|  |  |  |
| --- | --- | --- |
| **Syrian Arab Republic** |  | **الجمهورية العربية السورية** |
| **Ministry of Higher Education** | **وزارة التعـليــم العـالـــــــــي** |
| **Syrian Private University** | **الجامعة السورية الخاصة** |

تصميم ومحاكاة منظومة توثق في بيئة إنترنت الأشياء باستخدام بروتوكولات RADIUS , Kerberos

**إعداد :  
اميرة بدير**

**ثريا شيخة  
  
إشراف  
د. وسيم جنيدي**

2026

الملخّص (Abstract):

يهدف هذا المشروع إلى تحسين آليات كشف التطفل ضمن شبكات المنازل الذكية من خلال دمج تقنيات التعلّم الآلي مع أنظمة الكشف التقليدية المعتمدة على التواقيع(signature based). تم بناء بيئة افتراضية باستخدام محاكي NS-3 لمحاكاة أجهزة إنترنت الأشياء مثل الكاميرات والحساسات والأجهزة المنزلية، بالإضافة إلى عقدة تمثل المهاجم.

جُمعت آثار حركة المرور في هذه الشبكة بسيناريوهات طبيعية وأخرى هجومية، مع التركيز على هجوم جديد متقدّم يُعرف بـ القفز بين المنافذ (Port-Hopping)، حيث يقوم المهاجم بتغيير المنافذ بشكل عشوائي لتفادي أنظمة الكشف القائمة على القواعد مثل Snort.

تم استخراج ميزات حركة مرور الشبكة وتدريب نموذج يعتمد على خوارزمية XGBoost لتصنيف الحركة إلى سليمة أو خبيثة. أظهرت النتائج أن الحل المقترح حسّن قدرة النظام على كشف الهجمات غير المعروفة مسبقًا، مع دقة عالية ونسبة إنذارات كاذبة منخفضة، مما يؤكد أهمية الجمع بين الأنظمة التقليدية والنماذج المعتمدة على البيانات لحماية شبكات إنترنت الأشياء في المنازل .

This project aims to enhance intrusion detection within smart home networks by integrating a machine-learning component alongside traditional signature-based tools. A virtual IoT environment was built using NS-3, simulating devices such as cameras, sensors, and appliances, along with an attacker node.

After collecting traffic traces (normal and malicious), we focused on detecting a new stealthy attack, Port-Hopping, which changes destination ports dynamically to evade signature-based IDS like Snort.

An ML-based model using XGBoost was trained on extracted flow features to classify traffic as benign or malicious. Results showed that the proposed hybrid solution improved the detection of previously unseen attacks, with high accuracy and low false-positive rate. This demonstrates the potential of combining classical IDS with data-driven models for protecting IoT smart-home networks.

**فهرس المحتويات**

**المصطلحات والتعاريف ........................................................... 6**

**1.المقدمة:...........................................................................11**

**1.الفصل الأول :الدراسة النظرية:........................................... 25**

**القسم الأول : إنترنت الأشياء:.......................................25**

**ما هو إنترنت الأشياء؟ ........................................26  
 تحديد المعايير اللاسلكية التي تُمكّن إنترنت الأشياء ….......28  
 الهدف : قابلية التشغيل البينية …..............................29**

**فحص بنية انترنت الأشياء….................................30   
 بعض بروتوكولات انترنت الاشياء ............................32**

**القسم الثاني : المنازل الذكية :...................................... 35**

**وضع المنازل الذكية اليوم ....................................35**

**شبكة شبكية / كبسولة واحدة لكل غرفة ......................38**

**التغلب على التحديات .........................................42**

**التوافقية ...................................................42**

**تداخل الترددات الراديوية ...............................43**

**الحفاظ على اتصال سلس، موفر للطاقة، وموثوق ......44**

**إنشاء شبكة إنترنت أشياء سهلة الاستخدام ذاتية الإدارة ...46**

**أمان الشبكة والخصوصية .................................47**

**استهلاك الطاقة .............................................48**

**أهمية الاتصال الدائم …………………………..50**

**القسم الثالث : انظمة كشف التطفل على الشبكة :..................53  
 مقدمة عن انظمة كشف التطفل.................................53  
 انظمة كشف التطفل القائمة على التوقيع.......................57  
 نظام كشف التطفل القائم على الشذوذ..........................59  
 تقنيات تطبيق انظمة كشف التطفل القائمة على الشذوذ......61  
 تقنيات قائمة على المعرفة.......................................62  
 التعلم الخاضع للاشراف في نظام كشف التطفل...............64  
 التعلم غير الخاضع للاشراف في نظام كشف التطفل..........70**

**التعلم شبه الخاضع للاشراف في نظام كشف التطفل..........72  
 تقنيات قائمة على الهجين........................................74  
 مقاييس الاداء لانظمة كشف التطفل........................... .74**

**2.الفصل الثاني :تجهيز بيئة العمل:......................................76**

**3.الفصل الثالث :التجربة العملية:..........................................78**

**2.الفصل الرابع :النتائج والآفاق المستقبلية:.............................108**

**فهرس الأشكال:**

**الشكل 1-1: التحديات التي تواجه أنظمة كشف التطفل…………………………….. 25 الشكل 2-1: طبقة إنترنت الأشياء………………………………………………………27**

**الشكل 3-1: المراحل المبكرة لإنترنت الأشياء…………………………………………29**

**الشكل 4-1: معايير المنزل الذكي…………………………………………36**

**الشكل 5-1: منزل ذكي مع zigbee hub وBluetooth hubو ……………….37**

**الشكل 6-1: أجهزة المنزل الذكي في البنية التحتية للشبكة…………………...…39**

**الشكل 7-1: شبكة اتصال إنترنت الأشياء الموزعة على كبسولة واحدة لكل غرفة…….40**

**الشكل 8-1: دعم متعدد البروتوكولات الديناميكي و تقنية CurrentConnect ا…….45**

**الشكل 9-1: العمل المفاهيمي لمناهج أنظمة كشف التطفل القائمة على التوقيع……..59**

**الشكل 10-1: تصنيف أساليب انظمة كشف التطفل القائمة على الشذوذ…………..62**

**الشكل 11-1: التصنيف كمهمة…………………………………………….70**

**الشكل 12-1: مثال على التصنيف حسب اقرب جار ……………………………70**

**فهرس الجداول:**

**الجدول 1-1: ملخص الأوراق البحثية السابقة …19**

**الجدول 2-1: التطبيقات على أنظمة كشف التطفل في سياقات انترنت الاشياء…22**

**الجدول1-2: مقارنة بين المحاكيات. …………………………………..77المصطلحات و التعاريف**

**IoT Internet of Things إنترنت الأشياء**

**ITU International Telecommunication Union الاتحاد الدولي للاتصالات**

**IP Internet Protocol بروتوكول الإنترنت**

**LR-WPAN Low-Rate Wireless Personal Area Network شبكة شخصية لاسلكية منخفضة المعدل**

**IEEE Institute of Electrical and Electronics Engineers معهد مهندسي الكهرباء والإلكترونيات**

**PHY Physical Layer الطبقة الفيزيائية (في نموذج الشبكات)**

**MAC Medium Access Control التحكم بالولوج إلى الوسط**

**WLAN Wireless Local Area Network شبكة محلية لاسلكية**

**Wi-Fi (IEEE 802.11) Wireless Fidelity تقنية واي فاي – معيار IEEE 802.11**

**SIG Special Interest Group مجموعة الاهتمام الخاصة (يُستعمل مع البلوتوث)**

**BLE Bluetooth Low Energy بلوتوث منخفض الطاقة**

**IPv6 Internet Protocol version 6 بروتوكول الإنترنت – الإصدار السادس**

**LPWAN Low Power Wide Area Network شبكة واسعة النطاق منخفضة الطاقة**

**LoRa Long Range تقنية «المسافات الطويلة»**

**LoRaWAN Long Range Wide Area Network شبكة واسعة النطاق للمسافات الطويلة**

**NB-IoT Narrowband Internet of Things إنترنت الأشياء ضيق النطاق**

**5G Fifth Generation الجيل الخامس من شبكات الاتصالات**

**Node — عقدة (جهاز أو نقطة في الشبكة)**

**Gateway — بوابة تربط الشبكة بالإنترنت**

**Mesh Network — شبكة متشابكة (كل جهاز يعيد توجيه البيانات)**

**VMware Virtual Machine Ware برنامج لإنشاء وتشغيل الأنظمة الافتراضية**

**NS3 Network Simulator 3 محاكي شبكات (الإصدار الثالث)**

**ELM Extreme Learning Machine خوارزمية تعلم آلي سريعة للتصنيف**

**MUD Manufacturer Usage Description معيار يحدد سياسات استخدام أجهزة الـ IoT**

**DRL Deep Reinforcement Learning التعلم المعزز العميق (AI)**

**TCP Transmission Control Protocol بروتوكول التحكم بالنقل (موثوق)**

**UDP User Datagram Protocol بروتوكول بسيط لنقل الرسائل**

**IPv4 Internet Protocol version 4 بروتوكول الإنترنت – الإصدار الرابع**

**AP Access Point نقطة الوصول في شبكة لاسلكية**

**STAs Stations الأجهزة (المحطات) المتصلة بنقطة الوصول**

**CSMA Carrier Sense Multiple Access بروتوكول تحكم بالولوج للوسط**

**Tap Tap Interface واجهة شبكة افتراضية لربط المحاكيات بالنظام  
IDS: نظام كشف التطفل (Intrusion Detection System)**

**ACSC: المركز الأسترالي للأمن السيبراني (Australian Cyber Security Centre)**

**NIDS: نظام كشف التطفل في الشبكة (Network Intrusion Detection System)**

**SIDS: نظام كشف التطفل القائم على التوقيعات (Signature-based Intrusion Detection System)**

**AIDS: نظام كشف التطفل القائم على الشذوذ (Anomaly-based Intrusion Detection System)**

**ML: التعلم الآلي (Machine Learning)**

**DL: التعلم العميق (Deep Learning)**

**ANN: الشبكة العصبية الاصطناعية (Artificial Neural Network)**

**BP: الانتشار الخلفي (Backpropagation)**

**SVM: آلات المتجهات الداعمة (Support Vector Machines)**

**HMM: نموذج ماركوف المخفي (Hidden Markov Model)**

**KNN: أقرب جار (K-Nearest Neighbors)**

**GA: الخوارزميات الجينية (Genetic Algorithms)**

**UML: لغة النمذجة الموحدة (Unified Modeling Language)**

**IoT: إنترنت الأشياء (Internet of Things)**

**CPCS: أنظمة التحكم السيبرانية-الفيزيائية (Cyber-Physical Control System)**

**SLFN: شبكة عصبية أمامية ذات طبقة خفية واحدة (Single Hidden Layer Feed-Forward Neural Network)**

**TPR: معدل الإيجابية الحقيقية (True Positive Rate)**

**FPR: معدل الإيجابية الكاذبة (False Positive Rate)**

**FNR: معدل السلبية الكاذبة (False Negative Rate)**

**CR: معدل التصنيف (Classification Rate)**

**DR: معدل الكشف (Detection Rate)**

**ROC: منحنى خاصية تشغيل المُستقبِل (Receiver Operating Characteristic)**

**FAR: معدل الإنذار الكاذب (False Alarm Rate)**

**1.المقدمة :**

يعود الاهتمام بإنترنت الأشياء، بشكل عام، إلى عدة أسباب، منها:

يعمل إنترنت الأشياء على ربط الأشياء معًا عبر هوية خاصة. ولا تختلف تطبيقات إنترنت الأشياء كثيرًا بالنسبة للعاملين في مؤسسات المعلومات الذين تعاملوا سابقًا مع تقنية تتبع الأشياء بتقنية تحديد الهوية بموجات الراديو (RFID) إذ تتشابه في تتبع الأشياء عبر أجهزة استشعار متصلة عن بعُد . إلا أن الفرق هنا يكمن في أن التواصل بين الأشياء والأجهزة يتم عبر إنترنت الأشياء من خلال الإنترنت.

يعُد إنترنت الأشياء وسيلة فعّالة للتغلب على بعض المشكلات التي تواجه المتعلم، ويساعده على تجاوز حواجز الزمان والمكان، ويمُكّنه من إدارة التعلم عن بعُد بنجاح.

كما يمُكن لإنترنت الأشياء أن يسُاعد في تعزيز العلاقة بين الطالب والمعلم، بحيث يتمكن كل منهما من التواصل مع الآخر عبر تطبيقات إنترنت الأشياء دون الحاجة إلى مقابلة فعلية.

يمكن للشركات استخدام هذه التقنية لخفض تكاليف الإنتاج من خلال زيادة التعاون والأتمتة بين الآلات بدلاً من العمال. يمكن للمؤسسات تقديم عروض أكثر كفاءة وتنوعًا وفورية، استناًدًا إلى جمع البيانات من المستخدمين في الوقت الفعلي. يجب على المؤسسات تغيير سياستها في الإعلان عن سلعها للعملاء المحتملين، وتوصيل تلك العروض إلى المستخدم عند باب منزله عبر هاتفه الذكي في وقت قياسي ومناسب. يوفر إنترنت الأشياء:

* وسيلة فعّالة لتسويق خدماتها من خلال التواصل بين الجهات المعنية.
* استجابة سريعة وحساسة وآمنة لتلبية احتياجات المستفيدين من المعلومات ضمن شبكة إنترنت الأشياء.
* رفع إنتاجية الأجهزة والأنظمة من خلال زيادة دقة معالجة البيانات، وتنفيذ العمليات عن بعُد، وتقليل الاعتماد على العامل البشري.
* زيادة مستوى التوافر داخل أنظمة المعلومات من خلال تحسين قدرتها على أداء عملها وسرعة الوصول والحصول على المعلومات من خلالها.
* تمكين توصيل الأشياء في أي وقت وفي أي مكان لمن يستخدم خدمات شبكة إنترنت الأشياء بإتقان.
* تطوير خدمات مرجعية وتمكين المستخدمين من طرح أسئلة مرجعية والحصول على إجابات من داخل إنترنت الأشياء.
* ضمان وصول المستخدمين داخل شبكة إنترنت الأشياء إلى الموارد ومصادر المعلومات من خلال هوياتهم المُوثقّة والمُعرّفة، وأحيانًا من خلال رموز إضافية مُعرّفة.
* تسهيل عملية حفظ الموارد وتخزينها من خلال أنظمة الحوسبة السحابية والحوسبة الضبابية، والتي يتم من خلالها التحكم في موارد المعلومات ومصادرها ومراقبتها والتحكم بها، واستلام بياناتها بدقة وبشكل دائم.
* القدرة على استشعار الأشياء وإصدار التنبيهات والتحذيرات والتقارير المناسبة عنها من خلال قدرتها على معالجة البيانات وتحليلها، ومراقبتها وتتبعها واتخاذ قرارات ذكية باستمرار[20,24].

مزايا إنترنت الأشياء :

1. البيانات: يوفر إنترنت الأشياء كمًا هائلًا من المعلومات التي تساعدنا على اتخاذ القرارات الصائبة في الوقت المناسب.
2. الوقت: توفر تقنية إنترنت الأشياء الكثير من الوقت من خلال توفير معلومات دقيقة في الوقت المناسب وبأسرع وقت.
3. اقتصادية: تعُد تقنية إنترنت الأشياء اقتصادية للغاية، وذلك حسب سيناريوهات التطبيق.
4. التتبع: يساعد إنترنت الأشياء في تتبع أو مراقبة مختلف الأشياء المادية، مما يوفر الوقت والمال.
5. يسُهم بشكل كبير في توفير الوقت والجهد والمال، من خلال تمكين الفرد والمؤسسة من التحكم عن بعُد في الأشياء لتنفيذ ما هو مطلوب منها بدقة ، بالإضافة إلى إمكانية فهم الأشياء فيما بينها من خلال أجهزة استشعار تتواصل مع بعضها البعض عبر الإنترنت و ، قد حقق ذلك نتائج عديدة ساهمت في توفير الوقت والجهد والمال.
6. يتحرر الإنسان من قيود الزمان والمكان، حيث يستطيع إدارة الأمور والتحكم فيها عبر بروتوكول الإنترنت دون الحاجة إلى التواجد في نفس المكان؛ ودون تدخله المباشر في كثير من الأحيان، إذا أعطى تعليمات مسبقة.[1]

تعد الهجمات على البنى التحتية للشبكات من أكبر المشكلات التي تواجه الشبكات في العالم اليوم.

فمع النمو السريع للأنشطة غير القانونية في الشبكات أصبحت أمنية الشبكات تحديًا كبيرًا لا يمكن اعتباره محلولاً بالكامل بعد.

في البدايات كانت جدران الحماية(Firewalls) هي خط الدفاع الرئيسي والوحيد لحماية الشبكات غير أن أول هجوم واسع الانتشار على الإنترنت وقع في عام 1988 بواسطة (Morris Worm) التي استهدفت برنامج Send mail.

من ذلك الوقت ظهرت العديد من الأساليب للتغلب على هذه الثغرات وتوفير حماية أفضل للشبكات.

في البداية كانت من أكثر الطرق الشائعة لدى الشركات الموردة للأجهزة أن ترسل اسم المستخدم وكلمة المرور الإفتراضيين مع الأجهزة لتقليل خطر الاختراق.

و للمرة الأولى في منتصف الثمانينيات نشرت أبحاث (Denning) حول كشف التطفل حيث افترضت أن الأنشطة التطفلية تختلف عن الأنشطة العادية وأن الدور الأساسي لنظام كشف التطفل (IDS) هو اكتشاف النماذج المناسبة للسلوك الطبيعي بحيث يمكن التمييز بسهولة بين النشاط المشروع و النشاط التخريبي.

إن كشف التطفل اليوم يعتبر من أحدث وأهم مجالات البحث في شبكات الحاسوب و مازال قيد الدراسة المستمرة وقد تم تطوير العديد من النماذج الأولية التي تعمل على مناهج مختلفة للتطبيقات التجارية والعسكرية.

يستند نظام كشف التطفل إلى الدمج بين تقنيات الكشف عن التطفل وتقنيات الـ Brute Force. في الوقت الحالي يعد نظام كشف التطفل (IDS)جزء أساسي من منظومة أمن الشبكات لأنه يوفر حماية شاملة للشبكة من خلال قدرته على التعرف على كل محاولات التطفل الناجحة وغير الناجحة. وتتمثل وظيفة نظام كشف التطفل IDS في رصد جميع السلوكيات غير الطبيعية في النظام و استبعاد الأنشطة التي لا تعتبر هجمات من خلال دراسة معمقة لأنماط وسلوكيات الهجمات والتواقيع المرتبطة بها لذا يمكن لنظام كشف التطفل IDS أن يقدم استجابة فورية لمثل هذه الحوادث.

كما يمكن لنظام كشف التطفل أداء المهام التالية:

1.مراقبة أنشطة النظام والمستخدمين.

2.التحقق من أخطاء النظام.

3.تقييم سلامة الأنظمة وملفات البيانات.

4.تسجيل أي سلوك غير طبيعي وحفظه كسجلات إحصائية.

5.التعرف على الأنشطة التطفلية ورسم خرائط الهجمات المعروفة وتوليد التنبيهات المناسبة. [2]

لقد أصبحت أنظمة كشف التطفل(IDS) مقبولة كإضافة ضرورية إلى البنية التحتية الأمنية في كل مؤسسة. ورغم المساهمات الموثقة التي تقدمها تقنيات كشف التطفل في تعزيز أمن الأنظمة ما زال يتعين تبرير اقتناء هذه الأنظمة . وهناك عدة أسباب مقنعة تدفع إلى اعتماد واستخدام IDS :

1. منع السلوكيات الضارة من خلال زيادة الشعور بمخاطر الاكتشاف والعقوبة لمن يحاولون مهاجمة النظام أو إساءة استخدامه.
2. كشف الهجمات والانتهاكات الأمنية الأخرى التي لا تتمكن وسائل الحماية الأخرى من منعها.
3. التعرف على البدايات الممهدة للهجمات والتي غالبًا ما تظهر على شكل محاولات فحص الشبكات.
4. توثيق التهديدات التي قد تواجه المؤسسة.
5. العمل كأداة لمراقبة التصميم الأمني والإدارة الأمنية خصوصا في المؤسسات الكبيرة والمعقدة.
6. توفير معلومات مهمة حول الهجمات التي تقع بما يسمح بتحسين التشخيص ودعم الاستجابة والتعافي وتصحيح العوامل المسببة. [3]

المشكلة العلمية:

شهدت المنازل الذكية في السنوات الأخيرة انتشارًا واسعًا بفضل الاعتماد على أجهزة إنترنت الأشياء مثل الكاميرات الذكية، الأقفال الإلكترونية، الحساسات، والمساعدات الصوتية. ورغم ما تقدمه هذه الأجهزة من مزايا تتعلق بالراحة والأتمتة وكفاءة استهلاك الموارد، فإنها تفتح في الوقت نفسه سطح هجوم واسع أمام المخترقين . وقد أثبتت هجمات فعلية مثل برمجية Mirai botnet أو اختراق أجهزة مراقبة الأطفال مدى هشاشة بيئة المنازل الذكية من الناحية الأمنية.[4]

تعود خطورة هذه المشكلة إلى عدة أسباب؛ أبرزها أن أجهزة إنترنت الأشياء تمتلك قدرات محدودة من حيث العتاد والذاكرة، مما يجعل من الصعب تثبيت برامج الحماية التقليدية مثل مضادات الفيروسات أو تلقي التحديثات الأمنية بشكل مستمر . بالإضافة إلى ذلك، فإن تعدد الشركات المصنعة واختلاف بروتوكولات الاتصال يؤدي إلى غياب معايير موحدة للأمن. [4] كما أن معظم المستخدمين النهائيين يفتقرون إلى الخبرة التقنية الكافية للتعامل مع الاختراقات عند حدوثها.

أما أنظمة كشف التطفل التقليدية (IDS)، فهي غير ملائمة بالكامل لهذه البيئات، إذ أن بعضها يحتاج إلى موارد عالية لا تتوفر في أجهزة إنترنت الأشياء، بينما يعجز بعضها الآخر عن التمييز بدقة بين أنماط الهجمات المختلفة مثل هجمات حجب الخدمة (SYN Flooding) أو هجمات انتحال العنوان (ARP Spoofing) أو هجمات إعادة الإرسال HTTP Flooding)) .

بناءً على ذلك، تتمثل مشكلة البحث العلمية في غياب آليات كشف تطفل خفيفة وفعّالة ومصممة خصيصًا لبيئة المنازل الذكية، بحيث تكون قادرة على العمل ضمن القيود المفروضة على أجهزة إنترنت الأشياء، وفي الوقت نفسه تحقق قدرة عالية على التعرّف على مختلف أنواع الهجمات بدقة وكفاءة [4] .

الدراسة النظرية :

في هذا القسم سيتم عرض بعض الأبحاث السابقة التي قام بها باحثون في الموضوع المشترك بين كشف التطفل وإنترنت الأشياء ضمن المنازل الذكية حيث:

فقد قام أشرف وآخرون [5] بمراجعة شاملة لأنظمة كشف التطفل في إنترنت الأشياء باستخدام تقنيات التعلم الآلي والتعلم العميق، حيث ناقشوا التحديات والحلول والاتجاهات المستقبلية. وأكّدوا على الحاجة إلى طرق كشف فعّالة ودقيقة، لكنهم لم يقترحوا بنية أو تطبيق عملي محدد. أما في البحث قام شابوني وآخرون [6] باستعرض تقنيات كشف التطفل في شبكات إنترنت الأشياء اعتمادًا على خوارزميات التعلم، وركّزوا بشكل خاص على أمن المنازل الذكية. وقد حللوا بشكل مفصل الأعمال الحديثة في مجال التعلم الآلي، لكنهم لم يتطرقوا إلى قضايا تصميم البنية مثل القدرة على التكيّف ومتطلبات العمل في الزمن الحقيقي.

في البحث قدم الباحث التان [7] تطبيقًا للتعلم العميق في كشف التطفل ضمن أنظمة الاستشعار الخاصة بإنترنت الأشياء الصناعي. ورغم أهميته للتطبيقات الصناعية، إلا أنه قد لا يناسب البيئات المنزلية الذكية بسبب اختلاف القيود التشغيلية وأساليب الهجوم. بينما في هذا البحث اقترح سالاي [8] إطارًا متكاملًا متعدد الطبقات لكشف التطفل في إنترنت الأشياء، وطُبّق في المجال الصناعي، لكنه لم يوضح تفاصيل تصميم البنية أو كيفية النشر. جميع هذه الدراسات أشارت إلى أن أغلب الطرق الحالية تتجاهل قيود إنترنت الأشياء المهمة مثل: زمن الاستجابة المنخفض، تغيّر سلوك الأجهزة باستمرار، وقلة الموارد، وهي عوامل مؤثرة على قابلية التطبيق على نطاق واسع.

أما في هذا البحث ناقشت لين وآخرون[9] كشف التطفل في الحوسبة الضبابية وحوسبة الحافة المتنقلة، وهو عمل مهم خاصة مع ازدياد استخدام هذه التقنية في المنازل الذكية، لكنهم لم يتطرقوا إلى دور التعلم الآلي في الكشف وهذا لا يمكن الاستفادة منه في بحثنا. قدم الباحث لوكاس [10] نظامًا ذاتي التهيئة لكشف التطفل في المنازل الذكية باستخدام التعلم المعزز، حيث يتميز بقدرته على التكيّف مع الظروف المتغيرة وهو خطوة مهمة نحو أنظمة أمنية أكثر ديناميكية واستجابة. تناول الباحث الالادي [11] نهجًا هجينًا يعتمد على "الجهاز المناعي الاصطناعي" لكشف التطفل في شبكات المنازل الذكية، وأبرزت قوة خوارزمية ELM في سرعة التعلم والتعميم، لكنه لم يركز في هذه الدراسة على جانب العمل في الزمن الحقيقي.

دمج روسلي و آخرون في هذا البحث [12] بين الشبكات المعرفة برمجيًا، والتعلم الآلي، ومعيار أوصاف استخدام المُصنِّع **(**MUD**)** مع نظام كشف ومنع التطفل لدراسة تأثيره على أمن الشبكة. ورغم أن إدخال هذه المعايير خطوة مهمة، إلا أن العمل اقتصر على مجال التصنيع ولم يدرس فعالية البنية أو خصائص حركة مرور الشبكة.

بالنسبة لتحليل حركة البيانات، فقد أوضح الباحث ابراهيم واخرون [13] أهمية فهم طبيعة بيانات إنترنت الأشياء ونماذج الاندفاعات المفاجئة في الاستخدام، واقترح نموذجًا متقدمًا يعتمد على وضعيات ON/OFF لتغطية المدن الذكية. ومع ذلك، لم يتناول البحث تصميم البنية أو آلية النشر. بينما في هذه الدراسة قدم Kumar في [14] رؤى حول خصائص حركة مرور إنترنت الأشياء في المنازل الذكية والحرم الجامعي، وأظهرت أن معظم الأجهزة تعمل بشكل دوري مع فترات خمول طويلة، وتنتج كمية صغيرة من البيانات وتتواصل غالبًا مع عدد محدود من الخوادم البعيدة (غالبًا في نفس بلد الجهاز). كما اكتشف البحث مشكلات في الأمن والخصوصية مثل التواصل عبر قنوات غير مشفّرة أو مع خوادم في دول مشهورة بمخاطر الخصوصية.وبناءً على ذلك، يهدف هذا البحث إلى تصميم وبناء نظام كشف تطفل مرن وقابل للتوسع، يضمن الحماية بكفاءة في البيئات الحقيقية للمنازل الذكية، دون فقدان القدرة على التكيّف والتعميم وهذا البحث نستطيع الاستفادة منه في موضوعنا من خلال تحليل حركات المرور بين اجهزة IoT **.**

**في ما يلي ملخص لما سبق :**

الجدول 1-1: ملخص الأوراق البحثية السابقة.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| اسم الورقة البحثية | التاريخ | الموضوع | النتائج | الاستفادة في موضوعنا |
| A review of intrusion detection systems using machines and deep learning on the Internet of things: Challenges, solutions and future directions. | 2020 | مراجعة شاملة لأنظمة كشف التطفل باستخدام التعلم الآلي والتعلم العميق. | أكدوا أهمية طرق كشف فعّالة لكن لم يقدموا تصميم أو تطبيق عملي | |  | | --- | | يفيد كبنية نظرية لكن لا يوجد فيه تطبيق عملي يمكن البناء عليه. |  |  | | --- | |  | |
| Network intrusion detection for IoT security based on learning techniques. | 2019 | استعراض تقنيات كشف التطفل في شبكات إنترنت الأشياء اعتمادًا على خوارزميات التعلم، مع تركيز على أمن المنازل الذكية.   |  | | --- | |  |  |  | | --- | | ا | | |  | | --- | | تحليل مفصل للأعمال الحديثة، لكن لم يناقش متطلبات الزمن الحقيقي. |  |  | | --- | |  | | |  | | --- | | يفيد كمصدر لتحديد التحديات الحالية في المنازل الذكية، لكنه لا يعطي حلول قابلة للتطبيق في هذا المشروع. |  |  | | --- | |  | |
| A deep learning application for invasion detection in industrial Internet of things sensing systems | 2021 | |  | | --- | | تطبيق للتعلم العميق في كشف التطفل في IoT الصناعي. |  |  | | --- | |  | | |  | | --- | | مفيد للصناعة، غير مناسب للمنازل بسبب اختلاف طبيعة الهجمات والموارد. |  |  | | --- | |  | | |  | | --- | | محدود الفائدة، لكن يمكن الاستفادة من آلية استخدام التعلم العميق كمقارنة مع نموذجنا. |  |  | | --- | |  | |
| An integrated multilayered framework for IoT security intrusion decisions | 2023 | |  | | --- | | إطار متعدد الطبقات لكشف التطفل في IoT. |  |  | | --- | |  | | |  | | --- | | طُبق في الصناعة، بدون تفاصيل تصميم أو نشر. |  |  | | --- | |  | | |  | | --- | | يفيد كفكرة "تعدد الطبقات"، ممكن تطبّقها في مشروعنا (Snort + AI = طبقتين). |  |  | | --- | |  | |
| Sample selected extreme learning machine based intrusion detection in fog computing and MEC. Wireless Communications and Mobile Computing | 2018 | |  | | --- | | كشف التطفل في الحوسبة الضبابية. |  |  | | --- | |  | | |  | | --- | | لم يستخدموا تعلم آلي |  |  | | --- | |  | | يناقش الأمور الصناعية لا يفيد المشروع لأنه خارج الموضوع الاساسي |
| Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning | 2020 | |  | | --- | | نظام ذاتي التهيئة باستخدام التعلم المعزز للمنازل الذكية. |  |  | | --- | |  | | |  | | --- | | يتكيف مع الظروف المتغيرة، خطوة مهمة للأنظمة الديناميكية. |  |  | | --- | |  | | |  | | --- | | مهم جدًا لأنه قريب من بيئة المشروع (منازل ذكية)، يمكن الاستفادة منه عند شرح أهمية الأنظمة المتكيفة. |  |  | | --- | |  | |
| Intrusion detection system in smart home network using artificial immune system and extreme learning machine hybrid approach | 2020 | |  | | --- | | جهاز مناعي اصطناعي + خوارزمية ELM لكشف التطفل. |  |  | | --- | |  | | |  | | --- | | سريع في التعلم والتعميم، لكن بدون زمن حقيقي. |  |  | | --- | |  | | |  | | --- | | يفيد من حيث طرح نهج هجين (Snort + AI). لكن عيبه نفس مشكلة الزمن الحقيقي. |  |  | | --- | |  | |
| SDN based intrusion detection and prevention systems using manufacturer usage description: a survey | 2020 | |  | | --- | | دمج SDN + ML + معيار MUD لكشف ومنع التطفل. |  |  | | --- | |  | | |  | | --- | | ركز على التصنيع، ما درس فعالية البنية في المنازل. |  |  | | --- | |  | | |  | | --- | | محدود الفائدة، لكن يمكن الاستفادة من دمج المعايير والبنى المختلفة. |  |  | | --- | |  | |
| Traffic modelling of smart city internet of things architecture. | 2020 | |  | | --- | | تحليل طبيعة بيانات IoT ونموذج ON/OFF للمدن الذكية. |  |  | | --- | |  | | |  | | --- | | مهم لفهم خصائص حركة المرور، لكنه ما يناقش الكشف. |  |  | | --- | |  | | |  | | --- | | يفيد جدًا في جانب تحليل حركة مرور الشبكة على NS3، خصوصًا في توليد سيناريوهات حركة IoT واقعية. |  |  | | --- | |  | |
| Characterizing IoT traffic in smart home and campus environments | 2020 | |  | | --- | | خصائص حركة مرور IoT في المنازل الذكية والجامعات. |  |  | | --- | |  | | |  | | --- | | وجد أن الأجهزة ترسل بيانات قليلة وتتواصل مع خوادم محلية، مع مشاكل أمنية. |  |  | | --- | |  | | يعطي بيانات فعلية لطبيعة حركة المرور في المنازل الذكية، ويمكن الاستفادة منها في بناء سيناريوهات NS3. |

الجدول 2-1: التطبيقات على أنظمة كشف التطفل في سياقات إنترنت الأشياء.

|  |  |
| --- | --- |
| **قطاع إنترنت الأشياء** | **شرح مختصر** |
| أمن المنازل الذكية | يركز على تعزيز التدابير الأمنية في المنازل الذكية من خلال الكشف التكيفي عن التهديدات والاستجابة الفورية للتهديدات المتنوعة مثل هجمات حجب الخدمة الموزعة والهجمات الإلكترونية. |
| إنترنت الأشياء الصناعي | يناقش عملية صنع القرار المعقدة وتحسين العمليات في أنظمة إنترنت الأشياء، ومعالجة التحديات الأمنية عالية المخاطر. |
| أنظمة إنترنت الأشياء للرعاية الصحية | يطبق (Deep Reinforcement Learning)  DRL لضمان الدقة والخصوصية الحرجة، والتكيف مع الطبيعة الحساسة لبيانات وعمليات الرعاية الصحية. |
| أنظمة النقل | يعزز الأمن في النقل من خلال إدارة البيئات الديناميكية وتأمين شبكات المركبات عالية السرعة ضد الهجمات المتطورة. |
| المدن الذكية | يستخدم(Deep Reinforcement Learning)  DRL لإدارة أنظمة تكنولوجيا المعلومات و الاتصالات المعقدة و تحسين الأمن عبر شبكات المدن الكثيفة، وتعزيز بروتوكولات الاتصال على مستوى المدينة. |
| أمن إنترنت الأشياء العام | يستكشف التطبيق الأوسع ل (Deep Reinforcement Learning)عبر مختلف مجالات إدارة البيانات مع التركيز على التعلم التكيفي وتحسينات الأمان في سياقات تشغيلية متنوعة. |

**التحديات التي تواجه أنظمة كشف التطفل:**

تجري دراسات مستمرة حول أنظمة جديدة للكشف التلقائي عن الاستخدامات غير الطبيعية للأنظمة. إضافة ً إلى ذلك، أشار الباحثون إلى تطوير نموذج للكشف عن التطفل، واقترحوا كإطار عمل لنظام كشف التطفل

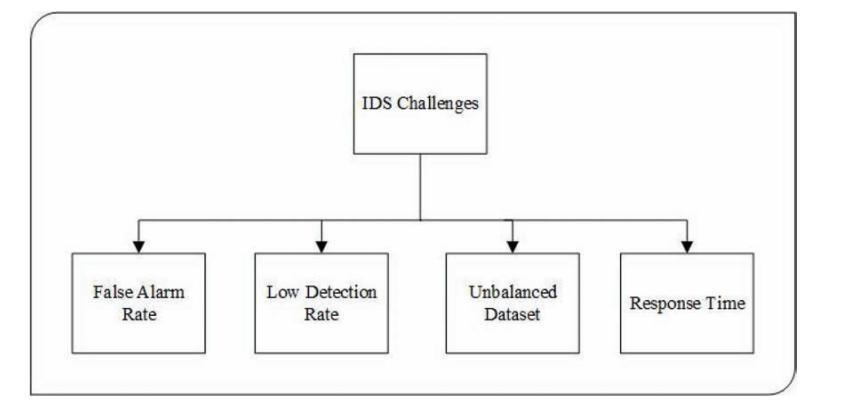
(IDS) عام الاستخدام [16]. منذ ذلك الحين، قام الخبراء بتطوير وتطبيق عدة خوارزميات لأتمتة عملية الكشف عن التطفل في الشبكات. كما سعوا باستمرار إلى ابتكار طرق أكثر دقة وأسرع وأكثر قابلية للتوسع لهذا الغرض. ومع قدوم عصر إنترنت الأشياء (IoT) و البيانات الضخمة، كان من المتوقع أن يتجاوز عدد الأجهزة المتصلة 26 مليار جهاز بحلول عام 2020 [17] ومع هذا التوجه، من المتوقع أيضًا أن يزداد نوع وعدد قضايا الأمن السيبراني. حيث يلخص الشكل (1) لتحديات في أنظمة كشف التطفل (IDS). وتشمل هذه التحديات: معدل الإنذارات الكاذبة، انخفاض معدل الكشف، عدم توازن مجموعات البيانات، وزمن الاستجابة .

وقد دعا بعض الباحثين مؤخرًا إلى تقسيمات إضافية لأنظمة كشف التطفل. على سبيل المثال، ذكر وا [18] أن أنظمة كشف التطفل IDS يجب أن تصُنّف إلى خمس فئات فرعية يمكن أن تنتمي لأي من الفئات السابقة. والفئات المقترحة هي: المعتمدة على الأنماط، المعتمدة على القواعد، المعتمدة على الإحصاء، المعتمدة على الحالة، والمعتمدة على الاستدلال (heuristic-based). إلا أن مثل هذا التصنيف قد يؤدي إلى إرباك بسبب أوجه التشابه بين نقاط قوة التقنيات المختلفة ، بالإضافة إلى غياب معايير واضحة لتمييز تقنية عن أخرى. غالبًا ما ترتبط أنظمة الكشف المعتمدة على التوقيعات أو القواعد بنسبة معينة من الإنذارات الكاذبة (FP- false positive)، كما أنها غير قادرة على اكتشاف أشكال جديدة من الهجمات [19] ومن المتوقع أن تظهر أنظمة كشف تطفل (IDS)

بمستوى عال من اكتشاف الإنذارات الكاذبة. أما الأنظمة المعتمدة على تحليل البروتوكولات بالحالة (stateful protocol analysis)، فإن أداء الكشف لديها يختلف باختلاف مستوى تعريف ملفاتها الشخصية [20]. ويتمثل التحدي الأكبر في هذا النهج في الحفاظ على تحديث مستمر لهذه الملفات مع تطور البروتوكولات بمرور الوقت.

وكما نوقش سابقًا، فإن هذه الدراسة تركز على تطوير نظام كشف تطفل معتمد على الشذوذ (anomaly-based IDS) يتميز بدقة جيدة ومعدل إنذارات كاذبة منخفض. وقد أجُريت العديد من الدراسات حول تقليل الإنذارات الكاذبة في نظام كشف التطفل IDS. حيث قدّر الخبراء أن حوالي %99 من تنبيهات الكشف عن التطفل لا تتعلق بمشاكل أمنية حقيقية، وذلك بسبب الفروقات البسيطة المرصودة بين الأنشطة العادية والأنشطة الخبيثة[21]. كما أشاروا إلى تحديات أخرى، مثل تطوير توقيعات دقيقة تستطيع اكتشاف السلوك غير الطبيعي دون أن تطُلق إنذارات أثناء الأنشطة العادية، إذ قد يسُمح ببعض الأنشطة في حالات معينة بينما تعُتبر تطفلًا في حالات أخرى.

واقترحوا نهج المتعلم التكيفي لتصنيف التنبيهات ALAC في[22]، والذي يعتمد على تقنيات التعلم الآلي (ML-machine learning) مقترنة بتدريب يعتمد على الملاحظة البشرية للتعلم التكيفي لقواعد التصنيف الضمنية. وبسبب تدخل العامل البشري أثناء التدريب، يمكن لنظام ALAC أن يتم تحديثه تدريجيًا مع تغير الظروف، فإن التحديات الرئيسية لأنظمة كشف التطفل المعتمدة على الحالات الخاصة تتمثل في أن بناء نظام بخصائص كهذه يصبح أكثر تعقيًدًا في حالة كشف سوء الاستخدام [23]. بالإضافة إلى ذلك، يرتفع معدل الإنذارات الكاذبة مع انخفاض معدل الكشف. وهناك أيضًا مشكلة عدم توازن البيانات، والتي تؤثر بشكل مباشر على تقييم النماذج [19].



الشكل 1-1: التحديات التي تواجه أنظمة كشف التطفل.

**الفصل الأول :الدراس المراجعية**

**القسم الاول: انترنت الأشياء**

إن إنترنت الأشياء (IoT) يخلق عالماً جديداً ــ عالماً قابلاً للقياس والرصد ــ يستطيع فيه الناس إدارة حياتهم بشكل أفضل، وتتمكن المدن من إدارة بنيتها التحتية بكفاءة أكبر، وتتمكن الشركات من إدارة أعمالها بفاعلية أعلى كما ان هذا العالم الذكي المتصل سيقدم تغييرات جوهرية للمستهلكين وللمجتمع، كما سيُحدث تحولاً عميقاً في صناعات كاملة. إن صعود إنترنت الأشياء سيحقق العديد من التحسينات المهمة في عالمنا وحياتنا اليومية من خلال مساعدتنا على اتخاذ قرارات أفضل وبشكل أسرع اعتماداً على معلومات آنية وذات جودة أعلى.

**ما هو إنترنت الأشياء؟**

لفهم إنترنت الأشياء، من المفيد أن نعيد بسرعة تتبّع كيفية تطور الإنترنت ككل.

بدأ الإنترنت كشبكة صغيرة نسبياً من الحواسيب العسكرية والحكومية الموصولة عبر اتصالات سلكية. ومع مرور الوقت، توسّع الإنترنت وأصبح متاحاً لملايين الأشخاص حول العالم، وجعلت شبكة الويب العالمية من الممكن لأي شخص نشر المعلومات للاطّلاع العام. جاءت القفزة التالية مع الانتشار السريع للاتصالات اللاسلكية. وبمساعدة شبكات Wi-Fi والاتصالات الخلوية، حدث توسّع هائل. فقد حررت الهواتف الذكية والأجهزة المحمولة المتصلة بالإنترنت الوصول إلى الشبكة من أماكن محددة، مما جعلها متاحة تقريباً في كل مكان.

لكن لم تكن الحواسيب وحدها هي التي تستخدم الإنترنت، بل بدأت العديد من أنواع الأجهزة الأخرى تتضمن قدرات بسيطة للحوسبة والشبكات. في أوائل العقد الأول من الألفية الجديدة ظهر مصطلح إنترنت الأشياء (IoT) لوصف النطاق المتزايد باستمرار من الأشياء المتصلة بالإنترنت واستخداماتها. وفي عام 2005، اعترف الاتحاد الدولي للاتصالات (ITU) رسمياً بهذا المصطلح. ويعرّف الاتحاد إنترنت الأشياء بأنه: "يتألف من أشياء ذكية تتصل بالإنترنت وتتواصل مع بعضها البعض بحد أدنى أو دون أي تدخل بشري."

عادةً ما تتصل هذه الأشياء عبر بوابة (Gateway) بمنصة إنترنت الأشياء، التي تتكون من أدوات وخدمات برمجية تجمع البيانات من أجهزة الاستشعار (Sensors) والمتحكمات (Controllers) والأجهزة الأخرى.

اليوم يتمحور إنترنت الأشياء (IoT) حول ربط العديد من أنواع الأجهزة المختلفة بالإنترنت، مثل أجهزة الاستشعار، ووحدات التحكم الصوتية (Hands-free controllers)، وأجهزة المراقبة عن بُعد. ووفقاً لشركة Cisco، فقد تجاوزنا بالفعل المرحلة التي أصبح فيها عدد "الأشياء" أو الأجهزة المتصلة بالإنترنت أكبر من عدد الأشخاص ــ وفي الواقع، لقد تجاوزنا هذه المرحلة منذ أكثر من عشر سنوات.

يوضح الشكل 1-1 ما يحدث بشكل عام. في طبقة الاستشعار والاتصال (Sense & Connect Layer)، تقوم المنصة بربط عتاد إنترنت الأشياء بالتطبيقات الشبكية التي تنفذ عمليات معالجة البيانات وتخزينها. في المنتصف توجد طبقة المنصة (Platform Layer)، حيث تُخزَّن البيانات وتُؤمَّن وتُعالج وتُحلَّل. أما في طبقة المستخدم النهائي (End-User Layer)، فهي ترتبط بالتطبيقات المخصصة للمستخدم النهائي، والتي تقوم بمراقبة وتفسير البيانات القادمة من أجهزة إنترنت الأشياء، ثم ترسل تعليمات تخبر الأجهزة بتنفيذ إجراءات مثل قفل باب منزلك أو رفع باب المرآب.

توفر منصات إنترنت الأشياء (IoT Platforms) عادةً خدمات تتميز بـ:

القدرة على التكيف (Adaptable): يمكن لأنظمة إنترنت الأشياء التكيف ديناميكياً مع تغيّر السياقات، بحيث تتصرف وفقاً لظروف التشغيل أو مدخلات المستخدم أو المعلومات المستشعرة.

هوية فريدة (Uniquely identifiable): يمتلك كل جهاز من أجهزة إنترنت الأشياء هوية فريدة، مثل عنوان بروتوكول الإنترنت (IP address). وتتيح هذه العناوين للمستخدمين الاستعلام عن الجهاز، ومراقبته، والتحكم به عن بُعد.

التكوين الذاتي (Self-configurable): يمكن للأجهزة ضمن شبكة إنترنت الأشياء أن تقوم بتكوين نفسها تلقائياً، مما يسمح للعديد من الأجهزة المتصلة بالتعاون فيما بينها لتوفير وظائف النظام الكاملة.

التكامل الشبكي (Network integrated): يتم دمج أجهزة إنترنت الأشياء في شبكة إنترنت الأشياء لتمكين الاتصال بين العقد (Nodes)، والبوابات (Gateways)، والبنية التحتية.

اتخاذ القرارات الذكية (Intelligent decision making): تستطيع أجهزة إنترنت الأشياء اتخاذ قرارات تمكّنها من التكيف مع الظروف المتغيرة.

**تحديد المعايير اللاسلكية التي تمكّن إنترنت الأشياء :**

تُستخدم حالياً مجموعة واسعة من معايير تقنيات الاتصال اللاسلكي لربط أجهزة إنترنت الأشياء. بعض هذه المعايير مألوف مثل Bluetooth و Wi-Fi و Zigbee، بينما يعتمد بعضها الآخر على حلول خاصة أقل شيوعاً. يلخّص الشكل 1-2 المشهد الحالي، حيث يقسّمه إلى ثلاثة أقسام بناءً على النطاق (Range). وكما هو موضح في الشكل، أصبحت منظومة إنترنت الأشياء معقداة وصعبة الإدارة من منظور المستخدم بسبب كثرة المعايير المختلفة المستخدمة.

عادةً ما تختار الشركات التي تصنع منتجات إنترنت الأشياء المعيار (أو مجموعة المعايير) المراد استخدامها بناءً على النطاق ونوع البيانات. فعلى سبيل المثال، قد تحتاج هذه الأجهزة إلى نقل محتوى وسائط (Media Content) أو بيانات الاستشعار والتحكم (Sense-and-control data). ومع وجود مجموعة كبيرة من المعايير القياسية للاختيار منها، بالإضافة إلى بعض الحلول الخاصة (Proprietary)، يمكن لمصممي الأنظمة اختيار التقنية الأنسب لتحسين أداء أجهزة المستخدم النهائي. لكن هذا لا يجعل الأمور دائماً سهلة بالنسبة للمستخدم العادي.

**الهدف: قابلية التشغيل البيني (Interoperability)**

تشير قابلية التشغيل البيني إلى قدرة منتج أو نظام ما على العمل مع منتجات أو أنظمة أخرى، سواء في الوقت الحاضر أو في المستقبل، دون أي قيود.

يرغب المستهلكون في أن تتواصل جميع أجهزتهم المنزلية اللاسلكية معاً بطريقة "التوصيل والتشغيل" (Plug-and-Play)، دون الحاجة إلى عناء التأكد من أن جهاز إنترنت الأشياء الجديد الذي يرغبون بشرائه سيعمل مع شبكتهم الحالية. فهم يريدون أن يتمكنوا من شراء أي منتج لاسلكي ويعمل تلقائياً. لكن، اليوم، هذا غير ممكن.

فعلى سبيل المثال، يصبح شراء قفل باب ذكي أو لمبة إضاءة متصلة بالإنترنت أمراً معقداً، لأن المستخدم بحاجة إلى التفكير بكيفية تواصل هذا الجهاز مع الأجهزة المنزلية الأخرى، بما في ذلك تلك التي تستخدم Alexa أو Google Assistant أو Siri.

بعض الشركات المصنعة تعتمد على المعايير اللاسلكية الأساسية لتأمين الاتصال، لكنها تضيف حلولاً خاصة بها (Proprietary Solutions) للتحكم والتفاعل مع أجهزة إنترنت الأشياء. غير أن هذا النهج له ثمن، خصوصاً بالنسبة للمستخدمين الذين يواجهون صعوبة أثناء عملية الشراء أو التثبيت، لأن أجهزتهم الجديدة لا تندمج بسهولة كما كانوا يتوقعون مع شبكتهم الحالية.

**فحص بنية إنترنت الأشياء (IoT Architecture) :**

بعض تطبيقات إنترنت الأشياء أصبحت واقعاً بالفعل، مثل القدرة على التحكم في منظم حرارة المنزل لاسلكياً أو استخدام الهاتف لفتح أبواب السيارة. لكن التطبيقات المستقبلية المحتملة لإنترنت الأشياء أوسع وأكبر بكثير.

هذه التطبيقات المستقبلية ستتطلب منصات بنية لإنترنت الأشياء قادرة على تنفيذ عمليات ضخمة من نقل البيانات ومعالجتها في الخلفية.

تتألف منصة/معمارية إنترنت الأشياء (IoT Platform/Architecture) من عدة طبقات مترابطة داخلياً (انظر الشكل 1-1). فيما يلي نظرة أقرب على المكوّنات الفردية الموجودة ضمن هذه الطبقات:

المستشعرات والمشغلات (Sensors and Actuators): تقوم مستشعرات ومشغلات إنترنت الأشياء بقياس عناصر مثل درجة الحرارة، الصوت، الرطوبة، والاهتزاز.

في منزل ذكي نموذجي، يحتوي جهاز ذكي مثل منظم الحرارة (Thermostat) على وحدة اتصال مدمجة تتصل بشبكة المنزل. تقوم هذه المستشعرات والمشغلات بتحويل هذه القياسات الفيزيائية إلى قيم كهربائية تُشغّل النظام.

بوابات إنترنت الأشياء (IoT Gateways): تعمل البوابة على نقل البيانات بين الشبكة المحلية والإنترنت. حيث تُستقبل القيم الكهربائية من المستشعرات والمشغلات ثم تُرفع إلى الشبكة المحلية باستخدام بروتوكولات شبكية مثل Bluetooth، أو Bluetooth Low Energy (BLE)، أو Cellular، أو LoRaWAN، أو Thread، أو Wi-Fi، أو Zigbee. تنشئ البوابة عموداً فقرياً شبكياً مترابطاً (Meshed Backbone) لتوزيع البيانات المجمّعة وإرسال الاستجابات إلى الأجهزة.

منصة إنترنت الأشياء السحابية (Cloud-based IoT Platform): يتم تخزين البيانات المُرسلة عبر البوابة ومعالجتها ضمن منصة سحابية لإنترنت الأشياء أو في مراكز بيانات الشركة. ثم تُستخدم هذه البيانات لتنفيذ إجراءات ذكية واتخاذ القرارات.

التطبيقات (Applications): في النهاية، تُستخدم البيانات القادمة من أجهزة إنترنت الأشياء ضمن التطبيقات لمساعدة الأفراد أو المؤسسات على اتخاذ قرارات أفضل أو القيام بإجراءات محددة. تقوم هذه التطبيقات بدفع المعلومات من السحابة إلى تطبيقات على الهواتف الذكية أو الأجهزة اللوحية أو الحواسيب. تُعد طبقة التطبيقات الأهم بالنسبة للمستخدمين لأنها تمثل واجهتهم مع شبكة إنترنت الأشياء، مما يمكّنهم من التحكم ومراقبة العديد من عناصر النظام، أحياناً بشكل لحظي (Real-time).

**بروتوكولات إنترنت الأشياء (IoT Protocols)**

تشكل بروتوكولات الاتصال العمود الفقري لأنظمة إنترنت الأشياء، حيث تربط أجهزة إنترنت الأشياء بالشبكة وفي النهاية بالتطبيقات والمستخدمين. تتيح هذه البروتوكولات ـ سواء كانت قائمة على معايير قياسية أو بروتوكولات خاصة (Proprietary) ـ تمرير البيانات بين الطبقات المختلفة لبنية إنترنت الأشياء، من خلال تحديد صيغ تبادل البيانات، وترميزها، وآليات عنونة الأجهزة، والطريقة التي تُوجَّه بها حزم البيانات من العقدة (Node) إلى الوجهة.

تتضمن منظومة إنترنت الأشياء مجموعة متنوعة من البروتوكولات التي تدعم الشبكات قصيرة المدى، والمحلية، وواسعة النطاق، وجميعها تتعايش معاً. وتتمتع كل تقنية بخصائص محددة من حيث النطاق (Range)، وقدرات الاستشعار والتحكم، والقدرة على نقل أنواع مختلفة من المعلومات (الشكل1-2 ).

معاً، يمكن لهذه التقنيات أن توفر تغطية سلسة عبر جميع النطاقات والقدرات اللاسلكية. فعلى سبيل المثال: يعمل Bluetooth بكفاءة في التطبيقات قصيرة المدى، بينما يُستخدم Narrowband IoT (NB-IoT) بشكل جيد في التطبيقات بعيدة المدى.

**ملخص حول بعض بروتوكولات الشبكات الرئيسية:**

معيار IEEE 802.15.4: هو مجموعة من معايير الشبكات الشخصية اللاسلكية منخفضة المعدل (LR-WPAN). توفّر هذه المعايير اتصالات منخفضة التكلفة ومنخفضة السرعة للأجهزة محدودة الطاقة. وهي تُشكل الأساس للمواصفات الخاصة ببروتوكولات اتصال عالية المستوى مثل Zigbee. يُعد Zigbee شبكة متشابكة (Mesh Network) مصممة للعمل منخفض الاستهلاك للطاقة، وتُستخدم في المنازل الذكية وفي تطبيقات الطاقة الذكية الخاصة بالمرافق. يستند Zigbee إلى طبقة الفيزيائية (PHY) وطبقة التحكم بالولوج للوسط (MAC) من معيار IEEE 802.15.4.

Wi-Fi: هو مجموعة من معايير الاتصال اللاسلكي ضمن الشبكات المحلية (WLAN) التي وضعتها IEEE 802.11. يوفر Wi-Fi معدلات بيانات عالية لكل من البيئات الداخلية والخارجية، ويُعد واسع الاستخدام عالمياً.

Bluetooth: معيار مفتوح تديره مجموعة الاهتمام الخاصة بالبلوتوث (Bluetooth SIG). يُعتبر تقنية اتصال لاسلكي منخفضة التكلفة مناسبة لنقل البيانات بين الأجهزة المحمولة لمسافات قصيرة تتراوح بين 8 و 10 أمتار. يُستخدم في تطبيقات مثل بث الصوت، السيارات، مكبرات الصوت، وسماعات الرأس.

Bluetooth Low Energy (BLE): جزء من معيار البلوتوث صُمم خصيصاً لتقليل استهلاك الطاقة. غالباً ما تستخدم أجهزة BLE بطاريات صغيرة من نوع (Coin Cell). يُستخدم BLE في أجهزة إنترنت الأشياء مثل المصابيح الكهربائية ومفاتيح الإضاءة.

Thread: تقنية شبكات متشابكة (Mesh Networking) آمنة ومنخفضة الاستهلاك للطاقة، قائمة على بروتوكولات الإنترنت، مخصصة لمنتجات إنترنت الأشياء.

في عام 2014،تم إنشاء مجموعة Thread Group لدعم اعتماد هذه التقنية. يدعم Thread معايير الاتصال الحالية القائمة على IPv6 ضمن شبكته المؤمنة والمنخفضة الطاقة.

LoRa: بروتوكول للشبكات واسعة النطاق منخفضة الطاقة (LPWAN) طُوّر من قبل LoRa Alliance. يُعد مثالياً لتمكين أجهزة الاستشعار في تطبيقات الزراعة واسعة النطاق بفضل قدرته على الاتصال لمسافات طويلة مع استهلاك منخفض للطاقة.

المعايير الخلوية (Cellular Standards): مثل الجيل الخامس (5G)، والتي توفّر العمود الفقري لشبكات إنترنت الأشياء، حيث تدعم كلّاً من معدلات البيانات العالية والاتصالات بعيدة المدى. من أكثر المعايير استخداماً في هذا المجال معيار NB-IoT، ويُستخدم في مواقف السيارات الذكية، وإدارة المرافق، وأتمتة عمليات التصنيع.

تُستخدم بروتوكولات المراسلة هذه لمشاركة البيانات عبر الأجهزة ومع السحابة. وتُعد بروتوكولات إنترنت الأشياء جزءًا أساسيًا من حزمة تقنيات إنترنت الأشياء، وبدونها لن تعمل الأجهزة المادية على الإطلاق. تمكّن بروتوكولات إنترنت الأشياء الجهاز من تبادل البيانات بطريقة مضبوطة وذات معنى.

على سبيل المثال، تُسمّى أجهزة إنترنت الأشياء "ذكية" لأنها لا تكتفي بالتحدث مع بعضها البعض، بل إذا واجهت مشكلات فإنها تستطيع تلقائيًا التخفيف من أثر المشكلة أو طلب المساعدة عبر الشبكة. إن هذا التفاعل لا يكون ممكنًا إلا من خلال بروتوكولات الاتصال أو اللغة المشتركة التي تُزوَّد بها أجهزة إنترنت الأشياء.

**القسم الثاني: المنازل الذكية**

في هذا القسم، سوف نتعمق في كيفية دعم إنترنت الأشياء للمنزل الذكي، وكيف تُمكّن الشبكات الشبكية / الموحدة ان تكون واحدة لكل غرفة من الاتصال بإنترنت الأشياء. كما أتناول بعض تحديات إنترنت الأشياء، وكيف تُساعد التطورات التكنولوجية الجديدة في معالجتها.

**وضع المنازل الذكية اليوم :**

شهد مفهوم المنزل الذكي رواجًا كبيرًا خلال السنوات القليلة الماضية، حيث طوّر المصنّعون مجموعة متنامية من الأجهزة التي يمكنها الاتصال بشبكات المنازل. تُمكّن شبكات المنازل الذكية أصحاب المنازل من استخدام الموارد بكفاءة، والتحكم في الأجهزة والأدوات باستخدام الأوامر الصوتية، واتخاذ القرارات بناءً على البيانات الواردة منها. وتتمتع المنازل الذكية بإمكانيات هائلة: إذ يُمكن استخدامها لتحسين كفاءة الطاقة، والراحة، والأمان، والترفيه، والرفاهية.

معظم المنازل الذكية اليوم مُجهزة بالعديد من أجهزة إنترنت الأشياء، والمحاور، وأجهزة الاستشعار التي تتواصل عبر شبكة/بوابة المنزل، وفي نهاية المطاف مع السحابة. ويمكن للمالك التحكم في كل ذلك من أي مكان في المنزل، أو حتى عن بُعد عبر الإنترنت.

قد تتضمن أنظمة المنازل الذكية العديد من معايير الاتصال اللاسلكي ذات الصلة بتطبيقات المنزل. يوضح الجدول خصائص بعض هذه المعايير والاختلافات بينها. علاوة على ذلك، قد تتكون هذه الشبكات المنزلية من عدة شبكات مترابطة تعمل تحت البوابة الرئيسية.

تتكون العديد من المنازل الذكية اليوم من مجموعة مخصصة من العقد. العقدة هي قطعة من الأجهزة لها عنوان فريد على الشبكة؛ ويمكن أن تكون العقدة إما جهازًا أو موزعًا:

» الأجهزة: عادةً ما يكون للجهاز (مثل منظم الحرارة أو مصباح كهربائي) اتصال واحد فقط بالشبكة. قد تحتاج الأجهزة إلى تتبع الوقت الفعلي أو لا، حسب وظيفتها.

» المحاور: المحور هو جهاز يدير حركة مرور الشبكة؛ قد يحتوي على العديد من الاتصالات لأنه يتصل بأجهزة متعددة. يجب أن تتبع المحاور الوقت الفعلي لإرسال الأحداث بكفاءة وفعالية.

» تتكون شبكة المحور الواحد من عقدة محور واحدة وعقدة جهاز واحدة أو أكثر. يدير المحور تبادل الأحداث والمعلومات بين الأجهزة في الشبكة. تحتوي شبكة المحاور المتعددة على أكثر من نوع واحد من المحاور، كما هو موضح في الشكل التالي. يحتوي مخطط الشبكة الموضح في الشكل التالي على محورين، يستخدم كل منهما بروتوكول شبكة مختلفًا (بلوتوث مقابل زيجبي). تتصل الأجهزة الفردية بأحد المحورين. ثم يتصل المحوران بالبوابة، التي يمكنها التواصل مع كليهما.

**الشبكة الشبكية / كبسولة واحدة لكل غرفة :**

لإنشاء منزل ذكي أكثر اتصالاً بشبكة اتصالات أكثر موثوقية، يتجه المستهلكون نحو طوبولوجيا أحدث تُعرف بالشبكة الشبكية، والتي يُشار إليها أحيانًا باسم "كبسولة واحدة لكل غرفة". تُوسّع الشبكات الشبكية نطاقات الأجهزة اللاسلكية بسهولة، وتوفر معدلات بيانات عالية ومتسقة في جميع أنحاء المكاتب والمنازل، وحتى في الهواء الطلق. بالإضافة إلى ذلك، يُمكن للشبكات الشبكية التي تستخدم "كبسولة واحدة لكل غرفة" مع إمكانيات متعددة البروتوكولات أن تُقلل من تكلفة وجود أنظمة شبكية متعددة داخل المنزل.

تُعدّ الشبكات الشبكية تطورًا هامًا في تطور تقنية Wi-Fi، وخاصةً في المنازل الذكية. تتضمن أنظمة Wi-Fi الشبكية جهاز توجيه يتصل باتصال الإنترنت الرئيسي، وأجهزة أو عُقدًا شبيهة بجهاز التوجيه عبر الأقمار الصناعية، موزعة حول المنزل لتوفير تغطية كاملة لإنترنت الأشياء المنزلي بتقنية Wi-Fi (انظر الشكل).

توفر هذه الشبكات الشبكية المتطورة تكرارًا كاملاً، وتُحسّن أداء الشبكة إلى أقصى حد.

كلما زاد عدد العقد، اتسع نطاق الاتصال، كما هو موضح في الشكل 7-1. تُوسّع شبكات الشبكية نطاق الإشارة بفعالية ليشمل منزلًا كاملًا، مما يزيد من الموثوقية ويُتيح التواصل الفوري مع جميع الأجهزة. تسمح التطورات في نشر شبكات Wi-Fi بفصل الطيف وضمان مسارات بيانات مخصصة لنقل المعلومات من وإلى السحابة. كما تُوفر تدفقات بيانات مخصصة للأجهزة. علاوة على ذلك، تُخزّن بعض الأجهزة البيانات، مما يُوفّر على المستخدمين المال، ويُعزز موثوقية الشبكة، ويُمكّن من تطبيقات أكثر ذكاءً تعتمد على البيانات.

يمكن لشبكة الشبكية أن تُهيئ نفسها تلقائيًا. وبالتالي، يمكنها دمج عقدة جديدة في الشبكة الحالية تلقائيًا دون الحاجة إلى تعديل من مسؤول الشبكة. هذا يجعل الشبكة أكثر قابلية للتكيف والتوسع. كما يمكن لشبكة المِشْب أن تُصلح نفسها تلقائيًا من خلال العثور على أسرع وأكثر إشارات موثوقية لنقل البيانات، حتى في حالة حجب إحدى العقد أو فقدانها.

تستخدم العديد من شبكات المِشْب الحالية ما يُسمى ببوابات واي فاي ثلاثية النطاقات والعقد الطرفية. تُحسّن شبكة واي فاي ثلاثية النطاقات سعة البيانات والتغطية باستخدام نطاقات 2.4 جيجاهرتز و5.2 جيجاهرتز و5.6 جيجاهرتز داخل البوابات والعقد الطرفية. في نظام ثلاثي النطاقات، يعمل النطاق الثاني 5.6 جيجاهرتز كخط اتصال مخصص بين جهازي توجيه على الشبكة لتسريع النظام بأكمله بنسبة تصل إلى 180% مقارنةً بالأنظمة القديمة ثنائية النطاقات المُهيأة.

وهكذا، تتضح مزايا واي فاي ثلاثية النطاقات. في البداية، يُسهّل ربط المزيد من الأجهزة اللاسلكية بالإنترنت باستخدام نطاق 5 جيجاهرتز الأسرع، ومع Wi-Fi 6E، نطاقي 5 و6 جيجاهرتز. وإذا كانت شبكتك عبارة عن نظام شبكي مع عدة أجهزة توجيه موزعة في جميع أنحاء المكان، فإن هذا النطاق الأعلى يعمل كخط اتصال مخصص بين جهازي التوجيه لتسريع النظام بأكمله.

يُستخدم أيضًا الراديو الثالث في نظام ثلاثي النطاق لنقل الاتصالات بين أجهزة توجيه الشبكة الشبكية. لذا، يُنشئ سلكًا مخصصًا فقط لغرض تدفق البيانات بين أجهزة التوجيه. على الرغم من أن أنظمة النطاق المزدوج تستخدم نفس نطاق Wi-Fi للاتصال بأجهزة التوجيه ونقاط الوصول الأخرى، إلا أنه في النطاق الثلاثي، تكون الأجهزة الطرفية متاحة فورًا للاتصال. وهذا يُحسّن الكفاءة بنسبة 50%، خاصةً مع إضافة المزيد من أجهزة الشبكة.

بالإضافة إلى ذلك، نظرًا لأن سرعة الراديو هذه أسرع، فإن سرعات الاتصال العالية الموجودة في مودم DSL/الكابل لا تتوقف عند هذا الحد. بل إنها تنتقل إلى الشبكة بأكملها. هذا مفيد جدًا لبث فيديو Wi-Fi إلى أجهزة التلفزيون الذكية والكاميرات المنتشرة في جميع أنحاء المنازل الذكية اليوم وغدًا.

لضمان مستقبل نظام شبكتك المنزلية الحالي، ستحتاج إلى استخدام نظام ثلاثي النطاقات. ستصبح خدمات الجيجابت قريبًا واقعًا ملموسًا للجميع، وتطبيق نظام ثلاثي النطاقات هو أفضل طريقة لضمان السعة والسرعة في المستقبل.

من التطورات الرئيسية الأخرى في أنظمة الشبكات الشبكية إدخال تقنية المرشحات لزيادة سعة ونطاق طوبولوجيا "كبسولة واحدة لكل غرفة". يساعد استخدام مرشحات bandBoost على تعظيم السعة والنطاق من خلال تعزيز عزل النطاق في أنظمة الشبكات ثلاثية النطاقات. كما يعزز استخدام مرشحات edgeBoost السعة والنطاق من خلال تعظيم طاقة الخرج في قنوات Wi-Fi القريبة من حافة النطاق.

سنتناول هذه المواضيع بمزيد من التفصيل، بالإضافة إلى كيفية معالجتها لتحديات التعايش في الشبكات الشبكية في القسم التالي.

كما نوقش في الفصل الأول، تعمل كبرى الشركات المصنعة على تطوير معيار جديد يُسمى Connected Home over IP (CHIP) لزيادة قابلية التشغيل البيني للأجهزة وتقليل التعقيد في الشبكات الشبكية.

خلال عملية الانتقال إلى CHIP، ستكون هناك حاجة إلى أجهزة راديو متعددة المعايير. ستُهيئ هذه الأجهزة الشبكة للمستقبل لدعم الانتقال إلى CHIP وتوفير التوافق مع الإصدارات السابقة لتوصيل العقد التي تستخدم المعايير القديمة. على الرغم من أن CHIP لا يزال قيد الإعداد، حيث من المتوقع طرحه في وقت ما في عام 2021، إلا أن التعاون بين هيئات المعايير والشركات المصنعة الرائدة يدفع إلى زيادة اعتماد الصناعة .

**التغلب على التحديات :**

الان سنقوم بعرض بعض التحديات التي تواجه مصنعي شبكات وأجهزة إنترنت الأشياء المنزلية الذكية.

**التوافقية :**

التوافقية هو قدرة الأنظمة والتطبيقات والخدمات على العمل معًا بشكل موثوق وبطريقة متوقعة. يساعد هذا على ضمان سهولة استخدام التكنولوجيا وتسريع اعتمادها. يتوقع كل مستخدم أن تتصل أجهزته الإلكترونية، السلكية واللاسلكية، بسهولة وتعمل معًا بأقل جهد، وهو ما يُعرف باسم "التوصيل والتشغيل". والأمر لا يختلف في شبكة المنزل الذكي، التي تتكون من العديد من الأجهزة التي طورتها العديد من الشركات المصنعة المختلفة. تساعد برامج التوافقية والاعتماد على ضمان التوافق التشغيلي بين الأجهزة التي تستخدم العديد من معايير إنترنت الأشياء الرئيسية. ويعود نجاح واي فاي الكبير إلى برنامج التوافق التشغيلي الذي يديره تحالف واي فاي، الذي يتمتع بأحد أكثر أنظمة الاعتماد موثوقية في العالم. وهناك عشرات الآلاف من أجهزة واي فاي المعتمدة التي تتميز باتصال سلس ومُثبت.  
اليوم، يوفر Zigbee 3.0 نفس مستوى التوافق التشغيلي، بفضل الشراكات والشهادات. كما أن الاتصال بين المنتجات التي تستخدم Zigbee وThread معتمد أيضًا بفضل الشراكات بين المجموعتين. كما يوفر Bluetooth برامج اعتماد تغطي حزمة البروتوكولات بأكملها، بالإضافة إلى ملف تعريف التطبيق، مما يساعد Bluetooth وBluetooth Low Energy (BLE) على تحقيق تجربة اتصال مثالية.

كانت هذه التحالفات والشهادات حاسمة في توفير التكامل في بيئة أجهزة إنترنت الأشياء المنزلية الذكية المجزأة ذات المعايير المتعددة. يجب على مصنعي الأجهزة التي تستخدم هذه البروتوكولات المتعددة الالتزام بمعايير الاعتماد والتحالف هذه للحصول على موافقة منتجاتهم قبل طرحها في السوق. وهذا يضمن حصول المستخدمين على التوافق التشغيلي الفوري الذي يتوقعونه.

**تداخل الترددات الراديوية :**

ازداد تعقيد التداخلات اللاسلكية (RF) في شبكات المنزل الذكي مع كل جيل جديد من التقنيات اللاسلكية. تستخدم العديد من أجهزة الاتصال اللاسلكي المنزلية معايير تعمل على نطاقات تردد متداخلة أو قريبة جداً من بعضها، وأحياناً تكون هذه النطاقات قريبة لدرجة أنها تسبب تداخلًا يؤثر على إشارات الإرسال والاستقبال الخاصة بالنطاق الآخر.

يُضيف كل من IoT و 5G مستوى آخر من التعقيد، مما يزيد من التحديات التي يواجهها مهندسو تصميم الأجهزة المنزلية الذكية. يجب على أجهزة IoT المنزلية الذكية اليوم أن تدعم العديد من المسارات اللاسلكية (RF paths) ، مع نطاقات تردد أكبر في بعض الأحيان، وأن تحافظ في الوقت نفسه على استهلاك منخفض للطاقة، كل ذلك دون حدوث تداخل بين المعايير والبيانات التي يتم إرسالها أو استقبالها. ومع وجود الكثير من المعايير التي تعمل على شبكة واحدة، أصبح تقليل التداخل أمراً حتمياً.

**الحفاظ على اتصال سلس، موفر للطاقة، وموثوق :**

تصنع بعض الشركات منتجات تدعم عدة معايير، مما يزيد من إمكانية التشغيل البيني في شبكات إنترنت الأشياء (IoT)، لأن ذلك يمكّن منتجاتها من الاتصال بمجموعة أكبر من الأجهزة الأخرى. فمع خاصية دعم البروتوكولات المتعددة (dynamic multi-protocol support)، يمكن للعقدة (node) التواصل مع أجهزة متعددة تستخدم معايير مختلفة.

على سبيل المثال، قد تتضمن شبكة المنزل الذكي أجهزة Zigbee و أجهزة BLE. في هذه الحالة، يمكن للعقدة الشبكية التي تدعم البروتوكولات المتعددة لكل من Zigbee و BLE، أن تقوم بتحويل الاتصال تلقائياً بين هذه المعايير، لتتواصل مع كل معيار على حدة في لحظة معينة.

وتضيف منتجات الاتصالات لإنترنت الأشياء من Qorvo، والتي تستخدم في الأجهزة المنزلية الذكية، قدرة إضافية عبر دعم تقنية ConcurrentConnect التي تستقبل وتترجم الاتصالات بشكل مستمر، كما هو موضح في الشكل 3-6. هذا الابتكار الإضافي يطبق خاصية تبديل البروتوكولات بطريقة أسرع وأكثر موثوقية لتقليل فقدان حزم البيانات، مع الحفاظ على دعم البروتوكولات المتعددة.

على سبيل المثال، وبالإشارة إلى الشكل 3-6، نرى في الجهة اليسرى أن منتجات اتصالات إنترنت الأشياء (IoT) تتضمن ميزة دعم البروتوكولات المتعددة **(**dynamicmultiprotocol support). هذا الدعم يسمح بالاتصال بين عدة أجهزة IoT تستخدم معايير مختلفة، مما يتيح التبديل من بروتوكول لآخر عند الحاجة.

لكن شركة Qorvo تضيف مستوى آخر من التعقيد في أجهزتها اللاسلكية (RF) الخاصة بإنترنت الأشياء، وهو ما يُعرف بتقنية ConcurrentConnect. هذه التقنية تجعل اتصالات أجهزة IoT أكثر موثوقية وسلاسة، لأنها تضيف القدرة على استقبال وإرسال اتصالات الأجهزة من كل الشبكة بشكل مستمر ومتزامن. وبالتالي، يصبح التبديل بين كل بروتوكول سلساً، مما يلغي الحاجة إلى إعادة إرسال "ping" ويمنع انقطاع الاتصالات المحتمل.

لنأخذ مثالاً على شبكة فعلية: بدون تقنية ConcurrentConnect، فإن أجهزة Zigbee**/**CHIP و( Bluetooth Low Energy (BLEستتبادل الاتصال بين المعيارين، وتتواصل مع أحدهما في كل مرة. لكن هذا التبديل بين البروتوكولات يسبب تأخيراً يؤدي إلى انقطاع الاتصالات. في المقابل، تسمح الأجهزة المزودة بتقنية ConcurrentConnect بالتبديل الفوري من BLE إلى Zigbee/CHIP مع القليل من الانقطاعات أو عدم وجودها على الإطلاق. وهذا لأن تقنية ConcurrentConnect تقضي على التأخير في تبديل البروتوكولات. وبذلك تصبح الاتصالات أسرع، وأكثر كفاءة، وأكثر قابلية للتوسع، وقادرة على استقبال عدد أكبر من حزم البيانات في وقت أقصر.

**إنشاء شبكة إنترنت أشياء سهلة الاستخدام ذاتية الإدارة :**يرغب معظم مستخدمي شبكات إنترنت الأشياء (IoT) في تجربة "التوصيل والتشغيل" (plug-and-play) التي تتطلب إعداداً بسيطاً أو معدوماً. كل ما نريده هو أن تعمل الأجهزة بمجرد تشغيلها. وهذا يضع مسؤولية سهولة الاستخدام على عاتق الشركة المصنعة للمنتج. وهذا التحدي ليس سهلاً دائماً، لأن شبكة كل مستخدم تختلف عن الأخرى.

ولتحقيق هذا الهدف، يجب أن تكون شبكة IoT الشبكية (mesh network) في المنزل ذاتية الإدارة وذاتية المعالجة، حتى يطمئن المستخدمون إلى استمرار عملها دون الحاجة إلى التدخل في التفاصيل التقنية لإدارة الشبكات. يجب أن تكون شبكة IoT قادرة على العمل ومراقبة المستخدمين وإخطارهم بالمشكلات المحتملة التي قد تحدث قبل حدوث انقطاع كامل للشبكة.

يجب أن تعمل العقد الفردية (individual nodes) والبوابات (gateways) مع بعضها البعض وتتكيف مع أي أعطال في الشبكة أو تغييرات بيئية. وتقوم الأنظمة الفرعية في شبكة المنزل الذكي بمراقبة قوة الإشارة، وعمر البطارية، والمزيد، حيث تتكيف باستمرار وتخطر المستخدم لضمان أفضل أداء.

تُقدم الشبكات الشبكية (mesh networking) مزايا حقيقية لتطبيقات إنترنت الأشياء، لأنها متاحة وسهلة الوصول دائماً. تستخدم الشبكة الشبكية خوارزمية "الشفاء الذاتي" (self-healing algorithm) التي تختار تلقائياً أفضل مسار لإرسال البيانات حتى لو فقدت بعض العقد اتصالها عن غير قصد. وتضمن هذه الخوارزمية أن يتم توجيه البيانات فقط عبر الاتصالات المتاحة والعاملة. وهكذا، تستمر الشبكة الشبكية في العمل حتى عندما لا تكون بعض العقد فعالة. كما تتيح الشبكات الشبكية للأجهزة أن تتواصل مباشرة مع بعضها البعض دون الحاجة إلى توجيه كل الاتصالات عبر البوابة (gateway).

**أمان الشبكة والخصوصية :**

يمكن أن يشكل تطبيق إجراءات الأمن والخصوصية الكافية تحديًا كبيرًا عند نشر أنظمة إنترنت الأشياء (IoT). فشبكات IoT اليوم غالبًا ما تكون مجزأة وتستخدم مجموعة متنوعة من البروتوكولات والتقنيات، مما يجعل التحكم في الأمن والخصوصية أمرًا صعبًا.

هذا الواقع يمثل حجة قوية لتوحيد المعايير (standardization)، الأمر الذي سيساعد على تحسين الأمن والخصوصية. كما أنه سيوفر سهولة أكبر في الاستخدام وقابلية للتوسع، مما يمكّن المستخدمين من إضافة أجهزة بسهولة إلى الشبكة. ويسهم التوحيد في مساعدة المستخدمين على إنشاء تصميم شبكة IoT الأمثل الخاص بهم بطريقة آمنة.

إن استخدام الشبكة الشبكية (mesh network)، كما وُصف سابقًا، يضع قوة التحكم والأمان في يد المالك. وعادةً ما يتم إعداد هذه الأنظمة الشبكية والتحكم بها ومراقبتها باستخدام تطبيق خاص. يساعد التطبيق في إعداد الشبكة ويضمن تعيين كلمة مرور آمنة. كما يساعد في إدارة مشكلات الشبكة، والتحقق من سرعات البيانات، ووضع parental controls (أدوات الرقابة الأبوية)، والمزيد. وتساعد بعض الأنظمة المالك على معرفة من هو المتصل بالشبكة في أي وقت.

تحديثات جهاز الكمبيوتر والهاتف الذكي ضرورية للحفاظ على أمان هذه الأجهزة. الأمر نفسه ينطبق على الشبكة الشبكية. لكن الشبكة الشبكية عادةً ما تقوم بتحديث نفسها تلقائيًا، مما يريح المالك من القلق بشأن إجراء تحديثات مزعجة.

تقدم بعض الشبكات الشبكية أيضًا رسوم اشتراك مدفوعة للحصول على ميزات أمان محسّنة، مثل الحماية من المتسللين وتهديدات المواقع الإلكترونية والفحوصات الأمنية. وقد تتضمن هذه الاشتراكات أيضًا الحماية من التهديدات مثل البرامج الضارة (malware) والفيروسات والمتسللين وحتى مجرمي الإنترنت.

إذا كان لديك منزل ذكي مزود بكاميرات أمنية متصلة بالشبكة، وأجهزة ترموستات، وأجهزة IoT ذكية أخرى، فإن نظام الشبكة الشبكية يُعد إضافة مفيدة جدًا. فميزات النظام الشبكي يمكن أن تساعد في حماية الشبكة بأكملها، بما في ذلك هذه الأجهزة، من الهجمات الإلكترونية.

**استهلاك الطاقة :**

تتضاءل مستويات الوقود الأحفوري في جميع أنحاء العالم بسرعات متزايدة. ويتزايد الضغط لتقليل استهلاك الطاقة وتقديم منتجات أكثر صداقة للبيئة. هذا الضغط نفسه يقع على عاتق الشركات المصنعة والموردين الذين ينتجون أجهزة إنترنت الأشياء (IoT) اليوم، وهذا التوجه سيزداد حدةً مع دفع قادة العالم للمزيد من المبادرات الخضراء.

تستخدم بعض منتجات IoT بطاريات بحجم العملة المعدنية (تدوم بعضها حتى عشر سنوات)، ولكن إنتاج هذه البطاريات يستهلك الوقود الأحفوري. بالإضافة إلى ذلك، لا تستخدم العديد من أجهزة IoT بطاريات بحجم العملة المعدنية؛ بل تستخدم الطاقة من الشبكة الكهربائية (grid). لذا، وللحفاظ على متطلبات استهلاك الطاقة تحت السيطرة، يتم أحياناً إضافة برامج وأجهزة إلى بعض أجهزة IoT هذه لضمان بقائها في وضع السكون (sleep mode) عندما لا تكون في حالة اتصال.

في بيئات التصنيع، لا تقتصر فوائد أجهزة تقنية IoT على دفع عجلة الكفاءة والأتمتة بشكل غير مسبوق فحسب، بل يجب أيضًا تصميم هذه الأجهزة لتستهلك طاقة أقل أثناء التشغيل. وقد وضعت الشركات المصنعة لأجهزة IoT بالفعل نصب أعينها إنتاج منتجات تستهلك طاقة أقل. وبذلك، تصبح منتجاتهم أكثر كفاءة وأصغر وأكثر أناقة. الجميع يربح من محاولة إنتاج أجهزة تستخدم طاقة أقل أثناء التشغيل، سواء كان المستهلك، أو الشركة، أو المصنِّع.

يمكن للعديد من الشركات الاستفادة من وضع إنترنت الأشياء (IoT) في طليعة الطاقة المتجددة. يمكن لتطبيق حساسات IoT على معدات التوليد والنقل والتوزيع أن يمكّن من مراقبة الأصول وإدارتها عن بُعد. بالإضافة إلى ذلك، يمكن أن يساعد تركيب IoT في جميع أنحاء بيئة التصنيع في تقليل التكاليف المرتبطة بالإضاءة والتدفئة والتبريد والسلامة.

يمكن لشبكة المنزل الذكي أن تتضمن العديد من أجهزة الاتصال التي تعمل على مدار الساعة طوال أيام الأسبوع (24/7). ولأن هذه الأجهزة تستهلك الطاقة حتى عندما لا تتصل بشكل فعال، فإن الكفاءة واستهلاك الطاقة سيظلان دائمًا مصدر قلق في التصميم. ويجب تحسين أجهزة IoT لتكون ذات كفاءة في استهلاك الطاقة بغض النظر عن البروتوكول الذي تستخدمه.

سنعرض الان ملخص عالي المستوى لاستهلاك الطاقة في المعايير المختلفة: WiFi و CHIP(Zigbee, Thread) لهما نطاق إشارة متشابه، لكن WiFi يستهلك طاقة أكبر بكثير بسبب دعمه لنطاق البيانات العالي.

تستهلك CHIP (Zigbee, Thread) و BLE طاقة متشابهة، وقد تم تطويرهما للحفاظ على طاقة البطارية.

* تستهلك CHIP (Zigbee, Thread) حوالي 1% إلى 3% من الطاقة التي يستهلكها Wi-Fi، وهذا يعتمد على التطبيق.

مع تطبيق المبادرات الخضراء على مستوى العالم، أصبح تقليل استهلاك الطاقة عبر شبكة إنترنت الأشياء (IoT) أمرًا ضروريًا. ويسعى كل من المستخدمين والشركات المصنعة لتحقيق استهلاك أقل للطاقة دون المساس بالأداء أو بأهداف الاتصال الشاملة لأجهزة IoT. ويمكن للأجهزة أن تضمن استمرار عملها من خلال إشعار المستخدمين تلقائياً عندما تحتاج البطاريات إلى استبدال.

**أهمية الاتصال الدائم :** توسعت شبكات إنترنت الأشياء (IoT) في المنزل ومكان العمل بشكل كبير خلال السنوات القليلة الماضية. وفي الوقت نفسه، ازداد اعتمادنا على هذه الشبكات. يعمل المزيد من الأشخاص من مكاتبهم المنزلية، وتستخدم العائلات شبكاتها المنزلية لإجراء مكالمات الفيديو، والألعاب، ومشاهدة التلفزيون، ومراقبة صحتهم، وتأمين منازلهم. هناك حاجة حقيقية لاتصالات موثوقة، مستمرة، وذات زمن انتقال منخفض (low-latency) لضمان دعم هذه الاستخدامات على مدار الساعة.

لحسن الحظ، يستجيب مزودو الخدمات اللاسلكية في جميع المناطق بعمليات طرح جديدة، بما في ذلك الانتقال إلى شبكات . 5G لم نعد بحاجة للقلق بشأن الاتصال أو سرعة نقل البيانات. بدلاً من ذلك، ستتركز اهتماماتنا على خصائص الشبكة ذات المستوى الأعلى مثل الخصوصية والأمان، خاصةً مع تزايد اعتمادنا على شبكات IoT للمنزل الذكي، والمدينة الذكية، والصناعة 4.0، و V2X، وغيرها من جوانب حياتنا. هذه الاهتمامات الجديدة تدفع جميع الشركات المصنعة ومقدمي الخدمات اللاسلكية للاستجابة من خلال وضع الأمان في صدارة تصميمات شبكاتهم وأجهزتهم.

يسمح العالم الرقمي الجديد للشركات والمستهلكين بالبقاء على اتصال دائم. يقضي مستخدمو IoT المتصلون بشكل كبير معظم أيامهم على الإنترنت، سواء في العمل، أو الدراسة، أو اللعب، أو استخدام وسائل التواصل الاجتماعي، وغيرها. لا نقتصر على قضاء 8 ساعات أو أكثر يومياً على الإنترنت، بل أجهزتنا IoT أيضًا تعمل على مدار الساعة. هذه التفاعلات عبر حساساتنا وكاميراتنا متصلة بالإنترنت طوال الوقت، وهذه الحساسات والكاميرات وأجهزة المراقبة تدفعنا أكثر نحو سيناريو الاتصال الدائم، خاصةً في عالم IoT .

هذا العالم الرقمي ديناميكي ويسمح لنا بالعديد من قنوات الاتصال المختلفة، وأهمها الإنترنت و IoT . الاتصال عبر الإنترنت اليوم سريع، وبسيط، وفوري، ويضمن أن تكون المعلومات والبيانات متاحة دائمًا تحت تصرفنا.

في عالم الأعمال، يتيح الاتصال الدائم (24/7) للمديرين والموظفين وأصحاب المصلحة وسلاسل التوريد الحصول على المعلومات المحدثة والاطلاع عليها في الوقت الفعلي. عندما تكون خارج المكتب، لا تحتاج أن تكون منقطعًا عن ما يحدث. ستكون المنتجات الخاصة بالصناعات هي السباقة في استخدام IoT، ولكن بمساعدة الصناعة 4.0، والمدفوعة بالبحث عن كفاءة التصنيع وإدارة التكاليف، أصبح المستهلكون أيضًا جزءًا أساسيًا من عالم IoT.

يشتري المستهلكون مليارات الوحدات لتثبيتها داخل منازلهم لمراقبة وتحديث كل شيء تلقائيًا ويدويًا، وكل ذلك على أمل الحصول على الراحة والأمان والصحة وتقليل التكاليف. يعد IoT للمستهلكين بجعل بيئاتنا ومنازلنا ومركباتنا أكثر ذكاءً، وأكثر قابلية للقياس، وأكثر قدرة على الاتصال. إنه يعمل دائمًا وينتظر منا التواصل، مثل Amazon's Alexa أو Echo، أو يراقب دائمًا ما يحدث لمساعدتنا على اتخاذ قرارات أفضل بشأن بيئاتنا المنزلية والأنشطة المرتبطة بها.

يُولد IoT كميات هائلة من البيانات لأنه يعمل 24/7، باستخدام حساسات مثبتة على أجزاء الآلات أو حساسات بيئية أو مكبر الصوت الذكي داخل غرف المعيشة. وهذا يعني أن IoT هو محرك كبير لإنشاء كم هائل من تحليلات البيانات للسماح للشركات بالتحليل ولأشياءنا الذكية بأن تصبح أكثر ذكاءً.

تأتي هذه البيانات بأشكال مختلفة، من طلبات صوتية وقراءات حساسات ومقاطع فيديو وغيرها. وتنمو بيانات IoT ، ويتم تغذية هذه البيانات الوصفية (metadata) في قواعد بيانات لإضفاء هيكل على المحتوى غير المهيكل، أو تُغذى في أنظمة معرفية (cognitive systems) لإضفاء مستويات جديدة من اتخاذ القرار والفهم والذكاء على بيئتنا.

كمية اتخاذ القرار والفهم والذكاء التي تحدث حولنا بفضل IoT يمكن أن تكون مذهلة. على سبيل المثال، يندهش العديد من الأشخاص من عدد أجهزة IoT الموجودة على شبكاتهم المنزلية. إذا كان لديك منزل جديد بأجهزة جديدة و Amazon Alexa أو اثنين، فقد يكون لديك قريبًا ما يصل إلى 15 أو 20 جهازًا متصلاً بشبكتك. يمكن أن يظهر لك مسح بسيط للتطبيقات على هاتفك مستوى IoT في منزلك: كاميرا عند بابك الأمامي، وداخل غرفة المعيشة، وفي فنائك الخلفي؛ وتطبيق آخر لغسالتك ومجففك الجديدين، ومن المحتمل أن يكون هناك ثلاجة وفرن وميكروويف؛ و Amazon Alexa أو اثنان حول المنزل. بالإضافة إلى ذلك، ربما لديك تطبيق لبعض الإضاءة في المنزل، وهذا يعني ثلاث أو عشر لمبات أخرى. . . . لقد فهمت الفكرة. اجمعها كلها، وقد يكون لديك 10 إلى 20 جهاز IoT منتشرًا، وعلى الأرجح ساعتان ذكيتان أو ثلاثة أو Fitbits متصلة ببضعة هواتف وأجهزة لوحية. هذه الأجهزة تعمل دائمًا وتتصل بشبكتك وببعضها البعض. أجهزة IoT تعمل دائمًا وتستشعر وتراقب وتتخذ القرارات لنا ومعنا. يمكن أن يكون مسح بسيط كهذا مذهلاً ورائعًا في الوقت نفسه، حيث يظهر لك أن IoT موجود في كل مكان حولك.

**القسم الثالث: - أنظمة كشف التطفل (IDS):**

**مقدمة عن أنظمة كشف التطفل (IDS) :**

يمثل التطور المستمر للبرمجيات الخبيثة تحديًا جوهريًا أمام تصميم أنظمة كشف التطفل (IDS). فالهجمات الخبيثة باتت أكثر تعقيدًا، والتحدي الأكبر يكمن في اكتشاف البرامج الخبيثة المجهولة والمموّهة. يلجأ مصممو هذه البرامج إلى استخدام تقنيات تمويه متقدمة لإخفاء المعلومات، بهدف تجنب الاكتشاف من قبل أنظمة IDS.

علاوة على ذلك، شهدنا ازديادًا ملحوظًا في التهديدات الأمنية، مثل هجمات على ثغرات غير مكتشفة بعد (Zero-day attacks)، التي تستهدف مستخدمي الإنترنت بشكل مباشر. ولهذا أصبح أمن الكمبيوتر أمرًا لا غنى عنه في حياتنا اليومية التي باتت تعتمد بشكل كبير على تقنية المعلومات.

لقد أثرت الهجمات على الثغرات الغير المكتشفة بعد بشكل كبير على دول مثل استراليا والولايات المتحدة. فوفقًا لتقرير Symantec لأمن الإنترنت لعام 2017، تم الإبلاغ عن أكثر من ثلاثة مليارات هجوم من هذا النوع في عام 2016، مما يؤكد أن حجمها وشدتها فاقا التوقعات السابقة. كما كشفت إحصائيات اختراق البيانات لعام 2017 عن فقدان أو سرقة ما يقرب من تسعة مليارات سجل بيانات على يد المخترقين منذ عام 2013.

تُظهر تقارير Symantec أن حوادث الاختراق الأمني في تصاعد. في الماضي، كان مجرمو الإنترنت يركزون بشكل أساسي على عملاء البنوك لسرقة الأموال من حساباتهم أو بطاقاتهم الائتمانية. لكن الجيل الجديد من البرامج الخبيثة أصبح أكثر جرأة وطموحًا، حيث يستهدف البنوك نفسها، وفي بعض الأحيان يحاول سرقة ملايين الدولارات في هجوم واحد. لهذا السبب، أصبح اكتشاف الهجمات على الثغرات الغير المكتشفة على رأس الأولويات.

أثبتت حوادث الجرائم الإلكترونية البارزة سهولة انتشار التهديدات السيبرانية على المستوى الدولي، حيث يمكن لاختراق بسيط أن يعطل الخدمات أو المرافق الحيوية لشركة ما. يوجد عدد كبير من مجرمي الإنترنت حول العالم، الذين تحفزهم دوافع لسرقة المعلومات، أو الحصول على إيرادات غير شرعية، أو البحث عن أهداف جديدة. يتم تصميم البرامج الخبيثة عمدًا لاختراق أنظمة الكمبيوتر واستغلال أي نقطة ضعف في أنظمة كشف التطفل. في عام 2017، قام المركز الأسترالي للأمن السيبراني (ACSC) بدراسة نقدية لمستويات التعقيد المختلفة التي يستخدمها المهاجمون.

لذلك، هناك حاجة ملحة لتطوير نظام كشف تطفل فعّال يمكنه اكتشاف البرامج الخبيثة المستجدة والمعقدة. يهدف نظام IDS إلى تحديد أنواع مختلفة من البرمجيات الخبيثة في أقرب وقت ممكن، وهو أمر لا يمكن للجدار الناري التقليدي (firewall) تحقيقه. ومع تزايد حجم البرمجيات الخبيثة على أجهزة الكمبيوتر، أصبح تطوير أنظمة IDS محسّنة أمرًا في غاية الأهمية.

في العقود القليلة الماضية، تم استخدام التعلم الآلي لتحسين كشف التطفل، وهناك حاجة حاليًا لتصنيف شامل وحديث، ومسح للأعمال الأخيرة في هذا المجال. هناك عدد كبير من الدراسات ذات الصلة التي تستخدم مجموعة بيانات KDD-Cup 99 أو DARPA 1999 للتحقق من تطوير أنظمة IDS ؛ ومع ذلك ، لا توجد إجابة واضحة على السؤال حول أي تقنيات استخراج البيانات هي الأكثر فعالية. وثانيًا، لا يتم أخذ الوقت اللازم لبناء نظام IDS في الاعتبار عند تقييم بعض تقنيات IDS، على الرغم من كونه عاملاً حاسماً في فعالية أنظمة IDS "اللحظية" (on-line).

تقدم هذه الورقة تصنيفًا محدثًا، بالإضافة إلى مراجعة لأبرز الأبحاث حول أنظمة IDS حتى الوقت الحاضر؛ وتصنيف للأنظمة المقترحة وفقًا للتصنيف. كما تقدم نظرة عامة منظمة وشاملة على أنظمة IDS الحالية حتى يتمكن الباحث من الإلمام بسرعة بالجوانب الرئيسية لكشف الشذوذ. وتقدم هذه الورقة أيضًا مسحًا لتقنيات استخراج البيانات المطبقة لتصميم أنظمة كشف التطفل. وتصف الأساليب القائمة على التوقيعات والقائمة على الشذوذ (SIDS وAIDS)، إلى جانب العديد من التقنيات المستخدمة في كل طريقة. يتم مناقشة تعقيد أساليب AIDS المختلفة وتقنيات تقييمها، يتبعها مجموعة من الاقتراحات لتحديد أفضل الأساليب، اعتمادًا على طبيعة التطفل. كما يتم مناقشة التحديات التي تواجه أنظمة IDS الحالية. مقارنة بالمنشورات الاستقصائية السابقة، تقدم هذه الورقة مناقشة لمشاكل مجموعات بيانات IDS التي تعد مصدر قلق رئيسي للمجتمع البحثي في مجال أنظمة كشف تطفل الشبكة (NIDS). لم تقم الدراسات السابقة بمراجعة شاملة لأنظمة IDS من حيث مجموعات البيانات، والتحديات، والتقنيات. في هذه الورقة، نقدم دراسة منظمة ومعاصرة وواسعة النطاق حول نظام كشف التطفل من حيث التقنيات ومجموعات البيانات؛ ونسلط الضوء أيضًا على تحديات التقنيات ومن ثم نقدم توصيات.

خلال السنوات القليلة الماضية، تم نشر عدد من الأبحاث الاستقصائية حول كشف التطفل. قام المسح حول نظام كشف التطفل وتصنيفه بواسطة (Axelsson (Axelsson , 2000 بتصنيف أنظمة كشف التطفل بناءً على طرق الكشف.

قام المسح الذي تم الاستشهاد به بشكل كبير بواسطة . (Debar et al.، 2000) بمسح طرق الكشف بناءً على سلوك وخصائص الهجمات. وقد قدم تصنيف أنظمة التطفل بواسطة Liao et al

(Liao et al., 2013a) ، تصنيفًا لخمسة فئات فرعية مع منظور متعمق لخصائصها: القائمة على الإحصاء، والقائمة على الأنماط، والقائمة على القواعد، والقائمة على الحالات، والقائمة على الاستدلال. من ناحية أخرى، يركز عملنا على مبدأ كشف التوقيعات، وكشف الشذوذ، والتصنيف، ومجموعات البيانات.

تركز مقالات المراجعة الحالية على تقنيات كشف التطفل، أو مشكلة مجموعة البيانات، أو نوع هجوم الكمبيوتر، أو تجنب IDS. لم تقم أي مقالة بمراجعة شاملة لكشف التطفل، ومشاكل مجموعة البيانات، وتقنيات التجنب، وأنواع مختلفة من الهجمات مجتمعة. بالإضافة إلى ذلك، كان تطوير أنظمة كشف التطفل بحيث تم اقتراح العديد من الأنظمة المختلفة في هذه الأثناء، ولذلك هناك حاجة لتحديث. تقدم هذه الورقة مسحًا محدثًا لتصنيف مجال كشف التطفل، مما يعزز التصنيفات المقدمة في (Liao et al., 2013a; Ahmed et al., 2016).

في ضوء مناقشة الدراسات الاستقصائية السابقة، تركز هذه المقالة على ما يلي:

\* تصنيف أنواع مختلفة من أنظمة IDS مع الأنواع الرئيسية للهجمات بناءً على طرق التطفل.

\* تقديم تصنيف لمقاييس تقييم أنظمة IDS الشاذة للشبكة ومناقشة أهمية اختيار الميزات.

\* تقييم مجموعات بيانات IDS المتاحة ومناقشة تحديات تقنيات التجنب.

يمكن تعريف التطفل بأنه أي نوع من الأنشطة غير المصرح بها التي تسبب ضررًا لنظام المعلومات. هذا يعني أن أي هجوم يمكن أن يشكل تهديدًا محتملاً لسرية المعلومات، أو تكاملها، أو توفرها، سيعتبر تطفلاً. على سبيل المثال، الأنشطة التي تجعل خدمات الكمبيوتر غير مستجيبة للمستخدمين الشرعيين تعتبر تطفلاً. نظام IDS هو نظام برمجي أو مادي يحدد الأنشطة الضارة على أنظمة الكمبيوتر من أجل السماح بالحفاظ على أمن النظام (Liao et al., 2013a). هدف نظام IDS هو تحديد أنواع مختلفة من حركة مرور الشبكة الضارة واستخدام الكمبيوتر، والتي لا يمكن تحديدها بواسطة جدار حماية تقليدي. وهذا أمر حيوي لتحقيق حماية عالية ضد الإجراءات التي تهدد توفر أنظمة الكمبيوتر أو تكاملها أو سريتها. يمكن تصنيف أنظمة IDS بشكل عام إلى مجموعتين: نظام كشف التطفل القائم على التوقيع (SIDS) ونظام كشف التطفل القائم على الشذوذ (AIDS).

**أنظمة كشف التطفل القائمة على التوقيع(SIDS) :**

تعتمد أنظمة كشف التطفل القائمة على التوقيعات (SIDS) على تقنيات مطابقة الأنماط للعثور على هجوم معروف مسبقاً؛ وتعرف هذه الأنظمة أيضاً باسم "الكشف القائم على المعرفة" أو "كشف سوء الاستخدام". في هذه الأنظمة، تُستخدم طرق المطابقة للعثور على تطفل سابق. بعبارة أخرى، عندما يتطابق توقيع تطفل حالي مع توقيع هجوم سابق موجود بالفعل في قاعدة بيانات التوقيعات، يتم إطلاق إشارة إنذار.

بالنسبة لـ SIDS، يتم فحص سجلات الجهاز المضيف للعثور على تسلسلات من الأوامر أو الأفعال التي تم تعريفها مسبقاً على أنها برامج خبيثة. وقد أُطلق على أنظمة SIDS في المراجع أيضاً أسماء مثل " الكشف القائم على المعرفة " أو "كشف سوء الاستخدام".

يوضح الشكل 1 المفهوم العملي لأساليب SIDS. تتمثل الفكرة الرئيسية في بناء قاعدة بيانات لتوقيعات التطفل، ومقارنة الأنشطة الحالية بالتوقيعات الموجودة، وإطلاق إنذار في حال العثور على تطابق. على سبيل المثال، قد تؤدي قاعدة على شكل "إذا: شرط - إذن: نتيجة" إلى "إذا (عنوان IP المصدر = عنوان IP الوجهة) إذن صنف على أنه هجوم".

عادةً ما تقدم أنظمة SIDS دقة ممتازة في الكشف عن التطفلات المعروفة مسبقاً. ومع ذلك، تواجه صعوبة في اكتشاف الهجمات على الثغرات الغير المكتشفة (zero-day attacks) لأنه لا يوجد توقيع مطابق في قاعدة البيانات حتى يتم استخراج توقيع الهجوم الجديد وتخزينه. تُستخدم أنظمة SIDS في العديد من الأدوات الشائعة، مثل Snort و NetSTAT.

تدرس الأساليب التقليدية لـ SIDS حزم الشبكة وتحاول مطابقتها بقاعدة بيانات التوقيعات. لكن هذه التقنيات غير قادرة على تحديد الهجمات التي تمتد عبر عدة حزم. وبما أن البرامج الخبيثة الحديثة أصبحت أكثر تعقيداً، فقد يكون من الضروري استخلاص معلومات التوقيع عبر حزم متعددة. وهذا يتطلب من نظام IDS استدعاء محتويات الحزم السابقة. فيما يتعلق بإنشاء توقيع لـ SIDS، عادةً ما تكون هناك عدة طرق حيث يتم إنشاء التوقيعات كـ "آلات حالات" (state machines)، أو أنماط لغوية رسمية، أو شروط دلالية.

إن المعدل المتزايد لهجمات على الثغرات الغير المكتشفة قد جعل تقنيات SIDS أقل فعالية تدريجياً، لأنه لا يوجد توقيع مسبق لمثل هذه الهجمات. كما أن الأشكال المتعددة للبرامج الخبيثة وزيادة الهجمات الموجهة يمكن أن تزيد من تقويض كفاءة هذا النموذج التقليدي. ويمكن أن يكون الحل المحتمل لهذه المشكلة هو استخدام تقنيات AIDS (أنظمة كشف التطفل القائمة على الشذوذ)، التي تعمل من خلال تحديد السلوك المقبول بدلاً من تحديد السلوك الشاذ، كما سيتم وصفه في القسم التالي.

**نظام كشف التطفل القائم على الشذوذ (AIDS) :**

حظيت أنظمة كشف التطفل القائمة على الشذوذ (AIDS) باهتمام كبير من الباحثين، وذلك لقدرتها على تجاوز القيود التي تعاني منها أنظمة SIDS ، في أنظمة AIDS يتم إنشاء نموذج للسلوك "الطبيعي" لنظام الكمبيوتر باستخدام طرق تعتمد على التعلم الآلي أو الإحصاء أو المعرفة. يُعتبر أي انحراف كبير بين السلوك الملاحظ والنموذج بمثابة "شذوذ" (Anomaly)، والذي يمكن تفسيره على أنه تطفل. تعتمد هذه المجموعة من التقنيات على افتراض أن السلوك الخبيث يختلف عن سلوك المستخدم المعتاد. لذا، يتم تصنيف سلوكيات المستخدمين غير الطبيعية التي لا تتوافق مع السلوكيات القياسية على أنها عمليات تطفل.

يتكون تطوير أنظمة AIDS من مرحلتين:

\* مرحلة التدريب: يتم فيها استخدام ملف تعريف حركة المرور الطبيعية لتعلم نموذج السلوك الطبيعي.

\* مرحلة الاختبار: يتم فيها استخدام مجموعة بيانات جديدة لتحديد قدرة النظام على التعميم واكتشاف التطفلات التي لم يسبق له رؤيتها.

يمكن تصنيف أنظمة AIDS إلى عدة فئات بناءً على الطريقة المستخدمة في التدريب، مثل الأنظمة القائمة على الإحصاء، أو القائمة على المعرفة، أو القائمة على التعلم الآلي.

المزايا الرئيسية لـ AIDS

تكمن الميزة الأهم لـ AIDS في قدرتها على اكتشاف الهجمات على الثغرات الغير المكتشفة (Zero-day attacks)، لأن عملية التعرف على نشاط المستخدم غير الطبيعي لا تعتمد على قاعدة بيانات التوقيعات. تطلق أنظمة AIDS إشارة خطر عندما يختلف السلوك الذي يتم فحصه عن السلوك المعتاد.

علاوة على ذلك، تتمتع أنظمة AIDS بفوائد أخرى متعددة:

\* اكتشاف الأنشطة الخبيثة الداخلية: إذا بدأ متطفل في إجراء معاملات على حساب مسروق لا تتطابق مع نشاط المستخدم المعتاد، فإن النظام يطلق إنذاراً.

\* صعوبة التجاوز: من الصعب جداً على المخترقين تحديد ما هو السلوك "الطبيعي" للمستخدم دون إطلاق إنذار، لأن النظام مصمم بناءً على ملفات تعريف مخصصة. يمكن لأنظمة SIDS أن تحدد فقط التطفلات المعروفة جيداً، بينما يمكن لأنظمة AIDS أن تكشف عن الهجمات على الثغرات الغير المكتشفة بعد . ومع ذلك، يمكن أن تؤدي أنظمة AIDS إلى معدل عالٍ من الإنذارات الكاذبة (False Positive)، لأن بعض الشذوذ قد يكون مجرد أنشطة طبيعية جديدة بدلاً من تطفلات حقيقية.

نظرًا لغياب تصنيف شامل لأنظمة كشف التطفل القائمة على الشذوذ، فقد تم تصنيفها هنا إلى خمس فئات فرعية بناءً على ميزاتها: القائمة على الإحصاء، القائمة على الأنماط، القائمة على القواعد، القائمة على الحالة، والقائمة على الاستدلال.

**تقنيات لتطبيق أنظمة كشف التطفل القائمة على الشذوذ (AIDS) :**

يقدم هذا القسم نظرة عامة على مناهج أنظمة كشف التطفل القائمة على الشذوذ (AIDS) التي تم اقتراحها في السنوات الأخيرة، بهدف تحسين دقة الكشف وتقليل الإنذارات الكاذبة.

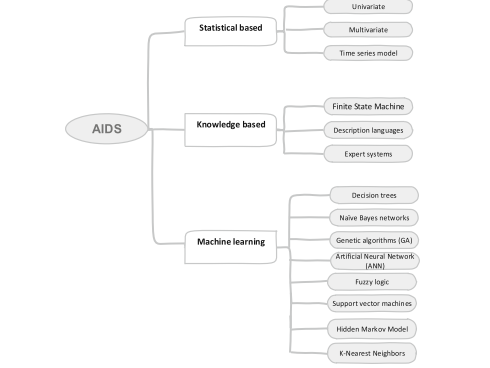
يمكن تصنيف أساليب AIDS إلى ثلاث مجموعات رئيسية:

\* الأساليب القائمة على الإحصاء (Statistics-based): تتضمن هذه الأساليب جمع وفحص كل سجل بيانات في مجموعة من العناصر، ثم بناء نموذج إحصائي لسلوك المستخدم الطبيعي.

\* الأساليب القائمة على المعرفة (Knowledge-based): تحاول هذه الأساليب تحديد الأنشطة المطلوبة من بيانات النظام الموجودة، مثل مواصفات البروتوكول وحالات حركة مرور الشبكة.

\* الأساليب القائمة على التعلم الآلي (Machine-learning based): تكتسب هذه الأساليب قدرات معقدة على مطابقة الأنماط من خلال بيانات التدريب.

يوضح الشكل 2 هذه الفئات الثلاث، بالإضافة إلى أمثلة على فئاتها الفرعية.



الشكل: تصنيف أساليب AIDS.

**التقنيات القائمة على المعرفة :**

تُعرف هذه المجموعة من التقنيات أيضًا بأسلوب "نظام الخبير". يتطلب هذا النهج إنشاء قاعدة معرفية تعكس ملف تعريف حركة المرور الشرعية. الأنشطة التي تختلف عن هذا الملف القياسي تُعامَل على أنها تطفل.

على عكس الفئات الأخرى من أنظمة AIDS، يتم إنشاء نموذج الملف القياسي عادةً بناءً على المعرفة البشرية، في شكل مجموعة من القواعد التي تحاول تعريف نشاط النظام الطبيعي.

الميزة الرئيسية للتقنيات القائمة على المعرفة هي القدرة على تقليل الإنذارات الكاذبة (false-positive alarms)، لأن النظام يمتلك معرفة بكل السلوكيات الطبيعية. ومع ذلك، في بيئة حوسبة تتغير ديناميكيًا، يحتاج هذا النوع من أنظمة IDS إلى تحديث منتظم للمعلومات المتعلقة بالسلوك الطبيعي المتوقع، وهي مهمة تستغرق وقتًا طويلاً، حيث إن جمع المعلومات حول جميع السلوكيات الطبيعية أمر صعب للغاية.

الآلة ذات الحالات المنتهية (Finite state machine - FSM):

FSM هو نموذج حوسبي يُستخدم لتمثيل تدفق التنفيذ والتحكم فيه. يمكن تطبيق هذا النموذج في كشف التطفل لإنتاج نموذج نظام كشف تطفل. عادةً ما يتم تمثيل النموذج في شكل حالات، وانتقالات، وأنشطة. تقوم الحالة بفحص البيانات التاريخية. على سبيل المثال، يتم ملاحظة أي تغييرات في المدخلات، وبناءً على التغيير المكتشف، يحدث الانتقال. يمكن لنموذج FSM أن يمثل سلوك النظام الشرعي، وأي انحراف ملحوظ عن هذا النموذج يعتبر هجومًا.

لغة الوصف (Description Language):

تعرّف لغة الوصف بناء القواعد التي يمكن استخدامها لتحديد خصائص هجوم معين. يمكن بناء القواعد بواسطة لغات وصف مثل N-grammars و UML.

النظام الخبير (Expert System):

يحتوي النظام الخبير على عدد من القواعد التي تحدد الهجمات. في النظام الخبير، عادة ما يتم تعريف القواعد يدوياً من قبل مهندس معرفة يعمل بالتعاون مع خبير في المجال.

تحليل التوقيع (Signature analysis):

هي أقدم تقنية مطبقة في أنظمة IDS. تعتمد على الفكرة البسيطة لمطابقة النصوص. في مطابقة النصوص، يتم فحص الحزمة الواردة، كلمة بكلمة، مع توقيع مميز. إذا تطابق التوقيع، يتم إطلاق إنذار. وإن لم يتطابق، يتم مطابقة المعلومات الموجودة في حركة المرور مع التوقيع التالي في قاعدة بيانات التوقيعات.

**التعلم الخاضع للإشراف في أنظمة كشف التطفل (IDS) :**

يعرض هذا القسم تقنيات التعلم الخاضع للإشراف المختلفة المستخدمة في أنظمة كشف التطفل. كل تقنية يتم تقديمها بالتفصيل مع إشارات إلى منشورات بحثية مهمة.

تقنيات أنظمة كشف التطفل القائمة على التعلم الخاضع للإشراف (Supervised learning) تكشف عن التطفلات باستخدام بيانات تدريب مصنفة. يتكون هذا النهج عادةً من مرحلتين: التدريب والاختبار. في مرحلة التدريب، يتم تحديد الميزات والفئات ذات الصلة ثم تتعلم الخوارزمية من عينات البيانات هذه. في أنظمة IDS القائمة على التعلم تحت الإشراف، كل سجل هو زوج، يحتوي على مصدر بيانات للشبكة أو الجهاز وله قيمة مخرجة مرتبطة به (أي تصنيف)، إما "تطفل" أو "طبيعي". بعد ذلك، يمكن تطبيق عملية اختيار الميزات لإزالة الميزات غير الضرورية. باستخدام بيانات التدريب للميزات المختارة، تُستخدم تقنية التعلم تحت الإشراف لتدريب مصنف لتعلم العلاقة الجوهرية الموجودة بين بيانات الإدخال وقيمة المخرج المصنفة. تم استكشاف مجموعة واسعة من تقنيات التعلم تحت الإشراف في الأدبيات البحثية، لكل منها مزاياها وعيوبها. في مرحلة الاختبار، يتم استخدام النموذج المدرب لتصنيف البيانات غير المعروفة إلى فئة "تطفل" أو "طبيعي". يصبح المصنف الناتج نموذجًا يتنبأ، عند إعطائه مجموعة من قيم الميزات، بالفئة التي قد تنتمي إليها بيانات الإدخال. يوضح الشكل 3 نهجًا عامًا لتطبيق تقنيات التصنيف.

هناك العديد من طرق التصنيف مثل أشجار القرار (Decision trees)، والأنظمة القائمة على القواعد (Rule-based systems)، والشبكات العصبية (Neural networks)، وآلات المتجهات الداعمة (Support Vector Machines)، وناييف بايز (Naïve Bayes)، وأقرب جار (Nearest-neighbor). تستخدم كل تقنية طريقة تعلم لبناء نموذج تصنيف. ومع ذلك، يجب أن يكون نهج التصنيف المناسب قادرًا ليس فقط على التعامل مع بيانات التدريب، بل يجب أن يحدد بدقة فئة السجلات التي لم يرها من قبل. يعد إنشاء نماذج تصنيف ذات قدرة تعميم موثوقة مهمة مهمة لخوارزمية التعلم.

أشجار القرار (Decision trees): تتكون شجرة القرار من ثلاثة مكونات أساسية. المكون الأول هو عقدة القرار (decision node)، والتي تستخدم لتحديد خاصية اختبار. والثاني هو الفرع (branch)، حيث يمثل كل فرع قرارًا ممكنًا بناءً على قيمة خاصية الاختبار. والثالث هو الورقة (leaf) التي تحتوي على الفئة التي ينتمي إليها العنصر. هناك العديد من خوارزميات أشجار القرار المختلفة بما في ذلك ID3 وC4.5 و CART.

ناييف بايز (Naïve Bayes): يعتمد هذا النهج على تطبيق مبدأ بايز مع افتراضات استقلالية قوية بين الخصائص. يجيب ناييف بايز على أسئلة مثل "ما هو احتمال حدوث نوع معين من الهجوم، بالنظر إلى أنشطة النظام الملحوظة ؟" من خلال تطبيق صيغ الاحتمال الشرطي. يعتمد ناييف بايز على الميزات التي لها احتمالات مختلفة للحدوث في الهجمات والسلوك الطبيعي. يُعد نموذج تصنيف ناييف بايز أحد أكثر النماذج شيوعًا في أنظمة كشف التطفل نظرًا لسهولة استخدامه وكفاءته الحسابية، وكلاهما مستمد من خاصية افتراض الاستقلالية الشرطية. ومع ذلك، لا يعمل النظام بشكل جيد إذا كان افتراض الاستقلالية هذا غير صالح، كما تم إظهاره على مجموعة بيانات KDD'99 لكشف التطفل التي تحتوي على تبعيات خصائص معقدة. تكشف النتائج أيضًا أن نموذج ناييف بايز لديه دقة منخفضة لمجموعات البيانات الكبيرة. أظهرت دراسة أخرى أنه يمكن تطبيق نموذج Hidden Naïve Bayes

(HNB) الأكثر تطورًا على مهام IDS التي تتضمن أبعادًا عالية، وخصائص مترابطة للغاية، وشبكات عالية السرعة.

الخوارزميات الجينية (Genetic algorithms - GA): الخوارزميات الجينية هي نهج استرشادي (heuristic) للتحسين، يعتمد على مبادئ التطور. يتم تمثيل كل حل ممكن كسلسلة من البتات (الجينات) أو كروموسوم، وتتحسن جودة الحلول بمرور الوقت من خلال تطبيق عوامل الاختيار والتكاثر، مع تفضيل الحلول الأكثر ملاءمة. عند تطبيق خوارزمية جينية على مشكلة تصنيف التطفل، يوجد عادةً نوعان من ترميز الكروموسوم: أحدهما يكون وفقًا للتجميع لتوليد طريقة ترميز كروموسوم ثنائي؛ والآخر هو تحديد مركز التجميع (مصفوفة نموذج التجميع) بواسطة كروموسوم ترميز عدد صحيح.

\* استخدم Murray et al. GA لتطوير قواعد بسيطة لحركة مرور الشبكة. يتم تمثيل كل قاعدة كجينوم، والعدد الأساسي للجينومات هو عدد من القواعد العشوائية. يتكون كل جينوم من جينات مختلفة تتوافق مع خصائص مثل IP المصدر، وIP الوجهة، ومنفذ المصدر، ومنفذ الوجهة، ونوع بروتوكول واحد.

الشبكة العصبية الاصطناعية (Artificial Neural Network - ANN): تعد ANN واحدة من أكثر طرق التعلم الآلي تطبيقًا على نطاق واسع وقد ثبت نجاحها في اكتشاف البرامج الضارة المختلفة.

تقنية التعلم الأكثر شيوعًا المستخدمة في التعلم تحت الإشراف هي خوارزمية الانتشار الخلفي (backpropagation - BP). تقييم خوارزمية BP تدرج خطأ الشبكة فيما يتعلق بأوزانها القابلة للتعديل. ومع ذلك، بالنسبة لأنظمة IDS القائمة على ANN، لا تزال دقة الكشف، خاصة للهجمات الأقل شيوعًا، ودقة الكشف بحاجة إلى تحسين. مجموعة بيانات التدريب للهجمات الأقل شيوعًا صغيرة مقارنة بتلك الخاصة بالهجمات الأكثر شيوعًا، وهذا يجعل من الصعب على ANN تعلم خصائص هذه الهجمات بشكل صحيح. نتيجة لذلك، تكون دقة الكشف أقل للهجمات الأقل شيوعًا. في مجال أمن المعلومات، يمكن أن يحدث ضرر كبير إذا لم يتم اكتشاف الهجمات منخفضة التردد. على سبيل المثال، إذا أفلتت هجمات(User to Root (U2R من الكشف، يمكن لمجرم إلكتروني الحصول على امتيازات ترخيص مستخدم الجذر وبالتالي تنفيذ أنشطة ضارة على أنظمة الكمبيوتر الخاصة بالضحية. بالإضافة إلى ذلك، غالبًا ما تكون الهجمات الأقل شيوعًا شاذة. غالبًا ما تعاني ANNs من الحدود الدنيا المحلية، وبالتالي يمكن أن يصبح التعلم مستهلكًا للوقت للغاية. تكمن قوة ANN في أنها، مع وجود طبقة مخفية أو أكثر، قادرة على إنتاج نماذج غير خطية بدرجة عالية تلتقط العلاقات المعقدة بين خصائص الإدخال وتصنيفات التصنيف. مع تطوير العديد من المتغيرات مثل الشبكات العصبية المتكررة و الالتفافية، تعد ANNs أدوات قوية في العديد من مهام التصنيف بما في ذلك IDS.

المنطق الضبابي (Fuzzy logic): تعتمد هذه التقنية على درجات عدم اليقين بدلاً من المنطق البولياني الثنائي الصحيح أو الخاطئ الذي تم بناء أجهزة الكمبيوتر المعاصرة عليه. لذلك، تقدم طريقة مباشرة للوصول إلى استنتاج نهائي بناءً على بيانات إدخال غير واضحة أو غامضة أو مشوشة أو غير دقيقة أو مفقودة. باستخدام مجال ضبابي، يسمح المنطق الضبابي للعنصر بالانتماء، جزئيًا ربما، إلى فئات متعددة في نفس الوقت. لذلك، يعد المنطق الضبابي مصنفًا جيدًا لمشاكل IDS لأن الأمن نفسه يتضمن غموضًا، والحدود الفاصلة بين الحالات الطبيعية وغير الطبيعية ليست محددة جيدًا. بالإضافة إلى ذلك، تحتوي مشكلة كشف التطفل على ميزات رقمية مختلفة في البيانات المجمعة والعديد من المقاييس الإحصائية المستمدة. يؤدي بناء أنظمة IDS بناءً على بيانات رقمية بحدود صارمة إلى إنذارات كاذبة عالية. لا يمكن التعرف على نشاط ينحرف قليلاً فقط عن النموذج أو قد يؤدي تغيير طفيف في النشاط الطبيعي إلى إنذارات كاذبة. باستخدام المنطق الضبابي، من الممكن نمذجة هذا الشذوذ البسيط للحفاظ على المعدلات الكاذبة منخفضة. أظهرت Elhag et al. أنه باستخدام المنطق الضبابي، يمكن تقليل معدل الإنذار الكاذب في تحديد الإجراءات التطفلية. وقد قاموا بتحديد مجموعة من القواعد الضبابية لوصف الأنشطة الطبيعية وغير الطبيعية في نظام الكمبيوتر، ومحرك استدلال ضبابي لتحديد التطفلات.

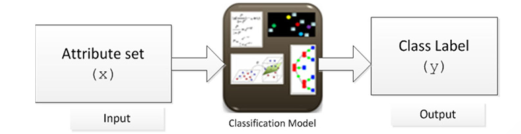
آلات المتجهات الداعمة Support Vector Machines - SVM): SVM)هو مصنف تمييزي يتم تعريفه بواسطة مستوى فاصل. تستخدم SVMs دالة نواة (kernel) لتعيين بيانات التدريب في فضاء ذي أبعاد أعلى بحيث يتم تصنيف التطفل بشكل خطي. تشتهر SVMs بقدرتها على التعميم وهي ذات قيمة أساسية عندما يكون عدد الخصائص كبيرًا وعدد نقاط البيانات صغيرًا. يمكن تحقيق أنواع مختلفة من المستويات الفاصلة عن طريق تطبيق دالة نواة، مثل (Linear، Polynomial، Gaussian Radial Basis Function (RBF، أو Hyperbolic tangent. في مجموعات بيانات IDS، العديد من الميزات زائدة عن الحاجة أو أقل تأثيرًا في فصل نقاط البيانات إلى فئات صحيحة. لذلك، يجب أخذ اختيار الميزات في الاعتبار أثناء تدريب SVM. يمكن أيضًا استخدام SVM للتصنيف في فئات متعددة. في العمل الذي قام به Li et al.، تم تطبيق مصنف SVM مع نواة RBF لتصنيف مجموعة بيانات KDD 1999 إلى فئات محددة مسبقًا. من إجمالي 41 خاصية، تم اختيار مجموعة فرعية من الميزات بعناية باستخدام طريقة اختيار الميزات.

نموذج ماركوف المخفي Hidden Markov Model - HMM): HMM)هو نموذج ماركوف إحصائي يُفترض فيه أن النظام الذي يتم نمذجته هو عملية ماركوف ذات بيانات غير مرئية. أظهرت الأبحاث السابقة أنه يمكن تطبيق تحليل HMM لتحديد أنواع معينة من البرامج الضارة. في هذه التقنية، يتم تدريب نموذج ماركوف المخفي مقابل ميزات البرامج الضارة المعروفة (مثل تسلسل رمز العملية) وبمجرد اكتمال مرحلة التدريب، يتم تطبيق النموذج المدرب لتسجيل حركة المرور الواردة. ثم يتم مقارنة النتيجة بحد محدد مسبقًا، وتشير النتيجة الأكبر من الحد إلى وجود برنامج ضار. وبالمثل، إذا كانت النتيجة أقل من الحد، يتم تحديد حركة المرور على أنها طبيعية.

مصنف أقرب جار (K-Nearest Neighbors - KNN): تقنية أقرب جار (k-NN) هي مصنف نموذجي غير معلمي يُطبق في التعلم الآلي.

فكرة هذه التقنيات هي تسمية عينة بيانات غير مصنفة إلى فئة أقرب k من جيرانها (حيث k هو عدد صحيح يحدد عدد الجيران المراد أخذهم في الاعتبار). يوضح الشكل 5 مصنف K-Nearest Neighbors حيث k = 5. تمثل النقطة X مثيلاً لتاريخ غير مصنف يحتاج إلى تصنيف. من بين أقرب خمسة جيران لـ X، هناك ثلاثة أنماط مماثلة من فئة "تطفل" واثنان من فئة "طبيعي". يتيح التصويت بالأغلبية تعيين X إلى فئة "تطفل".

يمكن تطبيق k-NN بشكل مناسب كمعيار لجميع المصنفات الأخرى لأنه يوفر أداء تصنيف جيدًا في معظم أنظمة IDS.



**التعلم غير الخاضع للإشراف في نظام كشف التطفل (IDS) :**

يُعدّ التعلم غير الخاضع للإشراف (Unsupervised learning) أحد فروع التعلم الآلي الذي يُستخدم لاستخلاص معلومات هامة من مجموعات بيانات الإدخال التي لا تحتوي على تصنيفات مسبقة. في هذا النهج، تُعامل نقاط بيانات الإدخال عادةً كمجموعة من المتغيرات العشوائية. بعد ذلك، يتم إنشاء نموذج كثافة مشترك لمجموعة البيانات بأكملها.

بينما يعتمد التعلم غير الخاضع للإشراف على تصنيفات محددة لتدريب النموذج، فإن التعلم غير تحت الإشراف يعمل بشكل مختلف؛ حيث لا تُعطى أي تصنيفات، بل يتم تجميع البيانات تلقائيًا في فئات مختلفة من خلال عملية التعلم. في سياق تطوير نظام كشف تطفل، يعني التعلم غير الخاضع للإشراف استخدم آلية لتحديد التطفلات بالاعتماد على بيانات غير مصنفة لتدريب النموذج.

بمجرد تجميع السجلات، يتم تصنيف جميع الحالات التي تظهر في المجموعات الصغيرة على أنها تطفل، وذلك لأن الحالات الطبيعية من المفترض أن تُنتج مجموعات كبيرة مقارنة بالشذوذ. بالإضافة إلى ذلك، بما أن التطفلات الخبيثة والحالات الطبيعية غير متشابهة، فإنها لا تقع في نفس المجموعة.

\* خوارزمية K-means (المتوسطات): تُعدّ تقنية K-means من أكثر تقنيات التحليل التجمعي شيوعاً، وتهدف إلى فصل 'n' من كائنات البيانات إلى 'k' من المجموعات، حيث يتم اختيار كل كائن بيانات في المجموعة الأقرب إلى متوسطها. إنها تقنية تجميع تعتمد على المسافة ولا تحتاج إلى حساب المسافات بين جميع توليفات السجلات. تستخدم مقياس المسافة الإقليدية كمقياس للتشابه. يتم تحديد عدد المجموعات مسبقًا من قبل المستخدم.

\* التجميع الهرمي (Hierarchical Clustering): هذه تقنية تجميع تهدف إلى إنشاء هيكل هرمي للمجموعات. تُصنف مناهج التجميع الهرمي عادةً إلى فئتين:

\* التجميع التراكمي (Agglomerative): وهو نهج "من الأسفل إلى الأعلى" حيث تحتوي المجموعات على مجموعات فرعية، والتي بدورها تحتوي على مجموعات فرعية، ويتم دمج أزواج من المجموعات معاً كلما صعدنا في الهيكل الهرمي.

\* التجميع الانقسامي (Divisive): وهو نهج "من الأعلى إلى الأسفل" حيث يتم تكرارًا اختيار المجموعة ذات القطر الأكبر في فضاء الميزات وتقسيمها إلى مجموعات فرعية ثنائية بمدى أقل.

لقد تم إنجاز الكثير من الأبحاث في مجال أنظمة التحكم السيبرانية-الفيزيائية (CPCS) فيما يتعلق بكشف الهجمات وتخفيفها باستخدام التعلم غير الخاضع للإشراف. على سبيل المثال، اقترح Alcaraz نهجًا يعتمد على التكرار لتحقيق المرونة. كما اقترح طبقة شبكة فرعية مخصصة لديها القدرة على التعامل مع السياق عن طريق جمع المعلومات بالإجماع من عقد السائقين التي يتم التحكم فيها في شبكة التحكم نفسها، والتمييز بين وجهات النظر المختلفة من خلال تقنيات استخراج البيانات مثل k-means وk-nearest neighbor. اقترح Chao Shen وآخرون تقنية "بصمة الجهاز الهجينة المعززة" (Hybrid-Augmented device fingerprinting) لأنظمة كشف التطفل في شبكات التحكم الصناعية. وقد استخدموا تقنيات تعلم آلي مختلفة لتحليل حزم الشبكة لتصفية حركة المرور الشاذة لاكتشاف التطفلات في شبكات أنظمة التحكم الصناعية.

**التعلم شبه الخاضع للإشراف في نظام كشف التطفل (IDS) :**

يقع التعلم شبه الخاضع للإشراف (Semi-supervised learning) في منطقة وسطى بين التعلم شبه الخاضع للإشراف (الذي يستخدم بيانات تدريب مصنفة بالكامل) والتعلم غير الخاضع للإشراف (الذي لا يستخدم أي بيانات تدريب مصنفة).

لقد أظهر الباحثون أن التعلم شبه الخاضع للإشراف يمكن استخدامه مع كمية قليلة من البيانات المصنفة لتعزيز أداء المصنفات في أنظمة كشف التطفل، مع تقليل الوقت والتكاليف المطلوبة. هذه الميزة ذات قيمة كبيرة، لأن البيانات المصنفة لمشاكل كشف التطفل غالبًا ما تكون نادرة أو يصعب الحصول عليها.

تم اقتراح عدد من التقنيات المختلفة للتعلم شبه الخاضع للإشراف، مثل خوارزميات "توقع الحد الأقصى" (Expectation Maximization)، و "التدريب الذاتي" (self-training)، و"التدريب المشترك" (co-training) ، بالإضافة إلى آلات المتجهات الداعمة شبه تحت الإشراف (Semi-Supervised SVM)، والأساليب القائمة على الرسوم البيانية، وأساليب التعلم شبه تحت الإشراف القائمة على التعزيز (boosting).

يقترح "رانا وآخرون" منهجًا جديدًا للتعلم شبه الخاضع للإشراف يعتمد على المنطق الضبابي (fuzzy-based)، وذلك بتطبيق عينات غير مصنفة مدعومة بخوارزمية تعلم الخاضع للإشراف لتعزيز أداء المصنف في أنظمة كشف التطفل. يتم تدريب شبكة عصبية أمامية بطبقة مخفية واحدة لإخراج متجه عضوية ضبابي، ويتم تصنيف العينات غير المصنفة إلى فئات (ضبابية منخفضة، متوسطة، وعالية) باستخدام الكمية الضبابية. يتم إعادة تدريب المصنف بعد دمج كل فئة بشكل منفصل في مجموعة التدريب الأصلية.

أظهرت نتائجهم التجريبية، باستخدام هذا النهج شبه الخاضع للإشراف لكشف التطفل على مجموعة بيانات NSL-KDD، أن العينات غير المصنفة التي تنتمي إلى مجموعات الضبابية المنخفضة والعالية تساهم بشكل كبير في تعزيز دقة أنظمة كشف التطفل مقارنة بالأساليب التقليدية.

**تقنيات قائمة على الهجين :**

تواجه أنظمة كشف التطفل التقليدية (IDS) مجموعة من القيود: يصعب تعديلها بسهولة، وتفشل في التعرف على الهجمات الخبيثة الجديدة، كما أنها تعاني من انخفاض الدقة وارتفاع معدل الإنذارات الكاذبة. وفي المقابل، فإن أنظمة AIDS وحدها لديها قيود مثل ارتفاع معدل الإنذارات الإيجابية الكاذبة.

للتغلب على هذه المشكلات، ظهرت أنظمة كشف التطفل الهجينة (Hybrid IDS) التي تعتمد على دمج تقنيات SIDS, AIDS. يجمع النظام الهجين بين نقاط القوة في كلا المنهجين، مما يمكنه من تجاوز نقاط الضعف الخاصة بكل منهما على حدة.

على سبيل المثال، اقترح "فريد وآخرون" نظام IDS هجينًا يجمع بين خوارزميات ناييف بايز وأشجار القرار، وقد حقق هذا النموذج معدل كشف بلغ 99.63% على مجموعة بيانات KDD'99.

**مقاييس الأداء لأنظمة كشف التطفل (IDS) :**

توجد العديد من مقاييس التصنيف لأنظمة كشف التطفل، وبعضها يُعرف بأسماء متعددة ، يتم عادةً تقييم أنظمة IDS بناءً على مقاييس الأداء القياسية التالية:

\* معدل الإيجابية الحقيقية (True Positive Rate - TPR): يُحسب كنسبة عدد الهجمات التي تم التنبؤ بها بشكل صحيح إلى العدد الإجمالي للهجمات. إذا تم اكتشاف جميع التطفلات، فإن TPR يساوي 1، وهو أمر نادر للغاية بالنسبة لأي نظام IDS. يُعرف TPR أيضًا باسم "معدل الكشف" (Detection Rate - DR) أو "الحساسية" (Sensitivity).

\* معدل الإيجابية الكاذبة (False Positive Rate - FPR): يُحسب كنسبة عدد الحالات الطبيعية التي تم تصنيفها بشكل خاطئ على أنها هجوم إلى العدد الإجمالي للحالات الطبيعية.

\* معدل السلبية الكاذبة (False Negative Rate - FNR): تعني السلبية الكاذبة أن الكاشف فشل في تحديد شذوذ ما، وصنفه على أنه طبيعي.

\* معدل التصنيف (Classification rate - CR) أو الدقة (Accuracy): يقيس CR مدى دقة نظام IDS في اكتشاف سلوك حركة المرور الطبيعية أو الشاذة. يُوصف بأنه النسبة المئوية لجميع الحالات التي تم التنبؤ بها بشكل صحيح إلى جميع الحالات.

\* منحنى خاصية تشغيل المُستقبِل (Receiver Operating Characteristic - ROC): يحتوي هذا المنحنى على محور x يمثل معدل الإيجابية الكاذبة (FPR) ومحور y يمثل معدل الإيجابية الحقيقية (TPR). في منحنى ROC، يتم رسم TPR كدالة لـ FPR لنقاط قطع مختلفة. تمثل كل نقطة على منحنى ROC زوجًا من FPR و TPR يتوافق مع عتبة قرار معينة. عندما تتغير العتبة الخاصة بالتصنيف، يتم اختيار نقطة مختلفة على منحنى ROC بمعدل إنذار كاذب (FAR) و TPR مختلفين. أي اختبار يتميز بتمييز مثالي (لا يوجد تداخل بين التوزيعين) يمتلك منحنى ROC يمر عبر الزاوية العلوية اليسرى (حساسية 100%، خصوصية 100%).

الفصل الثاني : تجهيز بيئة العمل :

لتجهيز بيئة العمل المناسبة للمشروع يجب علينا معرفة ماهي المحاكيات المتوفرة والمناسبة لتطبيقه بالشكل الأمثل والحصول على نتائج دقيقة تبين اهمية تحسين كشف التطفل ضمن المنازل الذكية لذلك نحتاج الى البحث عن محاكيات شبكات الانترنت واجهزة IoT تمت المقارنة بين عدة محاكيات مبينة في الجدول التالي :

الجدول1-2: مقارنة بين المحاكيات.

|  |  |  |  |
| --- | --- | --- | --- |
| المحاكي | NS-3 (Network Simulator 3) | OMNeT++ (Objective Modular Network Testbed in C++) | Cooja |
| الهدف الرئيسي | محاكاة دقيقة لبروتوكولات الإنترنت وأنظمة الشبكات على مستوى الحزم (packet-level). | بنية معيارية (modular) قابلة للتوسيع لمحاكاة أنظمة اتصالات متنوعة ومعقدة. | محاكي مخصص لشبكات الاستشعار اللاسلكية (WSNs) وContiki OS. |
| أداء المحاكاة | عالي: معروف بأدائه الممتاز وكفاءته العالية في محاكاة السيناريوهات الكبيرة. | جيد جدًا: يوفر أداءً ممتازًا، لكنه قد يكون أبطأ قليلاً من NS-3 في بعض الحالات. | جيد: مناسب لمحاكاة الأجهزة محدودة الموارد، ولكنه قد يواجه تحديات في قابلية التوسع (scalability) للشبكات الكبيرة. |
| نقاط القوة | دقة عالية: يوفر محاكاة واقعية جدًا للبروتوكولات.  مجتمع نشط: يمتلك مجتمعًا بحثيًا كبيرًا ومجموعة واسعة من النماذج (modules) المتطورة.  دعم لـ IoT: يحتوي على وحدات (modules) للعديد من بروتوكولات إنترنت الأشياء مثل LoRaWAN وZigbee. | بنية معيارية: يتيح بناء محاكاة معقدة من مكونات بسيطة وقابلة لإعادة الاستخدام.  واجهة رسومية قوية: تساعد في تصور المحاكاة وتتبع تدفق البيانات.  مرونة: يمكن استخدامه في مجالات أوسع من مجرد الشبكات. | محاكاة دقيقة للأجهزة: محاكاة سلوك الأجهزة الحقيقية (hardware-in-the-loop) بدقة عالية.  مدمج مع نظام تشغيل: يعمل بشكل متكامل مع نظام التشغيل Contiki OS |
| نقاط الضعف | منحنى تعلم حاد: يتطلب وقتًا وجهدًا كبيرًا لإتقانه.  غياب الواجهة الرسومية: لا يوفر واجهة رسومية مدمجة للتصميم | أقل انتشارًا من NS-3: على الرغم من قوته، إلا أن عدد النماذج المتوفرة قد يكون أقل مقارنة بـ NS-3. | متخصص جدًا: لا يناسب الأبحاث العامة في مجال الشبكات، ويقتصر استخدامه على بيئة Contiki |

وبناء على المقارنة السابقة تم اختيار المحاكي ns3 بسبب ان المشروع يركز على تحسين كشف الهجمات على مستوى البروتوكولات الشبكية و المحاكي مناسب لتحليل اداء البروتوكولات الخاصة بأنترنت الاشياء المعقدة .

كما انه تم استخدام المحاكي vmware لمحاكاة نظام كشفل التطفل snort للكشف عن الهجمات التقليدية ويعد snort الخيار المناسب لانه قائم على قواعد يتم كتابتها لاكتشاف انواع الهجمات المختلفة .

**الفصل الثالث:التجربة العملية**

**في هذا الفصل سوف نتكلم عن القسم العملي من المشروع ، سنقوم بمحاكاة شبكة لمنزل ذكي يحتوي على جهاز توجيه ، كاميرا ، حساس ، جهاز منزلي ، مهاجم على محاكي الشبكات NS3 سيتم تشغيله في بيئة العمل التي تكلمنا عنها في الفصل الثاني على نظام linux توزيعة Ubuntu**

**تم استخدام الNS3 والذي يوضح كيفية محاكاة الشبكة والاجهزة عليها ، سنقوم بتفصيل كل جزء من اجزاء الكود البرمجي المكتوب بلغة c++ .**

**اولاً : تم استدعاء مجموعة من مكتبات التي سوف نحتاجها لبناء الشبكة ؛ لأن كل مكتبة تضيف قدرات معينة للمحاكاة.  
المكتبات التي قمنا باستخدامها هي :**

**- core-module: للتحكم بالوقت**

**- network-module: لإنشاء العقد (Nodes) والأجهزة الشبكية (NetDevices).**

**- internet-module: لإضافة بروتوكولات الشبكات مثل IPv4, TCP, UDP.**

**- wifi-module + yans-wifi-helper: لتجهيز شبكة Wi-Fi مع نقطة وصول (AP) ومحطات (STAs).**

**- mobility-module: لتحديد نماذج الحركة للأجهزة (في حالتنا الأجهزة ثابتة).**

**- csma-module: لإضافة قناة سلكية (Ethernet/CSMA) بين جهاز التوجيه و نظام كشف التطفل snort.**

**- bridge-module: لربط عدة واجهات شبكية داخل عقدة واحدة (الجسر على جهاز التوجيه).**

**- tap-bridge-module: للربط بين الشبكة الافتراضية ومحاكي النظام الحقيقي عبر جهاز Tap.**

**- applications-module: لتشغيل تطبيقات توليد الترافيك (OnOff, PacketSink).**

**- flow-monitor-module: لجمع إحصائيات حول التدفقات (Packets sent, received, lost).**

**- ipv4-global-routing-helper: لإنشاء جداول التوجيه بشكل تلقائي.**

**الهدف من هذه المكتبات هي صندوق الأدوات الأساسي لبناء بيئة منزل ذكي قابلة للمحاكاة والتحليل.**

**A screenshot of a computer program

AI-generated content may be incorrect.**

**ثم قمنا بتعريف المكون الرئيسي والذي يعرف اسم مكون السجل (log component) في البرنامج حيث هي ميزة تتيح لك انشاء مكونات سجل NS\_LOG\_COMPONENT\_DEFINE داخل محاكاة الNS3 بحيث تسجل كل الأحداث او الأخطاء او التحذيرات في البرنامج .**

**اما الSmartHome\_TAP\_ns3.45 هو اسم مكون السجل .**

**A black background with red and white text

AI-generated content may be incorrect.**

**في هذا القسم قمنا بإنشاء العقد (Nodes) التي تمثل مكونات المنزل الذكي :**

**Router: جهاز التوجيه الأساسي الذي يربط الأجهزة المنزلية ببعضها وبالخارج.**

**TapHost: عقدة خاصة وظيفتها تمرير الترافيك بين الشبكة الافتراضية وجهاز Tap على النظام المضيف.**

**Camera (كاميرا مراقبة): جهاز منزلي ذكي يعمل عبر Wi-Fi.**

**Sensor (حساس IoT): يمثل جهاز استشعار (مثل درجة الحرارة أو الحركة).**

**Appliance (جهاز منزلي): يمثل جهازاً منزلياً متصلاً (ثلاجة ذكية أو لمبة).**

**Attacker (مهاجم): جهاز يحاول تنفيذ هجمات على الأجهزة المنزلية.**

**في النتيجة :**

**• أنشأنا 6 عقد: • راوتر (Access Point + Bridge).• TapHost (للربط مع النظام).**

**• 4 عقد: كاميرا – حساس – جهاز منزلي – مهاجم. • NodeContainer يسهل إنشاء عدة عقد دفعة واحدة.في المحاكاة، كلمة "Router" معناها عقدة ذكية جمعت وظيفتين:**

**Access Point: يوزّع Wi-Fi.**

**Bridge: يربط هالشبكة اللاسلكية بالشبكة السلكية (CSMA + Tap).**

**وبالتالي صار عندنا شبكة منزلية واقعية: أجهزة متصلة عبر Wi-Fi، ومتصلة بالنظام الحقيقي عبر Tap، وكل الترافيك يمر عبر "راوتر واحد مركزي".**

**A screen shot of a computer program

AI-generated content may be incorrect.**

**ثم قمنا بإنشاء قناة فيزيائية (YansWifiChannel) وهي البيئة اللاسلكية الفيزيائية التي تربط الاجهزة بالراوتر**

**وربطناها بطبقة فيزيائية (YansWifiPhy) المسؤلة عن تحويل البيانات الرقمية الى اشارات تماثلية ربطهم مع بعض يؤدي الى انشاء شبكة لاسلكية حقيقية بين الراوتر وبقية الاجهزة**

**بعد ذلك:**

**حددنا معيار Wi-Fi المستخدم (802.11g).**

**عرفنا SSID = "smart-home" ليكون اسم الشبكة المنزلية.**

**جعلنا الكاميرا، الحساس، الجهاز المنزلي، والمهاجم STAs (محطات Wi-Fi).**

**StaWifiMac: إعداد الأجهزة (الكاميرا، الحساس، الجهاز، المهاجم).**

**ApWifiMac:إعداد الراوتر كنقطة وصول.**

**NetDeviceContainer يخزن واجهات الشبكة لكل عقدة.**

**الهدف هو محاكاة شبكة Wi-Fi منزلية حقيقية حيث الأجهزة المنزلية والمهاجم يتصلون بنفس الراوتر.**

**A computer screen shot of white and orange text

AI-generated content may be incorrect.**

**ثم قمنا بتثبيت نموذج الحركة ConstantPositionMobilityModel على جميع الأجهزة , أي أن كل جهاز يبقى في مكانه طوال المحاكاة.**

**الهدف ان الأجهزة المنزلية عادةً ثابتة (الكاميرا على الجدار، الحساس في الغرفة، الجهاز المنزلي في مكانه).**

**A computer screen with text

AI-generated content may be incorrect.**

**أنشأنا رابط سلكي (Ethernet) بسرعة 100 ميغابت/ثانية بين الراوتر و TapHost.**

**هذا يربط الشبكة الافتراضية بالمضيف.**

**ومن ثم جمعنا واجهتي Wi-Fi وCSMA في الراوتر بجسر واحد هذا يسمح للراوتر بتمرير الترافيك بين الشبكتين بعد ذلك قمنا بإنشاء TapBridge وربطناه بجهاز TapHostهذا يسمح للترافيك بالمرور إلى جهاز Tap على النظام الحقيقي.**

**الهدف: تمكين المستخدم من رؤية الترافيك باستخدام Snort وكأنه ترافيك حقيقي على الحاسوب.**

**عمل الجسر: الراوتر هنا يستخدم الجسر ليتمكن من إعادة توجيه حركة المرور بين شبكة Wi-Fi و شبكة سلكية (Ethernet). بمعنى آخر، حركة البيانات بين الأجهزة اللاسلكية (على Wi-Fi) يمكنها الآن الانتقال إلى الأجهزة على الشبكة السلكية (مثل TapHost) والعكس.**

**CSMA (Carrier Sense Multiple Access)**

**المفهوم: هو بروتوكول للتحكم في الوصول إلى الوسيط في الشبكات السلكية، خصوصًا في شبكات إيثرنت.**

**الأجهزة في هذه الشبكة "تستمع" أولاً إلى القناة لمعرفة إذا كانت مشغولة أم لا، وإذا كانت القناة خالية، يمكنها إرسال البيانات.**

**العلاقة بين الجسر و CSMA:**

**الجسر يربط بين شبكة Wi-Fi و شبكة CSMA.**

**CSMA هو البروتوكول الذي يحدد كيفية التواصل بين الأجهزة عبر الشبكة السلكية.**

****

**تثبيت بروتوكولات TCP/IP على الراوتر والأجهزة الذكية.**

**• لم نثبتها على TapHost لأنه يعمل فقط في الطبقة الثانية لقد ثبتنا بروتوكولات الإنترنت (TCP/IP) على الراوتر والأجهزة الذكية، لكن لم نثبتها على tapHost السبب الرئيسي لانه لا يعمل كجهاز عادي في شبكة المحاكاة بل هو مجرد نقطة ربط بين محاكاة NS-3 و الجزء الذي سيربطه بsnort (أو النظام المضيف).**

**هو يعمل في الطبقة الثانية فقط (Layer 2)، مثل كأنه كابل فيزيائي، ولا يحتاج إلى IP أو بروتوكولات TCP/UDP داخل NS-3.**

**بروتوكولات الإنترنت (IP/TCP/UDP) تُثبت فقط على الأجهزة التي تشارك في نقل البيانات داخل المحاكاة تحتاج إلى إرسال/استقبال عبر الشبكة المنطقية تحتاج إلى توجيه (routing) أو مشاركة في تطبيقات NS-3 بينما tapHost هو فقط «ممر» للبيانات بين NS-3 وواجهة tap في النظام (مثل tap-smart).**

**لا يتعامل مع IP داخلياً كل ما يصله هو «إطارات Ethernet» تُمرر مباشرة عبر الجسر الموجود في الراوتر.**

**مبدأ عمل TapBridge:**

**بيأخذ الإطارات (frames) من NS-3 ويمررها إلى واجهة tap في النظام (tap-smart).**

**والعكس، أي ترافیک من tap-smart في النظام يمرّ إلى tapHost، ومنها إلى الراوتر.**

**لذلك tapHost لا يحتاج إلى IP ولا إلى . InternetStackHelper**

**A computer screen shot of white text

AI-generated content may be incorrect.**

**تخصيص عناوين IP خصصنا شبكة فرعية: 10.1.1.0/24, الراوتر: 10.1.1.1 ,الكاميرا: 10.1.1.2 الحساس: 10.1.1.3 ,الجهاز المنزلي :10.1.1.4 ,المهاجم: 10.1.1.5, الهدف: تحديد عناوين ثابتة تسهّل استهداف كل جهاز على حدة.**

**لقد قمنا ايضا باختصار لاسماء الاجهوة بحيث تمت تسمية :**

**R=ipRouter CAM= ipCamera ,SNSR= ipSensor , APP= ipAppliance ,**

**ATT= ipAttacker**

**A screenshot of a computer screen

AI-generated content may be incorrect.**

**في هذا القسم، نُحدّد أرقام المنافذ Port Numbers التي سيتم استخدامها في المحاكاة لتمثيل البروتوكولات والتطبيقات الحقيقية التي تعمل على كل نوع من الأجهزة الذكية في المنزل.**

**كل جهاز في الشبكة (كاميرا، حساس، جهاز منزلي) يتمتع بتطبيق معين يعمل على بروتوكول وشبكة مختلفة، ويحتاج إلى منفذ محدد للتواصل. رقم المنفذ يُستخدم من قبل التطبيقات للتمييز بين الخدمات المختلفة التي تعمل على نفس الجهاز.**

**1. الكاميرا — RTP عبر UDP:**

**الكاميرا عادةً تُرسل الفيديو عبر بروتوكول يسمى RTP (Real-time Transport Protocol).**

**RTP يعمل فوق UDP لأن الفيديو يحتاج لتأخير منخفض أكثر من الموثوقية الكاملة.**

**في هذا الكود، خصصنا المنفذ 5004 لتلقي بيانات الفيديو على الكاميرا.هذا رقم قياسي شائع جداً لـ RTP، ومُستخدم في الأنظمة الحقيقية**

**2. الحساس — CoAP عبر UDP:**

**CoAP (Constrained Application Protocol) هو بروتوكول خفيف مخصص لأجهزة إنترنت الأشياء مثل الحساسات.**

**يشبه HTTP لكنه يعمل فوق UDP ليكون أخف وأسرع.**

**المنفذ 5683 هو المنفذ الرسمي والمُعتمد عالميًا لبروتوكول CoAP.**

**3.الجهاز المنزلي — MQTT عبر TCP:**

**MQTT (Message Queuing Telemetry Transport) هو بروتوكول اتصال خفيف يعمل فوق TCp يستخدم في المنازل الذكية للتحكم بالأجهزة (مثل الثيرموستات، الإضاءة، إلخ).**

**المنفذ 1883 هو المنفذ الرسمي لبروتوكول MQTT بدون تشفير (MQTTS يكون على 8883).**

**5004 → شائع لبث الفيديو RTP.**

**5683 → مستخدم رسميًا من IETF لـ CoAP.**

**1883 → المنفذ العالمي لـ MQTT.**

**باستخدام هذه الأرقام، نستطيع محاكاة سلوك الأجهزة الذكية الحقيقي، وتحليل تأثير الهجمات عليها كما لو كنا نختبر شبكة منزلية فعلية.**

**A black background with white text

AI-generated content may be incorrect.**

**الفكرة الرئيسية هنا هي تحديد وتثبيت التطبيقات التي تستقبل الترافيك على الأجهزة المختلفة. هذا يشمل تحديد البروتوكولات والمنافذ التي سيتم الاستماع عليها (بمعنى استقبال البيانات عليها).**

**PacketSink هو تطبيق يتم تثبيته على الأجهزة ليقوم باستقبال هذه البيانات من الشبكة. كل جهاز في هذه الشبكة قد يكون لديه حركة مرور طبيعية من أجهزة أخرى (مثل جهاز استشعار يرسل بياناته بشكل مستمر إلى الخادم)، لكن المهاجم يمكنه أيضاً إرسال هجمات مثل UDP flood أو CoAP probing. وفي هذه الحالة، PacketSink يستقبل كل هذه الأنواع من الترافيك (سواء كان بيانات طبيعية أو هجومية).**

**1.الكاميرا تبث فيديو عبر RTP الترافيك الذي يتم استقباله: بيانات فيديو عبر بروتوكول RTP عبر UDP (المنفذ 5004).**

**الهدف: استلام البيانات التي تبثها الكاميرا في الشبكة. في العالم الحقيقي، الكاميرا قد تبث فيديو عبر الإنترنت باستخدام RTP.**

**البيانات العادية أو الهجمات: هذا التطبيق يستقبل بيانات الفيديو العادية التي يتم إرسالها من كاميرا أخرى أو من جهاز في الشبكة. لكن أيضاً إذا كان المهاجم يرسل بيانات عبر هذا المنفذ، مثل هجوم UDP flood، فسيتم استلامه أيضاً.**

**2. حساس (يستخدم بروتوكول CoAP عبر UDP)**

**الترافيك الذي يتم استقباله: بيانات حساس عبر بروتوكول CoAP عبر UDP (المنفذ 5683).**

**الهدف: استلام البيانات التي يرسلها الحساس مثل قراءات الحرارة أو الرطوبة.**

**البيانات العادية أو الهجمات: الحساس يستقبل عادة البيانات العادية من المستشعرات. ولكن إذا كان المهاجم يرسل CoAP probing (هجوم عبر إرسال الكثير من الحزم الصغيرة والسريعة إلى الحساس)، فسيتم استلام هذه الحزم أيضاً.**

**3. جهاز منزلي (يستخدم MQTT عبر TCP)**

**الترافيك الذي يتم استقباله: بيانات MQTT عبر TCP (المنفذ 1883).**

**الهدف: جهاز منزلي مثل جهاز تحكم ذكي في المنزل قد يستقبل رسائل عبر بروتوكول MQTT من جهاز آخر أو من الخادم المركزي.**

**البيانات العادية أو الهجمات: هذا التطبيق يستقبل البيانات العادية مثل رسائل MQTT، ولكن في حال وجود هجوم MQTT burst (هجوم عبر إرسال كمية ضخمة من البيانات بسرعة عالية)، ستتم استجابة الجهاز لهذه الرسائل كذلك.**

**PacketSink هو تطبيق لاستقبال الترافيك سواء كان طبيعيًا (مثل فيديو الكاميرا أو بيانات الحساسات) أو هجوميًا (مثل هجوم UDP flood أو CoAP probing).**

**يُستخدم PacketSink على كل جهاز من الأجهزة لتحديد المنفذ الذي يستقبل البيانات عليه، وبالتالي يقوم التطبيق باستقبال كل الترافيك الذي يُرسل إليه سواء كان عاديًا أو هجوميًا.**A computer screen shot of a program

AI-generated content may be incorrect.

**الان بعد ان تم تصميم كامل الشبكة وبناءها سنقوم الان بالانتقال لقسم الهجمات التي سوف تطبق على هذه الشبكة وهنا سوف نتحدث بالتفصيل عن ماهية الهجمات ومبدأ عملها وكيف سوف تتم :**

**1. هجوم UDP Flood على الكاميرا**

**في هذا الهجوم، يقوم المهاجم بإرسال تدفق كبير من حزم UDP (بسرعة 30Mbps) إلى الكاميرا ، معدل ارسال البيانات بينmbps 20 و40 mbps، وحجم الحزمة بين 400 و700 بايت، المهاجم يبدأ الهجوم من اللحظة 12 إلى اللحظة 18 من المحاكاة.**

**الهدف هو إغراق الكاميرا بحزم UDP كثيرة وبسرعة عالية حتى تصبح غير قادرة على معالجة الحزم القادمة، وبالتالي تعطيل بث الفيديو.**

**UDP هو بروتوكول لا يتطلب التأكد من وصول الحزم أو ترتيبها. هذا يجعله غير موثوق ولكنه أسرع مقارنة بـ TCP. لذلك، عندما يرسل المهاجم تدفقًا كبيرًا من حزم UDP، يتم تجاهل أي نوع من التأكيد أو الترتيب.**

**هذا يجعل من السهل على المهاجم إغراق جهاز المستلم (الكاميرا في هذه الحالة) دون الحاجة للانتظار أو إعادة إرسال الحزم.**

**الكاميرا تعتمد على UDP لبث الفيديو، الذي يحتاج إلى سرعة نقل عالية وتدفق مستمر للبيانات.**

**عندما يُغرق المهاجم الكاميرا بحزم UDP، تصبح الكاميرا غير قادرة على استقبال الحزم الصحيحة بسبب تكدس البيانات، مما يؤدي إلى توقف البث أو تأخيراته الكبيرة.**

**A computer screen with white and yellow text

AI-generated content may be incorrect.**

**2. هجوم CoAP Probing على الحساس**

**يبدأ الهجوم من اللحظة 32 إلى اللحظة 42 في المحاكاة ،و يبقى الهجوم لمدة بين 8 و 18 ثانية ، ويكون معدل حجم البيانات بين 1 و 5 . mbpsالهدف هو إرهاق الحساس من خلال إرسال عدد كبير جدًا من الحزم في فترة قصيرة، يتم إرسال هذه الحزم في شكل استعلامات أو طلبات CoAP.**

**البروتوكولات المستخدمة:**

**CoAP هو بروتوكول موجه للأجهزة ذات الموارد المحدودة مثل الحساسات. يستخدم UDP كوسيلة نقل له لأنه أسرع ويشغل أقل عرض نطاق ترددي مقارنة بـ TCP.**

**يعتمد البروتوكول على طلب-استجابة ويستخدم بشكل رئيسي في الأنظمة المدمجة (مثل الحساسات).**

**يرسل المهاجم طلبات CoAP كثيرة وبسرعة عالية لإغراق الحساس وإنهاكه، مما يؤدي إلى توقف الحساس عن الاستجابة أو زيادة استهلاك الموارد، الحساس عادة ما يستجيب لطلبات CoAP ولكنه يعالج عددًا محدودًا فقط من هذه الطلبات في وقت واحد.**

**عندما يتم إرسال العديد من الحزم في وقت قصير، فإن الحساس يصبح مشغولًا جدًا للتعامل مع كل هذه الطلبات، وبالتالي يؤدي إلى تأخير استجابة أو توقف النظام عن الاستجابة.**

**A computer screen shot of a program code

AI-generated content may be incorrect.**

**3. هجوم MQTT Burst على الجهاز المنزلي**

**في هذا الهجوم، يقوم المهاجم بإرسال تدفق من حزم TCP بسرعة بين 8 الى 22 Mbps إلى الجهاز المنزلي، بحجوم مختلفة وهي 200، 400، 600، 1000 بايت لكل حزمة ،يبدأ الهجوم من اللحظة 52 إلى اللحظة 62 من المحاكاة ،الهدف هنا هو إغراق الجهاز برسائل MQTT التي يتم إرسالها عبر TCP.**

**MQTT هو بروتوكول خفيف الوزن يستخدم في تطبيقات الإنترنت للأشياء (IoT). يعتمد على TCP لضمان توصيل الرسائل بشكل موثوق.**

**يستخدم MQTT بشكل رئيسي في تطبيقات المنزل الذكي مثل أجهزة الإضاءة، التدفئة، أو حتى الأجهزة مثل الترموستات الذكي ،يتم إرسال رسائل قصيرة الحجم (مثل أوامر تشغيل/إيقاف) بين الأجهزة عبر هذا البروتوكول.**

**الجهاز المنزلي يعتمد على MQTT للحصول على أوامر رسائل ، عند تلقي العديد من الرسائل بسرعة كبيرة، يصبح الجهاز محملاً بالبيانات ويصعب عليه معالجة هذه الرسائل ،هذا يؤدي إلى توقف أو تأخير في استجابة الجهاز، مما يسبب تشويشًا في التحكم بأجهزة المنزل الذكي.**

**الخلاصة:**

**هجوم UDP Flood يركز على إغراق الكاميرا من خلال إرسال بيانات ضخمة عبر UDP.**

**هجوم CoAP Probing يهدف إلى إرهاق الحساس عبر إرسال طلبات CoAP كثيرة وصغيرة الحجم.**

**هجوم MQTT Burst يستهدف إغراق الجهاز المنزلي برسائل MQTT لزيادة الحمولة على الجهاز.**

**A computer screen shot of a program code

AI-generated content may be incorrect.**

**بعد الانتهاء من بناء الشبكة بالكامل مع وضع الهجمات داخل ملف التنفيذ الرئيسي للمحاكي Ns3 قمنا بتجهيز وتهيئة نظام كشف التطفل snort لأكتشاف الهجمات المطبقة على الشبكة من خلال ربطه ب tap-smart التي تمر من خلالها حركة المرور الحاصلة على الشبكة و بعدها قمنا بكتابة القواعد المناسبة في ملف يسمى Local.rules داخل ملف النظام الخاص ب SNORT**

**القاعدة الاولى :**

****

**هذه القاعدة تعطي تنبيه عند وصول حزم UDP من اي ip الى الكاميرا على منفذ 5004 وتعطي رسالة تنبيه انها هجمة وتم اعطائها رقم تعريفي ورقم اصدار اول .**

**القاعدة الثانية :**

****

**هذه القاعدة تعطي تنبيه عند وصول حزمCOAP التي يتم نقلها عبر بروتوكول UDP الى جهاز المستشعر على المنفذ 5683 وتعطي رسالة تنبيه انها هجمة وتم اعطائها رقم تعريفي ورقم اصدار اول .**

**القاعدة الثالثة :**

****

**هذه القاعدة تعطي تنبيه عند وصول عدد هائل من طلبات الاتصال المتزامنة في فترة قصيرة مع الجهاز المنزلي التي يتم نقلها عبر بروتوكول TCP الى الجهاز المنزلي الذكي (ثلاجة / لمبة ) على المنفذ 1883 وتعطي رسالة تنبيه انها هجمة وتم اعطائها رقم تعريفي ورقم اصدار اول .**

**وبعد الانتهاء من كتابة القواعد ، قمنا بتشغيل snort ليراقب حركة المرور في الشبكة مستندا على هذه القواعد في اكتشاف الهجمات تم فتح عدة نوافذ على منفذ الاوامر في Ubuntu على الترتيب التالي في النافذة الاولى قمنا ببدأ المحاكاة للشبكة وتشغيلها ، وفي النافذة الثانية قمنا بتشغيل snort ، وفي النافذة الثالثة قمنا بتشغيل المراقبة على حركة المرور الحاصلة في tap-host ، وفي النافذة الرابعة تظهر لنا التنبيهات على الهجمات التي تم اكتشافها من قبلsnort**

**وهذه هي النوافذ التي يتم مراقبتها :**

A screenshot of a computer program

AI-generated content may be incorrect.

**A computer screen with white text

AI-generated content may be incorrect.**

**A computer screen with white text

AI-generated content may be incorrect.**

****

**تمت رؤية حركة المرور على النافذة الثانية :**

A screenshot of a computer program

AI-generated content may be incorrect.

**وقد اظهر snort تنبيهات لهجمتين من الثلاث هجمات السابقة :**

**التنبيه الاول يظهر هجمة من النوع UDP FLOOD من ال IP :10.1.1.5 الى الكاميرا** 10.1.1.2 **من المنفذ** 49153 **الى المنفذ** 5004

**التنبيه الثاني يظهر هجمة من النوع CoAP Probing من ال IP :10.1.1.5 الى الحساس** 10.1.1.3**من المنفذ** 49154 **الى المنفذ** 5683

**A computer screen shot of white text

AI-generated content may be incorrect.**

**و قد اظهرت النافذة الاولى عدد التدفقات التي حصلت داخل هذه الشبكة وهي التي تعتبر الهجمات :**

A screenshot of a computer

AI-generated content may be incorrect.

**وهذا يظهر لنا ان نظام كشف التطفل فقط استطاع اكتشاف هجمتين ولم يستطيع ان يكتشف الهجوم الثالث على الجهاز االمنزلي الذكي .**

**لذلك هنا تظهر الحاجة الى تحسين امكانية كشف التطفل ضمن المنازل الذكية التي خضعت الى عدة مراحل :**

**المرحلة الاولى : تم تشغيل المحاكاة من جديد مع اضافة هجمة جديدة Port-Hopping وتعد هذه الهجمة نوع من**

**التخفي في الشبكة حيث بدل من ان يبقى المهاجم ينفذ هجمته على منفذ واحد ثابت يقوم بتغير المنافذ بسرعة بشكل عشوائي او دوري ،و ان انظمة كشف التطفل التقليدية مثل snort تراقب منافذ محددة**

**في الهجوم الذي تم تصميمه في الكود كان المهاجم بقوم بإرسال حركة مرور كبيرة من نوع (UDP/TCP) على منافذ متغيرة باتجاه الكاميرا وتم ارسال اكثر من تدفق على منافذ مختلفة وهي (4000 ,4010 , 7777, 9001 ,10000, 15000 ) .**

**A computer screen shot of a program code

AI-generated content may be incorrect.**

**تم تسجيل حركة المرور الحاصلة داخل الشبكة باستخدام تابع flowmonitor حيث يقوم بتخزينها في ملفات بصيغة xml حيث تتضمن رقم تعريف لكل تدفق و البروتوكول و منفذ المصدر ومنفذ الوجهة و ip المصدر و ip الوجهة وعدد الحزم المرسلة و المستقبلة والضائعة .**

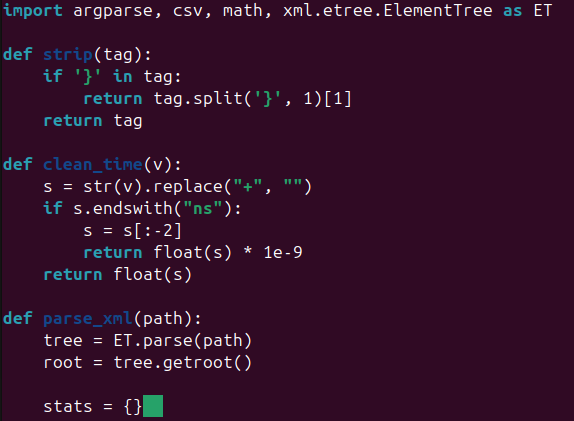
**A computer screen shot of a program code

AI-generated content may be incorrect.**

A computer screen shot of white text

AI-generated content may be incorrect.

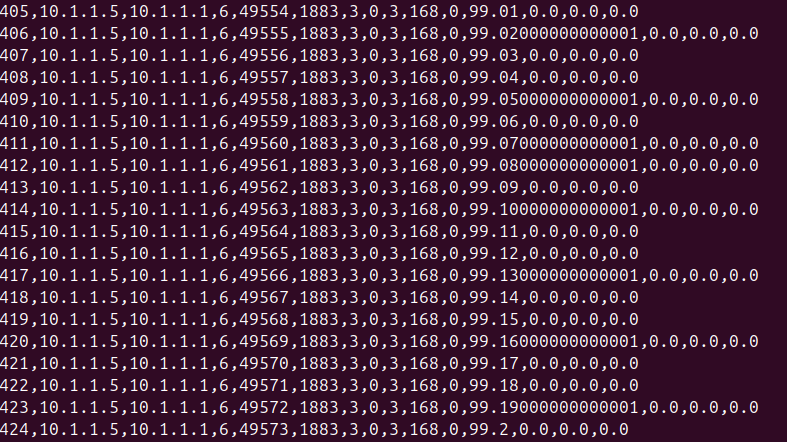
**المرحلة الثانية : قمنا بتحويل ملفات xml الى ملفات بصيغة csv للتوافق مع ادوات التعلم الالي ولسهولة قرأتها ومعالجتها باستخدام سيكربت مكتوب بلغة بايثون**

****

**A computer screen shot of a program code

AI-generated content may be incorrect.**

**وهذا هو الملف بعد تحويله الى csv :**

****

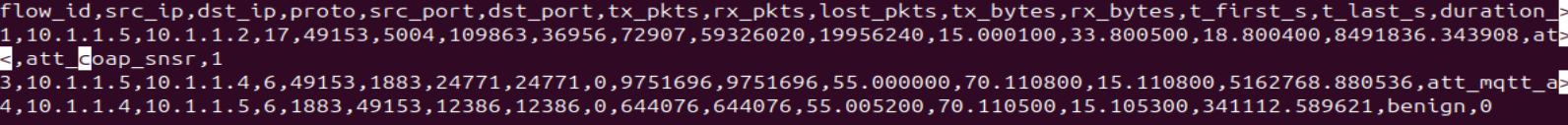
**المرحلة الثالثة : في هذه المرحلة كانت الخطوة الاهم في تجهيز البيانات في ملف csv واحد لكي نضيف اليها التوسيم المناسب الذي يعرف ب (Labeling) وهي طريقة تستخدم لتمييز حركة المرور السليمة من حركة المرور التي تعتبر هجوم ، وتتم من خلال سيكربت يكتب بلغة بايثون حيث نقوم بإعطائه الملف الموحد لحركة المرور ويقوم بوضع كلمة bengin ورقم 0 اي ان حركة المرور سليمة ويضع اسم الهجوم ورقم 1 ليدل على ان حركة المرور مريبة وتمثل هجوم.**

**وهنا يظهر الكود الخاص بالتوسيم :**

**A computer screen with text and images

AI-generated content may be incorrect.**

**وهذا جزء من نتيجة الملف بعد توسيمه :**

****

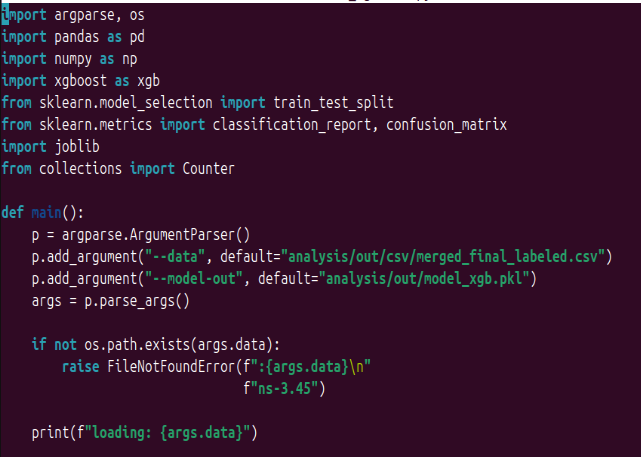
**الان اصبح لدينا ملف جاهز للتدريب يمكن قرائته ومعالجته من قبل خوارزمية التدريب التي قمنا باختيارها وهي خوارزمية XGBoost وتقوم هذه الخوارزمية على بناء اشجار متسلسلة تقوم بمعالجة الاخطاء الساببقة ضمن التدريب بدل من ان تبني شجرة واحدة او عدة اشجار مستقلة ، وهذا يساعد في ان يكون ادائها افضل من خوارزميات اخرى**

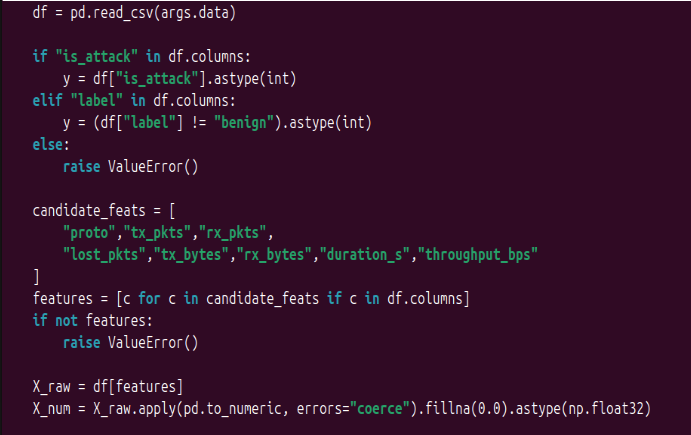
**حيث انها قوية جدا في التعامل مع البيانات الغير متوازنة وتعتمد في تدريبها على الدقة العالية حيث انها يمكنها تصنيف حركة المرور المعقدة وتتعامل مع بيانات كبيرة ، وتأخذ ارقام ومعلومات كثيرة للتدريب مثل :( tx\_pkts،rx\_pkts, throughput )**

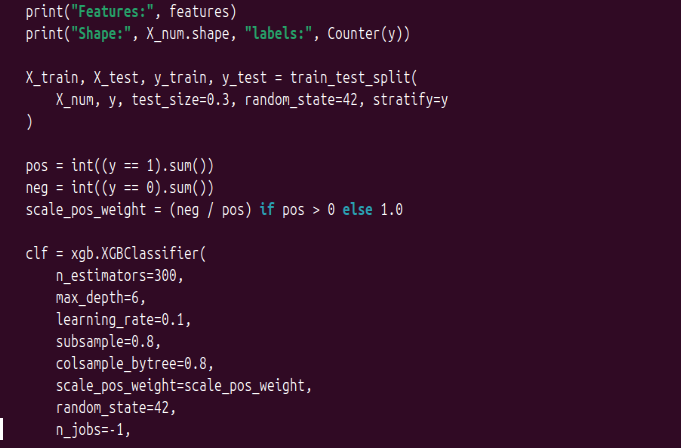
**ولكن لديها بعض العيوب حيث انها تستغرق وقت اطول مقارنة بخوارزميات اخرى مثل Random Forest وتحتاج ايضا الى ضبط المعلمات في الكود البرمجي المكتوب من عمق الشجرة ومعدل التعلم هنا يجب ان يكون اختيار هذه المعلمات دقيق لكي لا تعطي معلومات ونتائج غير متوازنة او غير دقيقة ، كما انها تستهلك الموارد من سعة ذاكرة وصول عشوائي ومعالجة بيانات و من خلال استهلاك وحدة المعالجة المركزية**

**في الخلاصة :تم اختيار XGBoost بسبب الدقة العالية والتعامل مع البيانات الغير متوازنة .**

**هنا يظهر الكود البرمجي الذي استخدمنا فيه هذه الخوارزمية لتدريب الملف الذي قمنا بتوسيمه :**

****

****

****

****

**هذه الخوارزمية تستخدم المكتبات التالية :**

**يستورد مكتبة pandas/numpy لقراءة البيانات .**

**مكتبة xgboost لعمله كنموذج .**

**مكتبة sklearn لاستدعاء الادوات الخاصة بالتقسيم والتقييم لملف csv .**

**مكتبة joblib لحفظ النموذج بعد الانتهاء من تدريبه .**

**مكتبة arg parse لقراءة وسائط سطر الاوامر عند تمرير الملف له .**

**اولا : نقوم بإعطائه مسار الملف وبعدها اين يقوم بحفظ النموذج حيث انه يتأكد من وجود النموذج قبل المتابعة ،**

**يقوم بتحميل البيانات الى datafram ثم بعدها يقوم بتحديد الهدف للتمييز بين الهجوم والحالة السليمة ،** **يضمن أن كل المميزات** رقمية **يحوّل أي قيم غير رقمية إلى NaN ثم يملؤها 0، ويحول لـ float32 أسرع وأخف للـ XGB ثم بعدها يقوم بأهم خطوة وهي تقسيم البيانات (30% اختبار) مع stratify للحفاظ على نفس نسبة الهجمات/السليم بين Train/Test..**

** n\_estimators: عدد الأشجار.**

**max\_depth : عمق الشجرة (التحكم بالتعقيد).**

** learning\_rate: معدل التعلّم (صغير = تعلّم أهدأ).**

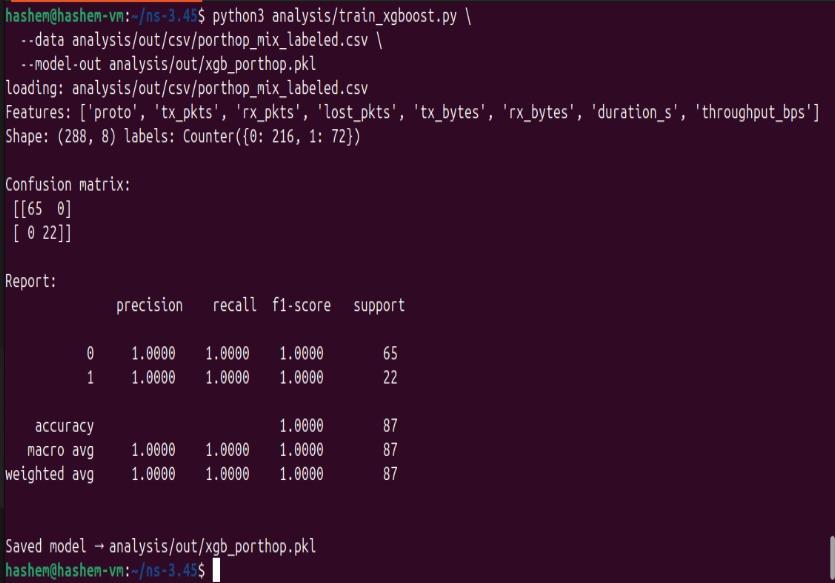
** subsample / colsample\_bytree : عيّنة جزئية للبيانات والميزات (تمنع overfitting).**

** scale\_pos\_weight : مهم مع البيانات غير المتوازنة.**

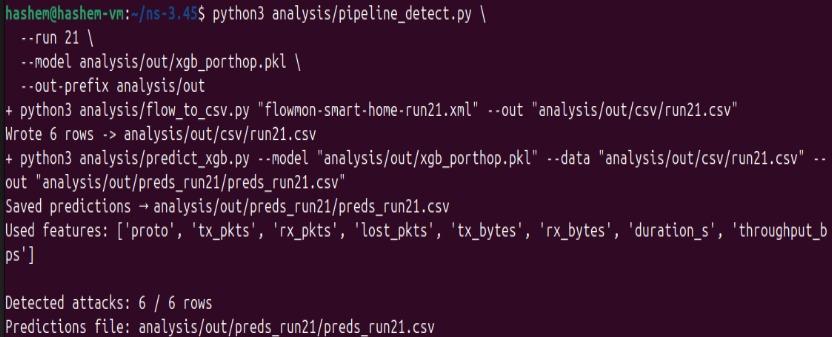
** tree\_method=hist : سريع على الجداول.**

**n\_jobs=-1: استخدم كل الأنوية المتاحة.**

**ثانيا : ثم بعدها قمنا بتدريب النموذج ليصبح جاهز للتقييم :**



**نلاحظ هنا اظهر النموذج نجاح في التدريب حيث انه قام باكتشاف 22 هجمة في الملف و وتصنيفها على انها تهديد للشبكة ، ومن جهة اخرى اظهر ان هناك 65 حالة سليمة على الشبكة ، وبعد الانتهاء ظهر ملف يحمل اللاحقة .pk وهو النموذج الجاهز للاختبار .**



**تم تشغيل النموذج على ملف csv جاهز يحتوي على حركة مرور جديدة للشبكة حيث قام بالكشف عن 6 هجمات مكررة على الشبكة وهو ما لم يستطيع القيام به نظام كشف التطفsnort وبذلك قمنا بما هو مطلوب من تحسين في نظام كشف التطفل بمساعدة نموذج الي للكشف عن بعض الهجمات الممكنة الغير تقليدية على المنازل الذكية .**

**الفصل الرابع: النتائج و الآفاق المستقبلية:**

**يهدف هذا الفصل إلى عرض أهم النتائج التي حصلنا عليها من تطوير و تحسين نظام كشف التطفل Snort من خلال استخدام تقنيات التعلم الآلي، بالإضافة إلى اقتراح آفاق مستقبلية يمكن أن تُبنى على ما تم إنجازه في هذا العمل.**

**-النتائج:**

**في هذا القسم نعرض أهم النتائج التي حصلنا عليها بعد تنفيذ مراحل المشروع بدءاً من إنشاء بيئة المحاكاة وصولاً إلى دمج تقنيات الذكاء الاصطناعي ضمن نظام كشف التطفل.**

**1- اكتشاف الهجمات التقليدية:**

**بعد القيام بالتجربة وجدنا أن نظام Snort عند ضبطه بقواعد مخصصة تمّكن من التعرف بدقة على الهجمات المعروفة مثل هجوم حجب الخدمة (DoS) و هجمات الإغراق (flooding) ، لكنه فشل في كشف الهجمات الغير تقليدية مثل Port-Hopping؛ و ذلك بسبب تغيير المنافذ بشكل عشوائي و هو ما يتجاوز آلية المطابقة القائمة على التوقيعات (signature).**

**2-أثر دمج الذكاء الاصطناعي:**

**بعد تطوير نموذج يعتمد على خوارزمية XGBoost، و قيامه بتحليل حركة المرور المستخرجة من ملفات csv أصبح بالإمكان رصد الهجمات غير المعروفة مسبقاً بمستوى دقة مرتفع.**

**3- تعزيز الأمان في بيئة المنازل الذكية :**

**أظهر الجمع بين آلية التوقيعات التقليدية في snort وخوارزمية XG Boost طبقة حماية مزدوجة عززت قدرة النظام على كشف كل من الهجمات المعروفة والهجمات الجديدة ، وقد أدى هذا التكامل الى خفض احتمالية مرور التهديدات الخفية وتحسين مستوى الأمان في بيئات المنازل الذكية ، مما يؤكد اهمية دمج تقنيات التعلم الألة مع انظمة كشف التطفل التقليدية لمواجهة التهديدات المتطورة .**

الخطط المستقبلية:

**1- تحسين الأداء من خلال خوارزميات إضافية ، في المرحلة القادمة يمكن توسيع نطاق التجارب عبر تطبيق خوارزميات تعلم آلي أخرى مثل Random Forest أو LightGBM، إضافةً إلى استخدام تقنيات Ensemble Learning لدمج أكثر من نموذج معًا لزيادة دقة الكشف وتقليل معدل التنبيهات الكاذبة، مما يرفع موثوقية النظام في مواجهة أنماط هجمات مختلفة.**

**2- الكشف في الزمن الحقيقي (Real-Time Detection)**

**يعتمد النظام على تحليل البيانات بعد جمعها، لكن خطوة مهمة نحو التطوير هي تحويل النموذج ليعمل بشكل لحظي أثناء تدفق الحزم داخل الشبكة. اعتماد آليات Online Learning أو دمج النموذج مع وحدة مراقبة مباشرة سيسمح بالتعرف على السلوكيات المشبوهة فور حدوثها، وبالتالي الاستجابة للهجوم قبل أن يتسبب بأضرار واسعة.**

**3- دمج الذكاء الاصطناعي مع آليات استجابة تلقائية ، إضافة طبقة استجابة تلقائية تمثل تطورًا طبيعيًا للنظام الحالي.**

**فهرس المراجع :**

[1] AL-TAAI, Suaad Hadi Hassan; KANBER, Huda Abbas; AL

DULAIMI, Waleed Abood Mohammed. The importance of using the internet of things in education. Int. J. Emerg. Technol. Learn., 2023, 18.1: 19 .

[2] ASIF, Muhammad K., et al. Network intrusion detection and its strategic importance. In: 2013 IEEE Business Engineering and Industrial Applications Colloquium (BEIAC). IEEE, 2013. p. 140-144 .

[3] BACE, Rebecca Gurley, et al. Intrusion detection systems 2001 .

[4] AMRU, Malothu, et al. Network intrusion detection system by applying ensemble model for smart home. International Journal of Electrical and Computer Engineering, 2024, 14.3: 3485-3494 .

[5] J., Asharf, N., et all. A review of intrusion detection systems using machine and deep learning in Internet of things: Challenges, solutions and future directions, Electronics, vol. 9 no. 7, pp. 11-77, 2020 .

[6] N., Chaabouni, M., Mosbah, A., Zemmari, C., Sauvignac, and P. Faruki, Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, vol. 21. no. 3, pp. 2671-2701. 2019 .

[7] G. Altan, SecureDeepNet‐IoT: A deep learning application for invasion detection in industrial Internet of things sensing systems. Transactions on Emerging Telecommunications Technologies, vol.32, no 4, pp. 42- 28.2021 .

[8] H. Sallay, An integrated multilayered framework for IoT security intrusion decisions. Intelligent Automation & Soft Computing, vol 36. no 1.pp. 429-444.2023 .

[9] X., An, X., Zhou, X., Lü, F., Lin, and L. Yang. Sample selected extreme learning machine based intrusion detection in fog computing and MEC. Wireless Communications and Mobile Computing, pp.1-10.2018 .

[10] R., Heartfield, G., Loukas, A., Bezemskij, and E. Panaousis, Selfconfigurable cyber-physical intrusion detection for smart homes using reinforcement learning. IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1720-1735. 2020 .

[11] E. D. Alalade. Intrusion detection system in smart home network using artificial immune system and extreme learning machine hybrid approach. In 2020 IEEE 6th World Forum on Internet of Things (WFIoT). pp. 1-2. 2020 .

[12] M., Noman S., Rosli A.H., Mohammad and, Z. Muhammad. SDN based intrusion detection and prevention systems using manufacturer usage description: a survey. (IJACSA) International Journal of Advanced Computer Science and Applications, vol 11, no 12, 2020 .

[13] A. S., Ibrahim, K. Y., Youssef, H., Kamel, and M. Abouelatta. Traffic modelling of smart city internet of things architecture. IET Communications, vol 4, no 8, pp.1275-1284.2020 .

[14] S., Kumar, et all. Characterizing IoT traffic in smart home and campus environments. Proceedings IEEE INFOCOM pp.2706-2715.2020 .

[15] JAMSHIDI, Saeid, et al. Application of deep reinforcement learning for intrusion detection in Internet of Things: A systematic review. Internet of Things, 2025, 101531 .

[16] D.E. Denning, An intrusion-detection model, IEEE Trans. Softw. Eng. SE-13 (1987), 222–232 .

[17] A. R. Bauer, K. T. Burns, M. V. Esposito, P. L. O’malley, B. J. Olexa, and R. Mcmillan , ”Monitoring system for determining and communicating a cost of insurance,” ed: Google Patents ., (2013 (

[18] H.J. Liao, C.-H. R. Lin, Y.C. Lin, K.Y. Tung, Intrusion detection system: a comprehensive review, J. Netw. Comput. Appl. 36 (2013), 16–24 .

[19] J.M. Fossaceca, T.A. Mazzuchi, S. Sarkani, MARK-ELM: application of a novel multiple kernel learning framework for improving the robustness of network intrusion detection, Expert Syst. Appl. 42 (2015), 4062–4080 .

[20] M. Tavallaee, E. Bagheri, W. Lu, A.A. Ghorbani, A detailed analysis of the KDD CUP 99 data set, in 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, Canada, 2009 .

[21] M. Moradi, M. Zulkernine, A neural network based system for intrusion detection and classification of attacks, in IEEE .

International Conference on Advances in Intelligent Systems-Theory and Applications, Luxembourg, 2004 .

[22] T. Pietraszek, ”Using adaptive alert classification to reduce false positives in intrusion detection,” in International Workshop on Recent Advances in Intrusion Detection, Springer, 2004. pp. 102– 124 .

[23] S. Elhag, A. Fernández, A. Bawakid, S. Alshomrani, F. Herrera, On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems, Expert Syst. Appl. 42 (2015), 193–202 .

[24] S.A.R. Shah, B. Issac, Performance comparison of intrusion detection systems and application of machine learning to Snort system, Future Gener. Comput. Syst. 80 (2018), 157–170 .

[25] C. Links, T. Testa, J. Anderton, W. Van Hoogstraeten, D. Schnaufer, and C. Warschauer, Internet of Things, Qorvo 2nd Special Edition. Hoboken, NJ: John Wiley & Sons, 2021 .