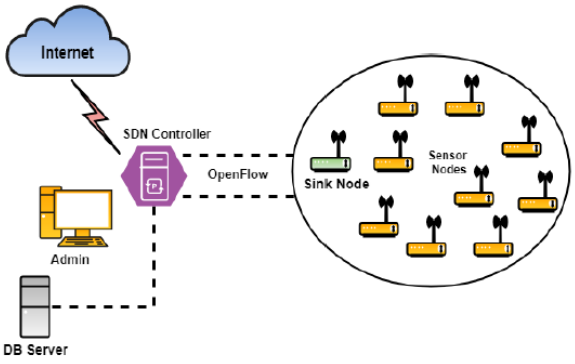
الشكل (2) البنية العامّة لشبكات SDWSN [11]

يتضمن مستوي البنية التحتية لشبكات SDWSN مجموعة من عقد التحسّس التي تقوم بالتحسّس وتعيد توجيه البيانات في الشبكة، بينما يتضمن مستوي التحكّم وحدة التحكّم Controller التي تتحكّم في كامل الشبكة، أمّا مستوي التطبيقات فيتضمن تطبيقات متنوعة مثل تطبيقات التوجيه (Ahmed et al., 2022, 7896).

يوضّح الشكل (3) مكوّنات المستويات المنطقية لشبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN، حيث يمكن اعتبار معمارية شبكات SDWSN امتداداً لمعمارية نموذج شبكات SDN، كما تسمح بدمج بروتوكولات شبكات SDN شائعة الاستخدام (مثل بروتوكول التدفّق المفتوح OpenFlow) لتحديد قواعد إعادة توجيه الرزمة، كما أن شبكات SDWSN ذاكرتها المحدودة وحساب مسار العقد الأخرى (Ahmed et al., 2022, 7896).

أمّا في شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN يتم نقل العديد من المهام التي تحتاج للكثير من الموارد إلى وحدة التحكّم لأنها تحتوي على مصدر طاقة ورؤيا على كامل الشبكة وموارد أفضل. فمثلاً لا تحتاج العقد إلى إرسال رسالة بث بشكل دوري لاكتشاف طوبولوجيا الشبكة ويتم اتخاذ قرارات التوجيه بواسطة وحدة التحكّم وبالتالي لا تتطلب العقد تخزين معلومات التوجيه داخل جداول التوجيه الخاصة بها. علاوة على ذلك يمكن لوحدة التحكّم أيضاً ضبط نطاق الإرسال لكل عقدة لتقليل تداخل الاتصال بين العقد، يمكن تنفيذ هذه المهام بواسطة وحدة التحكّم في شبكات SDWSN للحفاظ على الطاقة المتبقية في العقد (Ahmed et al., 2022, 7896).

يوضّح الشكل (1) نظرة عامّة على نموذج شبكات SDWSN، حيث تنفّذ عقد التحسّس وظائف إعادة التوجيه فقط ويكون ذكاء الشبكة في وحدة تحكّم نموذج شبكات SDN، كما تكون 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).



رسائل المراقبة للحصول على معلومات الشبكة، مثل مستويات الطاقة لعقد التحسّس أو المسافة من محطّة قاعدة البيانات وقائمة الجوار للعقد، ومعلمات حالة الارتباط مثل جودة الرابط وزمن الاستجابة وما إلى ذلك (Kobo et al., 2017, 1881).

يمكن التمييز بين طرق التحكّم في شبكات SDWSN وفق فئتين مختلفتين (Ahmed et al., 2022, 7896):

وحدة تحكّم متصلة مباشرة Directly connected controller تتصل وحدة التحكّم مباشرة بجميع عقد الاستشعار في هذه الفئة، ويتطلب المتحكّم وجود قناة منفصلة للتحكّم في الحركة.

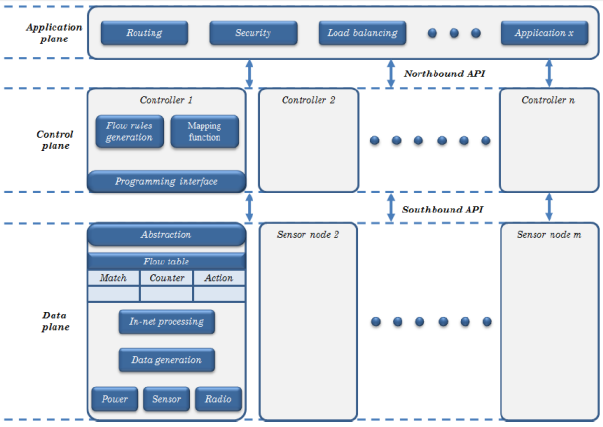
وحدة تحكّم متصلة بشكل غير مباشر Indirectly connected controller تتصل وحدة التحكّم بعقد الحسّاسات عبر عقد أخرى، أي باستخدام اتصالات متعددة القفزات، يقوم المتحكّم بالتحكّم بحركة مرور البيانات عبر البنية الأساسية للشبكة الرئيسية.

4-3- الهجمات الأمنية في شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً:

يقدم نموذج شبكات SDN بعض الحلول لأمن شبكات WSN والتي يمكن دمجها مباشرة في أمان شبكات SDWSN على اعتبار أنّ مركزية التحكّم تبسّط إدارة الأمن وتؤدي إلى تقليل قيود الموارد على العقدة نفسها، مما يسمح بتنفيذ الأمان (Pritchard et al., 2017, 168). وواحدة من أهم الميزات التي تقدمها شبكات SDN إلى شبكات WSN هي حقيقة أن عقدة التحسّس لا يمكنها قبول أوامر التحكّم بسبب فصل منطق التحكّم، ولهذا يصبح من الصعب استخدام عقد التحسّس لإجراء هجمات ضارّة على الشبكة، على الرغم من أنه لا يزال من الممكن استخدام هذه العقد كبوابات لهجمات مختلفة (Kobo et al., 2017, 1883).

من أجل تحديد الحلول الأمنية التي يمكن تكييفها من شبكات SDN وشبكات WSN في نموذج شبكات SDWSN، من المهم تحديد التهديدات الأمنية الموجودة في كل من شبكات تمتلك مستوى بيانات أكثر تعقيداً بسبب وجود العديد من العقد وبسبب عدم تجانس العقد (Buzura et al., 2020, 4779).

تشكّل عقد التحسّس أساس مستوى البنية التحتية أو مستوى البيانات، وتتألف هذه العقد من مكونات عتادية (مثل وحدة طاقة ووحدة التحسّس ووحدة الاتصال الراديوي) فيما يتكون جزء البرامج من جداول التدفّق وعناصر التحسّس والمعالجة. تقوم وحدة التحسّس بتوليد حركة المرور التي تمرّر بعد ذلك إلى المعالج، ويمكن أن تكون المعالجة داخل الشبكة هي تجميع البيانات في عقد التحسّس أو دمج البيانات في عقد المفرّغ (Kobo et al., 2017, 1881).



الشكل (3) المستويات المنطقية لشبكات SDWSN [7]

فيما تلعب وحدة التحكّم في شبكات SDWSN دوراً حاسماً للغاية لأنها تحمل ذكاء الشبكة بالكامل، وتتركز وظائفها الأساسية في إنشاء قواعد التدفّق ووظائف رسم الخرائط لواجهات البرمجة. وتستخدم شبكات SDWSN عادةً وحدة تحكّم مدمجة متّصلة مع عقدة المفرّغ Sink node عبر اتصال تسلسلي، كما تتصل هذه العقدة مع باقي عقد التحسّس الأخرى عبر واجهة اتصال لاسلكية. وتكون عقدة المفرّغ في حالات أخرى هي محطّة قاعدية تضم جهاز التحكّم وتكون الطبقة الوسيطة من وحدة التحكّم مسؤولة عن وظائف ومعلومات التعيين وتعريف جدول التدفّق. تتحكّم وحدة التحكّم في الشبكة وتديرها وتحافظ على تحديث حالة الشبكة باستخدام

التي تركز على أجهزة الشبكة مثل المبدّلات والموجّهات أو عناصر التحكّم، كما يجب أن يكون الأمان مدمجاً في بنية شبكات SDWSN نفسها (Kreutz et al., 2013, 56) وأن يكون متوافقاً مع متطلبات التصميم الأخرى (Kobo et al., 2017, 1883).

يوضح الجدول (1) التهديدات الأمنية المرتبطة بكل من مستويات شبكات SDN وطبقات شبكات WSN (Pritchard et al., 2017, 172).

الجدول (1) التهديدات الأمنية المرتبطة بكل من مستويات شبكات SDN وطبقات شبكات WSN [12]

طبقة شبكة WSN	مستوي شبكة SDN	التهديد
التطبيقات	التطبيقات	ضعف المصادقة والتحكّم
		إدراج قواعد التدفّق الاحتيالية
		ضعف التحكّم في الوصول
		التطبيقات الضارة
		هجمات حجب الخدمة DoS
		هجمات الواجهة الشمالية
النقل	التحكّم	هجمات حجب الخدمة DoS
الشبكة		الدخول غير المرخص
		قابلية التوسع وعدم المتاحية
		وحدة تحكّم معيبة أو ضارة
الوصل	البيانات	الدخول غير المرخّص
		القواعد الاحتيالية
		تدفّقات حركة المرور المزورة
		التعويم Flooding
		الانتحال Spoofing
الفيزيائية		هجمات الواجهة الجنوبية
		التشويش Jamming
		التلاعب Tampering
		سيبل Sybil
		جهاز تحكّم مخترق / مسروق

SDN وشبكات WSN. حيث يتكون مستوي التطبيقات Application Plane لمعمارية شبكات SDWSN من طبقة التطبيقات في مكدس شبكات WSN ومستوي التطبيقات في نموذج شبكات SDN، وغالباً ما يكون هذا المستوي عرضة للثغرات الأمنية مثل تحدّيات المصادقة والترخيص (Ahmad et al., 2015) ونقص آليات الثقة (Kreutz et al., 2013, 55) والتهديدات من تطبيقات الشبكة. ومن الحلول المقترحة لمعالجة هذه التهديدات هي تنفيذ نماذج للتحقق أو تنفيذ حلول التشفير لتأمين اتصالات الواجهة الشمالية (Pritchard et al., 2017, 169).

بينما يتكون مستوي التحكّم Control Plane لمعمارية شبكات SDWSN من طبقة النقل وطبقة الشبكة في مكدس شبكات WSN ومستوي التحكّم في نموذج شبكات SDN، ويمكن تطبيق حلول التشفير في شبكات WSN على وحدة التحكّم لتأمين مستوي التحكّم ضد هجمات طبقة النقل وطبقة الشبكة، كما هنالك عدة نماذج تستخدم وحدات تحكّم مخصّصة للحماية من التطبيقات الضارة وزيادة قابلية التوسعة لوحدة التحكّم بهدف التخفيف من هجمات حجب الخدمة DoS (Ahmad et al., 2015).

فيما يتكون مستوي البنية التحتية (أو مستوي البيانات) Data Plane لمعمارية شبكات SDWSN من طبقة ربط المعطيات والطبقة الفيزيائية في مكدس شبكات WSN ومستوي البيانات في نموذج شبكات SDN، ويتم تخفيف معظم نقاط ضعف طبقة ربط المعطيات والطبقة الفيزيائية في شبكات WSN باستخدام نهج SDN لأن عقدة التحسّس قادرة فقط على قبول أوامر التحكّم ولهذا السبب يصعب استخدامها كعقدة ضارّة (Kreutz et al., 2013, 56).

على الرغم من أن بعض الحلول المذكورة أعلاه قد تكون قادرة على تأمين شبكات SDWSN إلى حدٍّ ما، إلّا أنّها ليست حلولاً مثالية، حيث يعتمد معظمها على طرق الأمان الخارجية

et_count_per_second –byte_count_per_second – sfe – ssip – rfip – type

حيث أنّ:

tp_src: يعبّر عن منفذ Port الإرسال.

tp_dst: يعبّر عن منفذ Port الاستقبال.

icmpv4_ck: يعبّر عن التحقق من بروتوكول ICMP.

tcp_ck: يعبّر عن التحقق من بروتوكول TCP.

udp_ck: يعبّر عن التحقق من بروتوكول UDP.

icmp_code: يعبّر عن رقم نوع بروتوكول ICMP.

icmp_type: يعبّر عن نوع بروتوكول ICMP.

flow_duration_sec: يعبّر عن مرور حركة المعطيات بالثانية.

packet_count: يعبّر عن العدد التراكمي للرزم المرسلة.

byte_count: يعبّر عن عدد البايتات المرسلة.

packet_count_per_second: يعبّر عن عدد الرزم المرسلة خلال ثانية واحدة.

byte_count_per_second: يعبّر عن عدد البايتات المرسلة خلال ثانية واحدة.

sfe: يعبّر عن سرعة إدخالات التدفّق (Speed of Flow Entries) ، وهي العدد الإجمالي لإدخالات التدفّق إلى المبدّل في الشبكة N خلال فترة زمنية معينة T.

ssip: يعبّر عن سرعة مصادر العناوين المنطقية (Speed of IP Sources) وهي العدد الإجمالي للعناوين المنطقية الواردة في الشبكة خلال فترة زمنية معينة.

rfip: يعبّر عن نسبة إدخالات التدفّق الثنائي (Ratio of Pair-Flow Entries) وهي العدد الإجمالي لإدخالات التدفّق الواردة في المبدّل.

type: يعبّر عن وجود هجوم حجب خدمة أم لا، حيث تتم الإشارة إلى التدفّق الحميد بالرمز (0) والتدفّق المتولّد من هجوم بالرمز (1).

		العقدة الخبيثة

3- التطبيق العملي والنتائج والمناقشة:

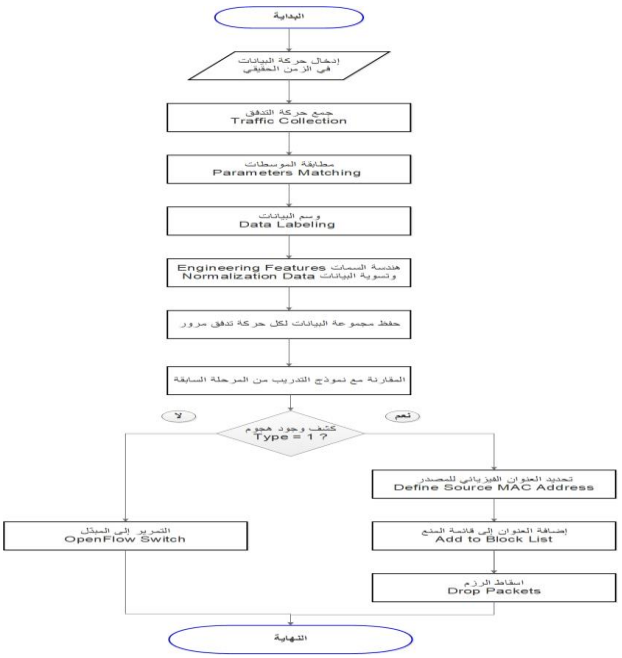
يشمل التطبيق العملي إجراء عملية مضاهاة Emulation باستخدام البرنامج Mininet-WiFi لشبكة حساسات لاسلكية معرّفة برمجياً SDWSN، مع استخدام متحكّم مفتوح المصدر من النوع Ryu-Manager Controller.

يهدف التطبيق العملي إلى تنفيذ الخوارزميّة المقترحة لكشف ومنع هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS المعتمدة على خوارزميات تعلّم الآلة في شبكات SDWSN في الزمن الحقيقي، ودراسة أداء هذه الخوارزميّة المقترحة في تحسين أداء الشبكة، وتوضّح الفقرات التالية المخطط التدفقي للخوارزمية المقترحة ومعاملات بيئة العمل وعملية المضاهاة التي تمّت لإجراء التطبيق العملي، بالإضافة إلى نتائج تحليل أداء الخوارزمية وفق مقاييس خصائص الأداء للشبكة من نسبة توصيل الرزم ومتوسط التأخير من نهاية إلى نهاية ومتوسط استهلاك الطاقة وتحليل مقاييس زمن الرحلة، وتحليل نتائج مقاييس خصائص الأداء لخوارزميات تعلّم الآلة.

3-1- الخوارزميّة المقترحة لكشف ومنع هجمات حجب الخدمة:

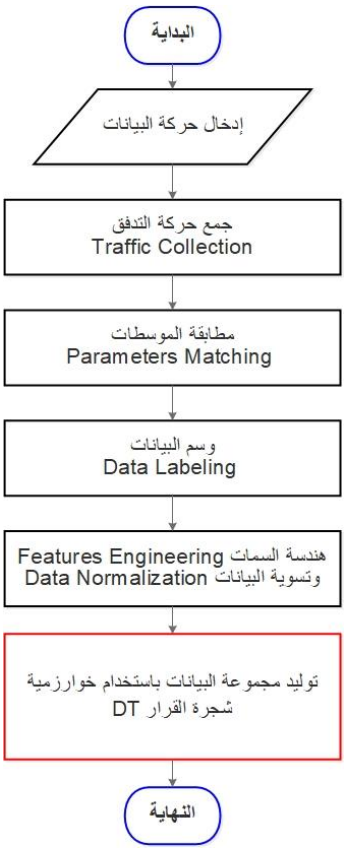
تعتمد الخوارزميّة المقترحة لكشف ومنع هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS في شبكات SDWSN على خوارزميات تعلّم الآلة، ويوضّح الشكل (4) المخطط التدفّقي لعملية جمع مجموعة البيانات المستخدمة في التدريب والمقارنة في الخوارزميّة المقترحة، وذلك باستخدام خوارزميّة شجرة القرار Decision Tree (DT)، واستخدام مجموعة السمات التالية:

tp_src – tp_dst – icmpv4_ck – tcp_ck – udp_ck – icmp_code – icmp_type – flow_duration_sec – packet_count – byte_count – pack-



الشكل (5) المخطط التدفّقي للخوارزميّة المقترحة في كشف ومنع هجمات حجب الخدمة

تعمل الخوارزميّة عن طريق إدخال حركة بيانات جديدة في عمليـة مضـاهاة لشـبكة حساسـات لاسـلكية معرّفـة برمجيـاً SDWSN، وإجراء عملية تبادل للمعطيات بين العقد والمتحكّم وبين ومحطّات الهجمات والمتحكّم كذلك، عن طريق نقاط الوصول ومبدّل التدفّق المفتوح OpenFlow Switch، وجمع حركة دفق البيانات وتخزينها، ثمّ مطابقة الموسطات لبناء مجموعة البيانات الجديدة بعد إجراء هندسة السّمات لهذه البيانات Feature Engineering عبر إجراء عملية مسح الاعمدة غير المطلوبة، وعملية التسوية (التقييس) Normalization لكل عمود من الأعمدة الموجودة في مجموعة البيانات بهدف جعل كافة السّمات ضمن نفس المجال (من 0 إلى 1)، باستخدام القيم العظمى والدنيا التي تم استنتاجها من مجموعة البيانات المولّدة مسبقاً بالشكل (4) والمستخدمة في التدريب والمقارنة ضمن هذه الخوارزميّة المقترحة. ثمّ تخزين مجموعة البيانات الجديدة الخاصّة بحركة البيانات الجديدة في الوقت الحقيقي بشكل آني في ملف خاص



الشكل (4) المخطط التدفّقي لعملية جمع مجموعة البيانات المستخدمة في الخوارزميّة المقترحة

2-4- المخطط التدفّقي للخوارزميّة المقترحة:

يوضّـح الشـكل (5) المخطـط التـدفّقي للخوارزميّـة المقترحـة لكشـف ومنـع هجمـات حجـب الخدمـة DoS وهجمـات حجـب الخدمـة الموزّع DDoS المعتمدة على خوارزميات تعلّم الآلة في شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN.

الجدول (2) 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 (3) 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 الهوائي لعقد التحسّس	3 [dBi]
ربح الهوائي لنقاط الوصول	9 [dBi]
ربح الهوائي لمحطّات 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

بالتنبؤ والكشف عن وجود هجمات حجب الخدمة Predict_Flow.

تعمل الخوارزميّة على كشف وجود هجمات حجب الخدمة عبر استنتاج حقل النمط Type، والذي يحدّد وجود هجوم من عدمه، عن طريق إدخال كل مجموعة بيانات تم حفظها في الملف Predict_Flow، إلى نموذج التدريب المولّد مسبقاً X_Flow_Predict ثمّ استنتاج Y_Flow_Predict الذي يتضمّن حقل النمط Type.

في حال كانت قيمة حقل النمط Type مساوياً للواحد فهذا يعني التحقق والتأكد من وجود هجوم، وعندها يتم البدء بعملية تحديد العنوان الفيزيائي للمهاجم MAC Address وإضافته إلى قائمة المنع Block List وتعديل حقل الإجراء Action في مبدّل التدفّق المفتوح OpenFlow Switch ليصبح اسقاط Drop لكل رزمة واردة إلى المتحكّم من هذا العنوان. أمّا في حال كانت قيمة من حقل النمط Type مساوياً للصفر فهذا يعني التحقق والتأكد من أن الاتصال حميد، وعندها يتم إبقاء حقل الإجراء Action في مبدّل التدفّق المفتوح OpenFlow Switch في حالة تمرير Forward لكل رزمة واردة إلى المتحكّم من هذا العنوان إلى المتحكّم Controller.

نضمن بهذه الخوارزميّة عدم ورود أي هجمات إلى المتحكّم بقيام المبدّل بإسقاط جميع الرزم الواردة الناتجة عن هجمات حجب الخدمة، مما يضمن استمرار عمل المتحكّم وعمل الشبكة.

3-3- معاملات بيئة العمل:

تبيّن الجداول (2) و (3) و (4) المعاملات الأساسية في بيئة العمل المقترحة لسيناريوهات المضاهاة المختلفة، وهي: معاملات البيئة العامة ومعاملات القناة اللاسلكية والهوائيات ومعاملات الطاقة على الترتيب.

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 ترسلها العقدة المصدر إلى عدد الرزم التي تستقبلها العقدة الوجهة (العلاقة 1) وعندما تكون هذه النسبة عالية يمكن القول أنّ الأداء أفضل.

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

حيث أنّ:

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

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

TTP (Total Transmitted Packets): 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 الرزم التي تفشل بالوصول إلى عقدة الوجهة أو المتحكّم، إلى عدد الرزم التي ترسلها العقدة المصدر (العلاقة 2)، ويكون الأداء أفضل عندما تكون هذه النسبة منخفضة.

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

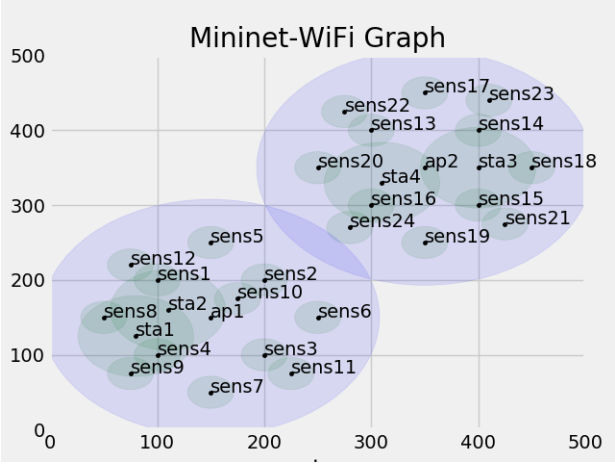
حيث أنّ:

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

الجدول (4) معاملات الطاقة

المعامل	القيمة
الطاقة الابتدائية لعقد التحسّس	10 [Volt]
الطاقة الابتدائية لنقاط الوصول	10 [Volt]
الطاقة الابتدائية لمحطّات الهجمات	10 [Volt]
طاقة الإرسال لعقد التحسّس	3 [dBm]
طاقة الإرسال لنقاط الوصول	30 [dBm]
طاقة الإرسال لمحطّات الهجمات	15 [dBm]
معامل الاستطاعة في حالة الخمول	0.273 [Watt]
معامل الاستطاعة في حالة الارسال	0.380 [Watt]
معامل الاستطاعة في حالة الاستقبال	0.313 [Watt]
معامل الاستطاعة في حالة النوم (التوقف)	0.033 [Watt]

كما يوضّح الشكل (6) التوزيع الثابت للعقد ضمن بيئة العمل، حيث تمّ إسناد الأرقام التسلسلية من sens1 وحتى sens24 لعقد التحسس، وإسناد الأرقام التسلسلية من sta1 وحتى sta4 لمحطات الهجمات، وإسناد الأرقام التسلسلية من ap1 وحتى ap2 لنقاط الوصول، ذلك بهدف تسهيل عملية الترميز لغرض المحاكاة.



الشكل (6) التوزيع الثابت للعقد ضمن بيئة العمل

4-3- مقاييس خصائص الأداء للشبكة:

(Energy Consumption) EC: يعبّـر عـن اسـتهلاك الاستطاعة.

(Time) T: يعبّر عن زمن التشغيل.

(Voltage) V: يعبّر عن الجهد.

(Current) C: يعبّر عن التيار المار في العقدة.

(Factor) F: معامل خاص ببرنامج المضاهاة، ويعبّر عن حالة عمل العقدة.

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 فقدان الرزم.

5-3- مقاييس خصائص الأداء لخوارزميات تعلّم الآلة

على الرغم من القوّة التمثيلية لمصفوفة الالتباس Confusion Matrix في دراسة أداء خوارزميات تعلّم الآلة المعتمدة على التصنيف، إلّا أنها ليست أداة مفيدة جداً من أجل المقارنة بين أنظمة كشف التسلّل IDS، بالتالي يتم تحديد مقاييس أداء مختلفة من حيث متغيرات مصفوفة الالتباس، وذلك عن طريق حساب بعض القيم الرقمية التي يمكن مقارنتها بسهولة، وتجدر الإشارة إلى أنّه يمكن التعبير عن قيم مقاييس الأداء هذه كنسبة مئوية أو ما يعادلها من رقم معياري (رقم بين القيمة 0 والقيمة 1) (Wa Umba et al., 2019, 2224).

نبيّن فيما يلي مقاييس أداء خوارزميات تعلّم الآلة.

معدّل التصنيف Classification Rate (CR): يعرّف على أنه نسبة الحالات المصنّفة بشكل صحيح إلى العدد الإجمالي للحالات (العلاقة 5).

$$CR = \frac{TP+TN}{TP+FP+TN+FN} \quad (5)$$

حيث أنّ:

(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: يُحسب 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. كما يُحسب متوسط التأخير من طرف إلى طرف بحساب متوسط كل تأخير الرزم التي تم إنشاؤها بواسطة شبكة العقد بأكملها (العلاقة 3) ويقاس بالميلي ثانية.

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

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.

$$EC\ [mJ] = T * V * C * F \quad (4)$$

حيث أنّ:

Ryu-Manager Controller، وأربع وعشرون عقدة تحسّس تتصل مع المتحكّم عبر نقطتي وصول مع إجراء عملية تبادل للمعطيات بين العقد والمتحكّم وبين ومحطّات الهجمات والمتحكّم، عن طريق نقاط الوصول ومبدّل التدفّق المفتوح OpenFlow Switch، حيث تمّ شن الهجمات من أربع محطّات.

تمّ جمع وتخزين مجموعة البيانات الجديدة الخاصّة بحركة البيانات الجديدة في الوقت الحقيقي بشكل آني في الملف الخاص بالتنبؤ والكشف عن وجود هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS عبر إجراء عمليات تبادل المعطيات الآتية:

عقد 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.

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

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

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

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

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

7-3- 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

TP (True Positive): وهو الصواب الموجب ويعبّر عن عدد محاولات الاختراق التي تم كشفها بشكل صحيح.

FP (False Positive): وهو الخطأ الموجب ويعبّر عن عدد التنبيهات بوجود محاولات اختراق علماً أن سلوك النّظام كان سليماً.

TN (True Negative): وهو الصواب السالب ويعبّر عن عدد المرات التي تمّ اختبار سلوك النظام إذا كان سليماً عندما يكون السلوك سليماً.

FN (False Negative): وهو الخطأ السالب ويعبّر عن عدد الهجمات التي وقعت على النظام والتي لم يتمكن نظام كشف الاختراق من اكتشافها.

معدّل الكشف Detection Rate (DR): يُحسب على أنّه النسبة بين عدد الهجمات المكتشفة بشكل صحيح والعدد الإجمالي للهجمات (العلاقة 6).

$$DR = \frac{TP}{TP+FN} \qquad (6)$$

معدّل الخطأ الموجب False Positive Rate (FPR): يعبّر عن عدد حالات السلوك السليم التي تمّ اعتبارها محاولة اختراق إلى العدد الكلّي لحالات السلوك السليم (العلاقة 7).

$$FPR = \frac{FP}{FP+ TN} \qquad (7)$$

معدّل الخطأ السالب False Negative Rate (FNR): يعبّر عن عدد حالات السلوك الناتج عن وجود هجوم التي تمّ اعتباره سلوكاً سليماً إلى العدد الكلّي لحالات الهجمات (العلاقة 8).

$$FNR = \frac{FN}{FN+ TP} \qquad (8)$$

6-3- عملية المضاهاة:

تمّ إجراء المضاهاة بهدف دراسة وتحليل أداء الخوارزميّة المقترحة مع وجود مجموعة من هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS التي يتم شنّها من محطّات الهجمات. وذلك في حقل أبعاده [m] 500 X 500 وتوزع ثابت للعقد غير المتحركة، مع وجود متحكّم من النوع

يُلاحظ من الشكلين السابقين أن الخوارزميّة المقترحة قد قدّمت تحسّناً في مقدار استهلاك الطاقة بالمقارنة مع حالة وجود هجمتين حجب خدمة من محطتي هجمات على كل نقطة وصول، وأصبحت مستويات استهلاك الطاقة قريبة من حالة العمل الطبيعية دون وجود الهجمات، وذلك بعد استخدام الخوارزميّة المقترحة في كشف ومنع هجمات حجب الخدمة، مما يطيل عمر الشبكة ويحسّن أداءها.

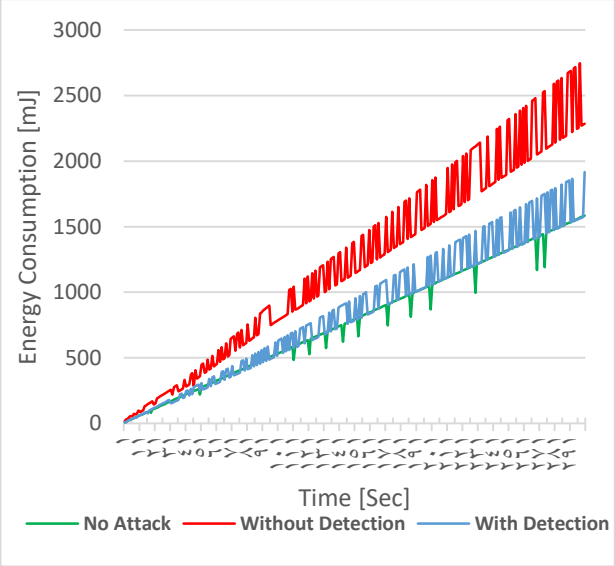
يبيّن الجدول (5) متوسط استهلاك الطاقة لعقد التحسّس خلال زمن التشغيل في حال عدم وجود هجمات حجب الخدمة DoS وفي حالة وجود هجمتين من محطتي هجمات على كل نقطة وصول دون استخدام الخوارزميّة المقترحة في كشف ومنع هجمات حجب الخدمة وفي حالة وجود هجمتين من محطتي هجمات مع استخدام الخوارزميّة المقترحة، ويُلاحظ أن الخوارزميّة المقترحة قد قدّمت تحسّناً في متوسط استهلاك الطاقة لعقد التحسس.

الجدول (5) متوسط استهلاك الطاقة لعقد التحسّس

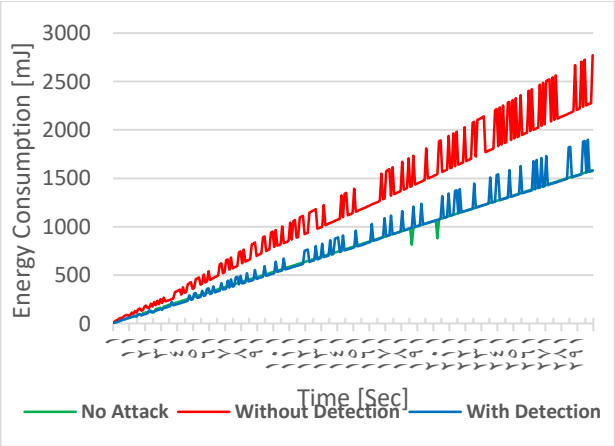
الحالة	القيمة
عدم وجود هجمات	795.921
وجود هجومين على كل نقطة وصول دون استخدام الخوارزميّة المقترحة	1005.973
وجود هجومين على كل نقطة وصول مع استخدام الخوارزميّة المقترحة	924.706

أُجريت المقارنة كذلك 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 في حال عدم وجود هجمات حجب الخدمة وفي حالة وجود هجمتين من محطتي هجمات دون استخدام الخوارزميّة المقترحة في كشف ومنع هجمات حجب الخدمة وفي حالة وجود هجمتين من محطتي هجمات مع استخدام الخوارزميّة المقترحة.

لنقطة الوصول الأولى (AP1) ونقطة الوصول الثانية (AP2) في حال عدم وجود هجمات حجب الخدمة وفي حالة وجود هجمتين من محطتي هجمات دون استخدام الخوارزميّة المقترحة في كشف ومنع هجمات حجب الخدمة وفي حالة وجود هجمتين من محطتي هجمات مع استخدام الخوارزميّة المقترحة.



الشكل (7) استهلاك الطاقة لنقطة الوصول الأولى AP1 بعد استخدام الخوارزميّة المقترحة



الشكل (8) استهلاك الطاقة لنقطة الوصول الثانية AP2 بعد استخدام الخوارزميّة المقترحة

نهاية إلى نهاية) وذلك من زمن يقدّر بحوالي 12016 ميلي ثانية في حالة وجود الهجمات ودون استخدام الخوارزميّة، إلى حوالي 297 ميلي ثانية بعد استخدامها وفقاً للجدول (6) السابق، مما ينعكس إيجاباً على تحسين إدارة موارد الشبكة وتحسين أدائها بما يخدم استخدامها في سياقات وتطبيقات انترنت الأشياء IoT المختلفة، نظراً لأن أن الهدف الرئيسي من هذه التطبيقات هو اتخاذ القرارات بناءً على معطيات صحيحة وبأسرع وقت ممكن.

يبيّن الجدول (7) نتائج مقاييس خصائص أداء خوارزميات تعلّم الآلة المطبّقة على الخوارزمية المقترحة، ونجد من هذا الجدول أن الخوارزميّة المقترحة قادرة على التنبؤ وإيقاف أي هجوم حجب الخدمة DoS أو هجوم حجب الخدمة الموزّع DDoS في الزمن الحقيقي Real Time Prediction حيث بلغت نسبة معدّل الكشف DR مساوياً إلى 100% ومعدّل الخطأ السالب FNR مساوياً إلى الصفر، ودقّة في الكشف تصل إلى 100%، وذلك وفقاً لمقاييس خصائص الأداء لخوارزميات تعلّم الآلة.

الجدول (7) نتائج مقاييس أداء خوارزميات تعلّم الآلة المطبّقة على الخوارزمية المقترحة

CR	DR	FPR	FNR
1.000	1.000	0.000	0.000

يبيّن الجدول (8) نتائج عملية المقارنة بين الخوارزمية المقترحة مع الأبحاث السابقة التي تناولت الحلول المقترحة لكشف هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS في شبكات SDWSN والحلول المقترحة لذلك في نموذج شبكات SDN لاستخدامها في شبكات SDWSN، حيث يوضّح الجدول منهجية الأبحاث التي تمّت المقارنة معها من ناحية نوع الشبكة ونوع الهجمات الخاضعة للدراسة

الجدول (6) نتائج تحليل إحصائيات مقاييس زمن الرحلة

المتوسط / المعامل	حالة عدم وجود هجمات	دون استخدام الخوارزميّة المقترحة	مع استخدام الخوارزميّة المقترحة
عدد الرزم المرسلة	800	800	800
عدد الرزم المستقبلة	791	12	582
عدد الرزم الضائعة	9	788	218
نسبة تسليم الرزم PDR	99%	1.45%	72.74%
نسبة فقد الرزم PLR	1%	98.55%	27.26%
متوسط التأخير من نهاية إلى نهاية	7.099	12016.059	296.855

8-3- الاستنتاجات والمقارنة:

نجد من الشكل (7) والشكل (8) السابقين، أنّ الخوارزميّة المقترحة لكشف ومنع هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS المعتمدة على خوارزميات تعلّم الآلة في شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN قد قدّمت تحسّناً في مقدار استهلاك الطاقة وأنّها أصبحت أقرب لحالة العمل الطبيعية دون وجود الهجمات، كما أن الخوارزميّة قدّمت تحسّنا في مقدار متوسط استهلاك الطاقة لعقد التحسّس في شبكة WSN بالمقارنة مع هذا المقدار في حال وجود هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS وفقاً للجدول (5) السابق، مما يطيل عمر تشغيل الشبكة. بالإضافة إلى أنّ هذه الخوارزميّة قد قدّمت تحسناً كبيراً في نسبة تسليم الرزم PDR حيث لم يتجاوز 1.45% من إجمالي الرزم المرسلة في حالة وجود الهجمات ودون استخدام الخوارزميّة، إلى 72.74% بعد استخدامها، كما قدّمت تحسناً كبيراً في متوسط زمن وصول الرزم من العقدة المصدر إلى نقطة الوصول أو المتحكّم (متوسط التأخير من

والمنهجية أو الطريقة المستخدمة، بالإضافة إلى المقارنة من ناحية الخوارزميّات المستخدمة ومجموعة المعطيات المستخدمة، بالإضافة إلى اهتمامات كل بحث ودقّة الكشف لكلٍّ منها.

الجدول (8) المقارنة بين الخوارزمية المقترحة مع الأبحاث السابقة

البحث	اهتمامات البحث				الخوارزميّات المستخدمة	مجموعة المعطيات	دقة الكشف
	كشف الهجمات	تسليم الرزم	زمن التأخير	استهلاك الطاقة			
(Chen et al., 2020)	√				DT	Smartcity	97.39%
(Kgogo, 2019)	√				DT – SVM – LR	KDD-Cup99	77.43%
(Wa Umba et al., 2019)	√		√		NB – DT – Deep ANN	NSL-KDD	99.98%
(Indira et al., 2020)	√	√	√	√	RF – KNN	NSL-KDD	X
هذا البحث	√	√	√	√	DT	Generated	100%

4- الخاتمة والآفاق المستقبلية:

لكفاءتها وفعاليتها في الكشف عن محاولات اختراق الشبكة في الوقت الفعلي وخاصّةً للتطبيقات الحسّاسة للتأخير.

أوضحت دراسة أداء هذه الخوارزميّة المقترحة أنّها قد قدّمت تحسّناً في مقدار استهلاك الطاقة لنقاط الوصول ومتوسط استهلاك الطاقة لعقد التحسّس في شبكة WSN، وأصبحت مستويات استهلاك الطاقة قريبة من حالة العمل الطبيعية دون وجود الهجمات، مما يطيل عمر تشغيل الشبكة ويحسّن أداءها، كما أنّها قد قدّمت تحسناً كبيراً في نسبة تسليم الرزم PDR وفي متوسط زمن وصول الرزم من العقدة المصدر إلى نقطة الوصول أو المتحكّم (متوسط التأخير من نهاية إلى نهاية)، مما قمنا في هذا البحث باقتراح خوارزميّة تعتمد على تعلّم الآلة لكشف ومنع هجمات حجب الخدمة DoS وهجمات حجب الخدمة الموزّع DDoS في شبكات الحسّاسات اللاسلكية المعرّفة برمجيّاً SDWSN في الزمن الحقيقي، بالاستعانة بمجموعة متنوعة من السمات، مثل نوع الرزمة وحجم الرزمة ومعدل الرزمة ومصدر ووجهة الرزمة وعدد من السمات المحسوبة إحصائياً لتدريب المصنّف الذي يمكنه التمييز بين حركة المرور المشروعة أو الحميدة وحركة المرور الناتجة عن الهجمات. كما تستخدم خوارزميّة شجرة القرار DT نظراً

تعلّم آلة معتمدة على التصنيف في هذه الخوارزمية مثل خوارزميّة الغابة العشوائية Random Forest (RF) وخوارزميّة آلة دعم المتّجه Support Vector Machines (SVM) وخوارزميّة الانحدار اللوجستي Logistic Regression (LR) أو استخدام تقنيات تعلّم الآلة الأكثر تعقيداً مثل التعلّم العميق، وذلك في تطوير بروتوكول توجيه معتمد على الخوارزميّة المقترحة، عبر استخدام نموذج شبكات SDN للتحكم في توجيه البيانات في شبكات WSN ممّا يساعد على تحسين معدّلات استهلاك الطاقة في عقد التحسّس.

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

ينعكس إيجاباً على تحسين إدارة موارد الشبكة وتحسين أدائها بما يخدم استخدامها في سياقات وتطبيقات انترنت الأشياء IoT المختلفة، نظراً لأن أن الهدف الرئيسي من هذه التطبيقات هو اتخاذ القرارات بناءً على معطيات صحيحة وبأسرع وقت ممكن. كما أنّ الخوارزميّة المقترحة قادرة على التنبؤ وإيقاف أي هجوم حجب الخدمة DoS أو هجوم حجب الخدمة الموزّع DDoS في الزمن الحقيقي Real Time Prediction حيث بلغت نسبة معدّل الكشف Detection Rate (DR) مساوياً إلى 100% ومعدّل الخطأ السالب FNR مساوياً إلى الصفر.

نقترح في العمل المستقبلي تقييم عمل الخوارزمية مع أكثر من مجموعة معطيات للتحقق من مدى كفاءتها مع السمات المتغيرة لكشف هجمات حجب الخدمة مما يساعد على فهم قيود الخوارزمية وتحسين أدائها. كما نوصي باستخدام خوارزميات

References:

1. Ahmad, I., Namal, S., Ylianttila, M., and Gurtov, A. (2015, Fourthquarter). 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. Buzura, S., Iancu, B., Dadarlat, V., Peculea, A., and Cebuc, E (2020, August, 24) Optimizations for Energy Efficiency in Software-Defined Wireless Sensor Networks. Sensors Journal 2020, 20(17), 4779. DOI: https://doi.org/10.3390/s20174779

4. Chen, Y.-W., Sheu, J.-P., Kuo, Y.-C., & Van Cuong, N. (2020, June, 15-18). Design and Implementation of IoT DDoS Attacks Detection System based on Machine Learning. 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 122–127. DOI: https://doi.org/10.1109/eucnc48522.2020.9200909

5. Indira, K., and Sakthi, U. (2020). A Hybrid Intrusion Detection System for SDWSN using Random Forest (RF) Machine Learning Approach. International Journal of Advanced Computer Science and Applications (IJACSA), 11(2), 275-284. DOI: https://doi.org/10.14569/IJACSA.2020.0110236

6. Kgogo, A. T. (2019). Intrusion detection system in software defined wireless sensor networks. Master thesis in Computer Science at the North West University, Potchefstroom, South Africa.

7. Kobo, H. I., Abu-Mahfouz, A. M., & Hancke, G. P. (2017, February). A survey on software-defined wireless sensor networks: Challenges and design requirements. IEEE Access, 5, 1872–1899. DOI: https://doi.org/10.1109/ACCESS.2017.2666200

8. Kreutz, D., Ramos, F. M. V., & Verissimo, P. (2013, August, 13). Towards secure and dependable software-defined networks. Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. 55–60. DOI: https://doi.org/10.1145/2491185.2491199

9. Letswamotse, B. B., Malekian, R., Chen, C. Y., and Modieginyane, K. M. (2018, September, 01). 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

10. Mathebula, I., Isong, B., Gasela, N., and Abu-Mahfouz, A. M. (2019, June, 12-14). Analysis of SDN-Based Security Challenges and Solution Approaches for SDWSN Usage. 2019 IEEE 28th International

Symposium on Industrial Electronics (ISIE), Vancouver, Canada. 1288-1293. DOI: https://doi.org/10.1109/isie.2019.8781268

11. Mostafaei, H., and Menth, M. (2018, October, 01). 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

12. Pritchard, S. W., Hancke, G. P., and Abu-Mahfouz, A. M. (017, July, 24-26). Security in software-defined wireless sensor networks: Threats, challenges and potential solutions. 2017 IEEE 15th International Conference on Industrial Informatics (INDIN), Emden, Germany, 168–173. DOI: https://doi.org/10.1109/indin.2017.8104765

13. Sezer, S., Scott-Hayward, S., et al. (2013, July). Are we ready for SDN? Implementation challenges for software-defined networks. IEEE Communications Magazine, 51(7), 36–43. DOI: https://doi.org/10.1109/mcom.2013.6553676

14. Wa Umba, S. M., Abu-Mahfouz, A. M., Ramotsoela, T. D., and Hancke, G. P. (2019, June, 12-14). Comparative Study of Artificial Intelligence Based Intrusion Detection for Software-Defined Wireless Sensor Networks. 2019 IEEE 28th International Symposium on Industrial Electronics (ISIE), Vancouver, Canada, 2220–2225. DOI: https://doi.org/10.1109/isie.2019.8781114

15. Yan, Z., and Prehofer, C. (2011, November). Autonomic Trust Management for a Component-Based Software System. IEEE Transactions on Dependable and Secure Computing, 8(6), 810–823. DOI: https://doi.org/10.1109/tdsc.2010.47