تحسين عملية اكتشاف هجمات رفض الخدمة البطيئة باستخدام المصفوفات الانقباضية

الباحث: م. عمار أسد العساف

كلية: الهمك جامعة: دمشق

المخلص

توفر الشعبية المتزايدة للإنترنت العديد من الخدمات التي تدعم الشبكة والتي يمكن للمستخدم الوصول إليها. ومع ذلك يحاول المهاجمون حرمان المستخدم من هذه الخدمات الحيوية من خلال هجمات DoS (رفض الخدمة). يعد التعامل مع هجوم DoS الذي يستهدف طبقة التطبيق بمعدل بطيء لحركة المرور أحد التحديات الرئيسية التي يواجهها مقدمو الخدمة الآن.

في هذا البحث تم اقتراح نموذج تصنيف عميق باستخدام بيانات التدفق والمصفوفات الانقباضية لاكتشاف هجوم DoS بطيء على HTTP. تم تقييم المصنف باستخدام مجموعة بيانات CICIDS2017. أظهرت النتائج التي تم الحصول عليها أن المصنف يمكن الحصول على دقة 99.9952٪.

الكلمات المفتاحية: رفض الخدمة البطيء ، تدفق البيانات ، المصفوفات الانقباضية ، التعلم العميق.

Improve Detection Of Slow Dos Attacks Using Systolic Arrays

Abstract

The growing popularity of the Internet offers many network-enabled services that the user can access. However, the attackers try to deprive the user of these vital services through DoS (Denial of Service) attacks. Dealing with a DoS attack targeting the application layer with a slow rate of traffic is one of the main challenges that service providers face now.

In this paper, a deep classification model using flow data and systolic matrices is proposed to detect a slow DoS attack on HTTP. The classifier was evaluated using the CICIDS2017 dataset. The obtained results showed that the classifier could obtain an accuracy of 99.9952%.

Keywords: slow denial of service, data flow, systolic matrices, deep learning.

1. المقدمة

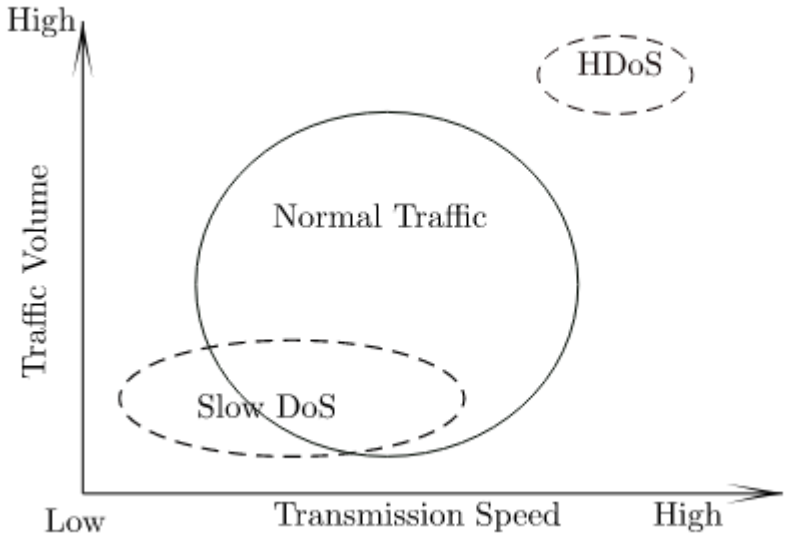
تطور الإنترنت في السنوات القليلة الماضية كمنصة قوية للتواصل. ومن ثم فإن العديد من الخدمات مثل التجارة الإلكترونية والحوسبة السحابية والتمويل وخدمات المواطنين يتم تمكينها عبر الإنترنت. يمكن الوصول إلى هذه الخدمات من قبل المستخدم دون أي حدود جغرافية. نظرًا لأنه يتم الوصول إلى هذه الخدمات الهامة من الخادم عبر الشبكة، يجب ضمان توفر هذه الخدمات لمستخدم حقيقي. لكن المهاجمون يعطلون أو يرفضون الخدمات لمستخدم حقيقي باستخدام هجمات رفض الخدمة (Denial of Service) DoS، هجوم DoS هو هجوم على الإتاحة حيث يرسل المهاجم طلبات غير مرغوب فيها إلى الخادم لإفساد المورد. الإصدار المعقد من DoS يُعرف باسم هجوم الحرمان الموزع للخدمة DDoS (Distributed Denial of Service)يرسل طلبات من عدة مهاجمين إلى نفس الخادم لرفض الخدمات للمستخدمين الحقيقيين[1] .

هجوم DoS / DDoS يهدف لاستهلاك عرض النطاق الترددي للشبكة بين الخدمة المستهدفة والعملاء، يقوم المهاجمون لتحقيق هذا الهجوم بحقن قدر كبير من حركة المرور باستخدام مضيفين مخترقين أو شبكات بوت على الجهاز المستهدف. في الوقت الحاضر تستهدف هجمات DoS / DDoS بيئات مختلفة مثل البنية التحتية السحابية وشبكات المحمول واللاسلكية.[2]

2. مشكلة البحث

فئة من هجمات DoS والمعروفة باسم DoS البطيء، تستهدف موارد التطبيق والخادم عن طريق ضخ حركة مرور قانونية منخفضة الحجم بمعدل بطيء للغاية. نظرًا لأن حجم حركة المرور في DoS البطيء منخفض جدًا، يمكن تنفيذ هذا الهجوم باستخدام عدد أقل من الأجهزة. ونظرًا لأن حركة مرور DoS البطيئة تبدو قانونية، فقد تفشل الأساليب التقليدية في اكتشاف هذه الهجمات.[3]

يوضح الشكل(1) الفرق بين حركة المرور العادية وهجمات DoS / DDoS الضخمة وهجمات DoS البطيئة. كما هو مبين في الشكل، من خلال النظر في حجم حركة المرور وسرعة الإرسال، تتداخل حركة المرور العادية ومناطق حركة مرور DoS البطيئة. هذا يجعل من الصعب التمييز بين هجمات DoS البطيئة وحركة المرور العادية وكذلك منعها.[4]



الشكل(1) رسم توضيحي لحركة المرور العادية وDoS البطيئة وDoS الضخمة.

التحديات الرئيسية في تصنيف DoS البطيء من حركة المرور العادية هي:

- يستخدم اتصالًا شرعيًا أثناء الهجوم.
- مطلوب عدد أقل من الاتصالات لشن الهجوم.
- استخدام النطاق الترددي وحجم حركة المرور لهجوم DoS البطيء منخفضان. ومن ثم فإن الأنظمة التقليدية غير قادرة على اكتشافها.

تم اقتراح طرق مختلفة لاكتشاف هجمات DoS البطيئة. في الآونة الأخيرة تم استخدام الشبكات المعرفة بالبرمجيات (SDN) والنهج القائم على التعلم الآلي لاكتشاف هجمات DoS البطيئة.[5] في هذا البحث تم اقتراح مصنف DoS البطيء المستند إلى التعلم العميق والمصفوفات الانقباضية.

النهج المقترح له المزايا التالية مقارنة باكتشاف هجوم DoS البطيء المستند إلى المضيف:

- يمكن جمع بيانات التدفق وتحليلها من بوابة الشبكة، لذلك يمكن تنفيذ نظام وقائي لخطورة DoS البطيئة قبل وصول حركة مرور الهجوم إلى الجهاز المصاب.
- يمكن استخدام مصنف DoS البطيء في أي خادم ويب دون أي تغييرات في التكوين على مستوى الخادم.

3. الدراسات المرجعية

تمت مناقشة اكتشاف الاختراق في شبكات الحاسوب على نطاق واسع في الأبحاث المختلفة. تم اقتراح العديد من تقنيات الكشف واستراتيجيات الحماية في السنوات الأخيرة. تصنف الدراسات في الأدبيات أنظمة IDS على أنها أنظمة

مبنية على التوقيع، وقائمة على السلوك غير الطبيعي، وأنظمة هجينة. يحدد النوع الأول الهجمات المحتملة من خلال مقارنة الأحداث الحالية التي تمت ملاحظتها بالتوقيعات المخزنة. يكتشف الثاني السلوك غير الطبيعي من خلال تحديد الانحرافات الكبيرة بين الملف الشخصي العادي المحدد مسبقًا والأحداث الجارية. الميزة الرئيسية للنهج القائم على التوقيع هو معدل الإنذار الخاطئ المنخفض. ومع ذلك فإن التحدي يكمن في كتابة التوقيعات التي تغطي جميع أشكال الهجوم المحتملة. على النقيض من ذلك فإن النهج القائم على السلوك غير الطبيعي لديه القدرة على اكتشاف الهجمات غير المعروفة، لكنه يتطلب المزيد من الموارد الحسابية وغالبًا ما ينتج المزيد من الإنذارات الكاذبة. تحاول الحلول الهجينة استغلال فوائد كلتا الطريقتين [6]. تعد هجمات DoS نوعًا محددًا من اقتحام الشبكة الذي لفت انتباه الأوساط الأكاديمية. تم اقتراح العديد من استراتيجيات التصنيف لهجمات DDoS في الأدبيات في العقد الماضي. تستهلك هجمات DoSعلى مستوى التطبيق عمومًا نطاقًا ترددياً أقل وتكون بطبيعتها أكثر سرية من الهجمات الضخمة لأنها تشبه إلى حد بعيد حركة المرور غير الضارة .يكمن التحدي الأكبر في مكافحة هجمات DoS في الاكتشاف المبكر للهجمات والتخفيف من حدتها في أقرب مكان ممكن من مصدرها، ومع ذلك فإن تنفيذ حل شامل يعالج هذه الميزات لم يتحقق بعد. ألهمت بعض الأعمال الحديثة تطوير نظام الاكتشاف المقترح.

الجدول(1) مقارنة الدراسات المرجعية

References	Dataset	Online	L/H DoS	Sampling
[7]	CIC-DoS	✗	✓	✓
[8]	CICIDS2017	✗	✓	✗
[9]	CICIDS2017	✗	✓	✗
[10]	CICIDS2017	✗	✓	✗
[11]	None	✓	✗	✗
[12]	MIT Lincoln, FIFA98, DDoSTB, CAIDA	✓	✓	✗
[13]	Customized (developed by the authors)	✓	✓	✗
[14]	Customized (developed by the authors)	✓	✓	✗
[15]	CICIDS2017	✗	✓	✗

4. هجوم DoS البطيء

يستهدف DoS البطيء طبقة التطبيق عن طريق إرسال حركة مرور قانونية بمعدل منخفض جدًا. الخاصية الشائعة لهجمات DoS البطيئة هي أن الخوادم يبدو أنها تحتوي على عدد كبير من العملاء المتصلين ولكن حمل المعالجة الفعلي سيكون منخفضًا للغاية. نظرًا لأن HTTP هو بروتوكول طبقة تطبيق بارز يستخدم في الإنترنت لذلك أصبح أحد الأهداف الشائعة لهجوم DoS البطيء. وتظهر الدراسات الحديثة أن HTTP\2، هو أيضًا عرضة للعديد من هجمات DoS البطيئة. ومن ثم فإن اكتشاف ومنع هجوم DoS البطيء له أهمية قصوى في الإنترنت في يومنا هذا.[16]

4.1. Slowloris

تبدأ خوادم الويب المعرضة لهجوم بطيء في معالجة الطلب فقط بعد تلقي الطلب بالكامل من العميل. من خلال معرفة ذلك يرسل المهاجم طلبات HTTP جزئية لفتح اتصالات بخادم الويب المعرض للخطر. بمجرد فتح الاتصال يحاول المهاجم الحفاظ على هذه الاتصالات حية لأطول فترة ممكنة عن طريق إرسال الجزء التالي من الطلب قبل انتهاء مهلة الاتصال مباشرة، مما يؤدي إلى إرباك خادم الضحية وإبطائه.[7]

4.2. Slow POST

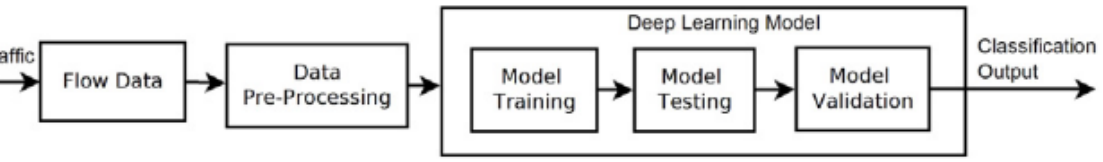
في هجوم Slow POST يستخدم المهاجم طريقة HTTP POST قانونية من خلال تعيين رقم كبير جدًا لقيمة "طول المحتوى content-length " في الطلب. عند تلقي هذا الطلب يخصص الخادم الموارد اللازمة لمعالجة بيانات طول المحتوى المحددة. في وقت لاحق يرسل العميل البيانات بمعدل بطيء للغاية مما ينتج عنه اتصال مفتوح مطول في الخادم.[17]

4.3. Slow read

يرسل العميل طلبات HTTP قانونية إلى الخادم ويقرأ الاستجابة بمعدل بطيء جدًا. يمنع المهاجم الخادم من إعادة تعيين الاتصال عن طريق تعيين حجم الإطار الصفري في الحزمة. عند استلام الحزمة بحجم نافذة صفري، يعتقد الخادم أن العميل يقرأ البيانات بالفعل وبالتالي يبقي الاتصال مفتوحًا.[18]

5. نموذج مصنف DoS البطيء باستخدام التعلم العميق

يوضح الشكل (2) سير العمل لنموذج تصنيف DoS البطيء[8]. يأخذ النموذج حركة مرور الشبكة كمداخل ويقدم النتائج المصنفة بناءً على عملية التعلم العميق. يتم تجميع البيانات ومعالجتها بشكل مسبق ومن ثم إدخالها في نموذج التعلم العميق. تتمثل إحدى مزايا التعلم العميق على التعلم الآلي في أنه يمكنه تعلم الميزات المهمة تلقائيًا بدون مدخلات يدوية. ونظرًا لأن عدد الميزات وحجم البيانات أكبر فقد تم استخدام نموذج شبكة عصبية عميقة للتصنيف.



الشكل 2: سير عمل نموذج تصنيف DoS البطيء المعتمد على التعلم العميق.

5.1. بيانات تدفق الشبكة

يمكن تعريف تدفق الشبكة Network flow على أنه تسلسل أحادي الاتجاه لحزم بروتوكول معين تنتقل بين عنوان IP المصدر والوجهة والمنافذ خلال فترة زمنية. يتم إنشاء التدفقات من الحزم عن طريق تجميعها باستخدام الحقول الرئيسية key fields. الحقول المستخدمة لاشتقاق بيانات التدفق من حزم الشبكة موضحة أدناه. [8]

$$Key = \{SrcIP,\ DstIP,\ SrcPort,\ DstPort,\ Proto\} \quad (1)$$

بالإضافة إلى هذه الحقول، تتكون بيانات التدفق من معلومات مشتقة من الاتصال مثل المدة والبايت والحزم المنقولة وقيم علم TCP (TCP flag).[19]

هناك عدة أسباب لاختيار بيانات مستوى التدفق كمدخل لتصنيفنا:

- حجم البيانات أقل مقارنة بمعلومات مستوى الحزمة.
- حجم البيانات أقل وبالتالي يمكن جمع البيانات طويلة الأجل (long term data) وتحليلها. سيساعد هذا في اكتشاف الهجمات البطيئة التي تستمر لفترة أطول.

5.1.1. مجموعة البيانات المستخدمة

تُستخدم مجموعة بيانات تقييم كشف الاختراق المتوفرة في المعهد الكندي للأمن السيبراني (CICIDS2017) في نموذج التدريب والتحقق.[13] يحتوي على بيانات متعددة الاتجاهات بما في ذلك DoS وهجمات الويب والاختراق و botnet و DDoS. لقد اخترنا مجموعة بيانات DoS لنموذج التصنيف الخاص بنا.

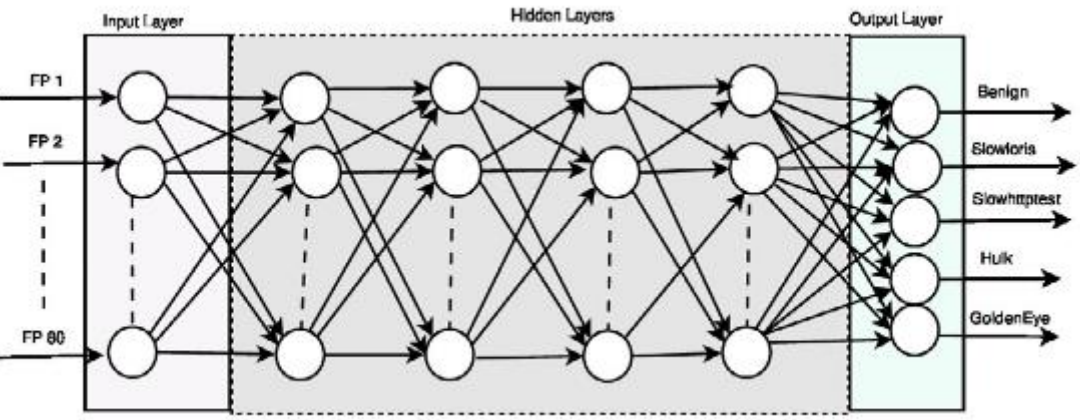
5.1.2. المعالجة المسبقة للبيانات

تتكون مجموعة بيانات CICIDS2017 من تدفقات ثنائية الاتجاه مصنفة بتنسيق مفصولة بفواصل (.CSV)، مجموعة البيانات النهائية المختارة للتصنيف تتكون من 80 معلمة. حركة المرور الحميدة يتم تصنيفها على أنها "Benign"، ويتم تصنيف سجلات التدفق الخاصة بالمهاجمين على أنها "Slowloris" و "Slowhttptest" و "Hulk" و "GoldenEye". يتم تحويل هذه التسميات إلى قيم صحيحة تبدأ من واحد وتنتهي بخمسة والتي تمثل تدفقات "Benign" و "Slowloris" و "SlowHTTP" و "Hulk" و "GoldenEye" على التوالي.

5.2. المصنف القائم على التعلم العميق

كما هو مبين في الشكل 3، يتكون نموذج التعلم العميق من 3 طبقات مختلفة ("طبقة الإدخال" و "الطبقات المخفية" و "طبقة الإخراج"). طبقة الإدخال تعطي معلومات للشبكة. تعالج الطبقة المخفية العلاقات غير القابلة للفصل خطيًا وتمرر المعلومات من طبقة الإدخال إلى طبقة الإخراج. تقوم طبقة الإخراج بتصنيف حركة المرور إلى الحميد أو DoS البطيء.

يتم استخدام شبكة متصلة بالكامل في نموذج التصنيف، تأخذ طبقة الإدخال معلمات مستوى التدفق كمدخلات. نظرًا لأننا حددنا 80 ميزة في بيانات التدفق، فإن عدد الخلايا العصبية في طبقة الإدخال ثابت على أنه 80. يتم تمثيل ميزات مستوى التدفق المستخدمة في طبقة الإدخال من "FP1" إلى "FP80". تحتوي طبقة الإخراج على نفس عدد الخلايا العصبية في عدد الفئات في مجموعة البيانات. ومن ثم فإن الخلايا العصبية في طبقة الخرج ثابتة على أنها خمسة.



الشكل(3) نموذج التعلم العميق المستخدم لتصنيف DoS البطيء

5.2.1. تدريب النموذج

لتصنيف سجلات تدفق DoS البطيئة وسجلات التدفق الحميد، تم تدريب النظام باستخدام بيانات التدريب. وتم تطبيق تقنية تعلم خاضعة للإشراف. يتم تلخيص البيانات المستخدمة للتدريب والاختبار والتحقق من المصنف في الجدول 2. وتم استخدام الوحدة الخطية المصححة (ReLU) كوظيفة التنشيط في الطبقة المخفية. يستخدم نموذجنا لتصنيف أربعة DoS بطيئة مختلفة من حركة المرور الحميدة. وتم استخدام وظيفة التنشيط "softmax" في طبقة الإخراج. تم استخدام خوارزمية التحسين "adam" لتحسين دالة التكلفة. تُستخدم تقنية التحسين هذه في نموذجنا لدعم البيانات الكبيرة بعدد أكبر من المعلمات. تم تنفيذ النموذج باستخدام "API Keras" [20] و "SciKit" [21]. لقد قمنا بتكوين خيار "الإيقاف المبكر" في العصر بخمسة هي قيمة الصبر.

Total records	Training	Testing	Validation
32,190	19,314	6,438	6438

الجدول 2: ملخص البيانات المستخدمة في التدريب والاختبار والتحقق.

6. المصفوفة الانقباضية

المصفوفة الانقباضية عبارة عن شبكة متخصصة من الخلايا التي تؤدي العمليات الحسابية المعقدة للبيانات بسرعة، ويتميز النمط الانقباضي بتطبيق مكثف لكل من الأنبوبية والتوازي، ويتم التحكم فيهما بواسطة ساعة عالمية ومتزامنة تمامًا. تتدفق

تدفقات البيانات بشكل إيقاعي عبر شبكة الاتصالات، مثل تيارات الدم تنطلق من القلب عبر الأوردة في الجسم. هنا لا يتم تقييد خطوط الأنابيب على محور فضاء واحد ولكن يتعلق بجميع تدفقات البيانات التي ربما تتحرك في اتجاهات مختلفة وتتقاطع في خلايا المصفوفة الانقباضية.[9] يتكون النظام الانقباضي عادة من جهاز كمبيوتر مضيف، ومصفوفة انقباضيه فعليه. [22] وتعرف الخوارزمية الانقباضية بانها البرنامج الذي يتم تنفيذه بشكل تعاوني بواسطة خلايا المصفوفة الانقباضية. [9]

6.1. المصنف القائم على المصفوفات الانقباضية

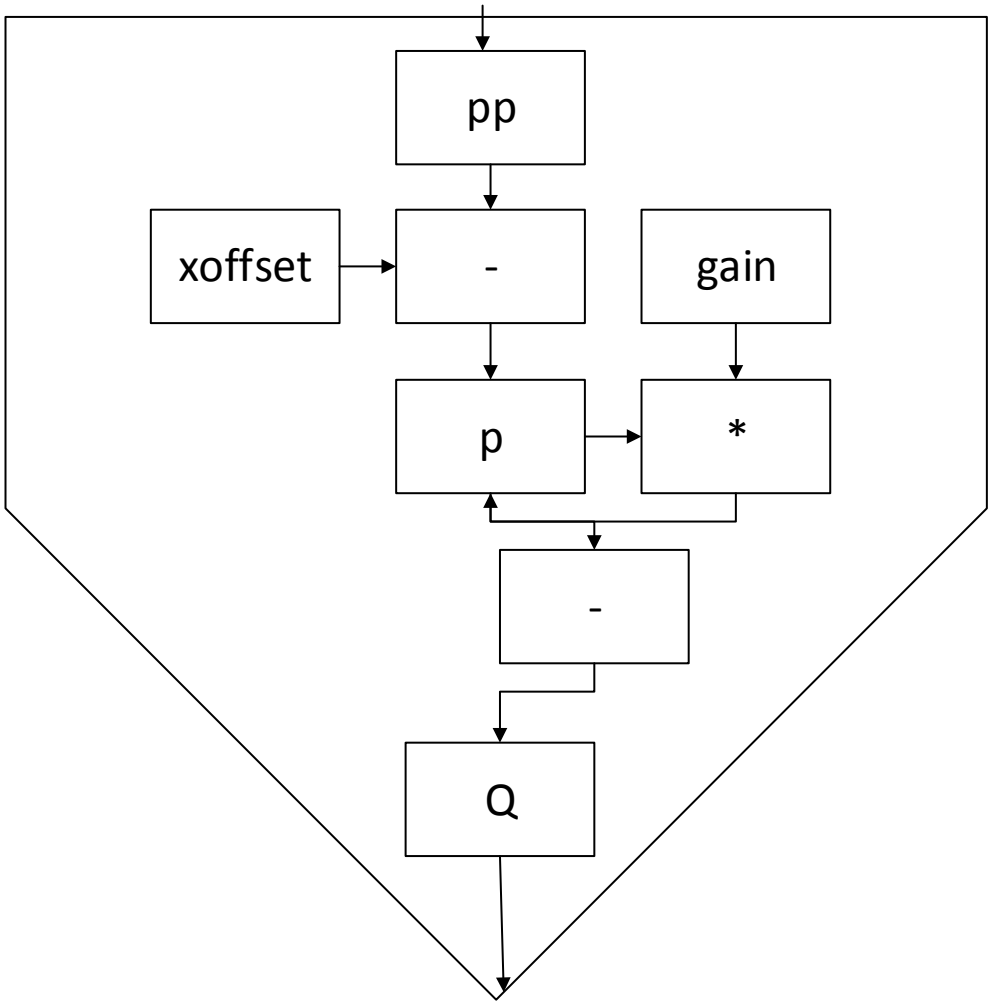
النموذج الرياضي لكل خلية من خلايا المصفوفة الانقباضية، حيث سنستخدم عدة أنواع من الخلايا يمكن توصيفها رياضيا كالتالي:

النوع الأول:

$$p=pp-xoffset \quad (3)$$

$$p=p*gain \quad (4)$$

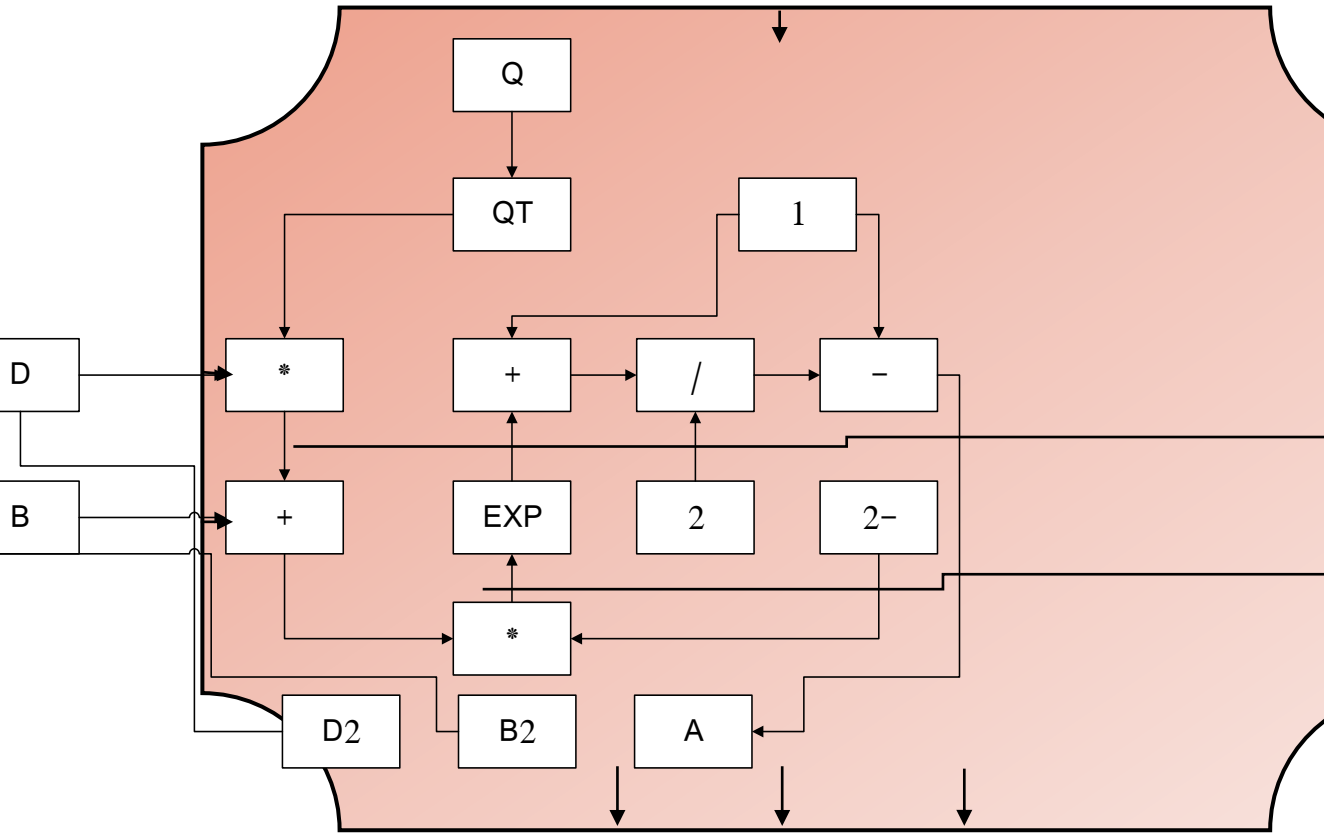
$$Q=p+ymin \quad (5)$$



الشكل(6) بنية الخلية الأولى

النوع الثاني:

$$A= (2 / (1 + \exp(-2*(B+D*Q^T)))-1) \quad (5)$$

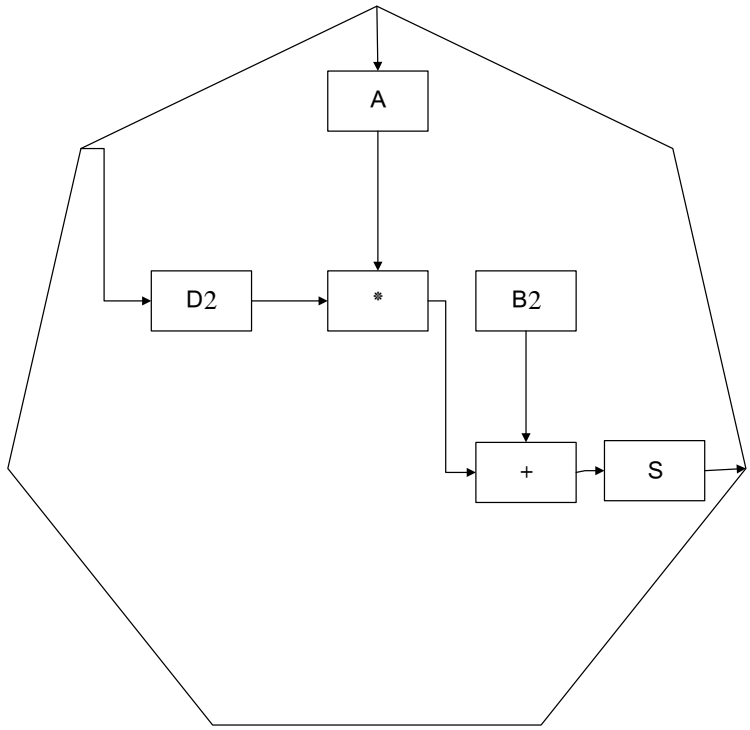


الشكل(7) بنية الخلية الثانية

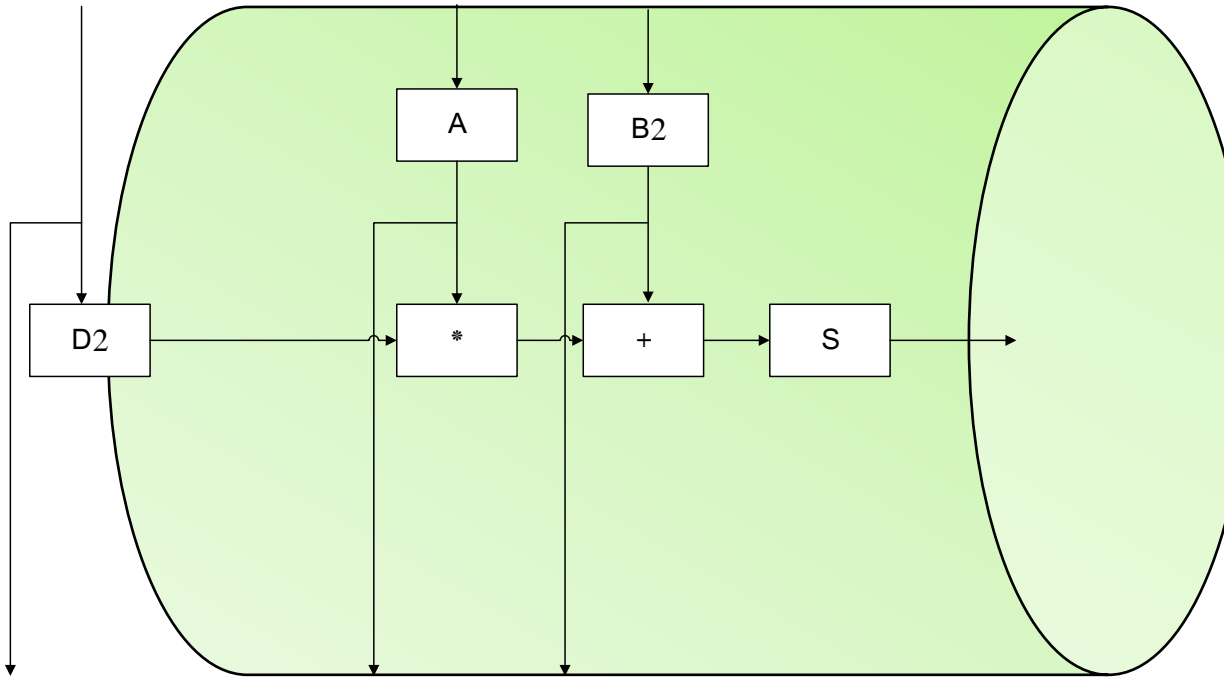
النوع الثالث:

$$S=B_2+D_2*A^T \qquad (6)$$

حيث أن البنية المقترحة تتطلب تمثيل المعادلة(6) بنوعين من الخلايا، النوع الأول ويمثل الخلية الثالثة وهو خاص بطبقة الدخل، والنوع الثاني يمثل الخلية الرابعة وهو خاص بالطبقات الخفية.



الشكل(8) بنية الخلية الثالثة

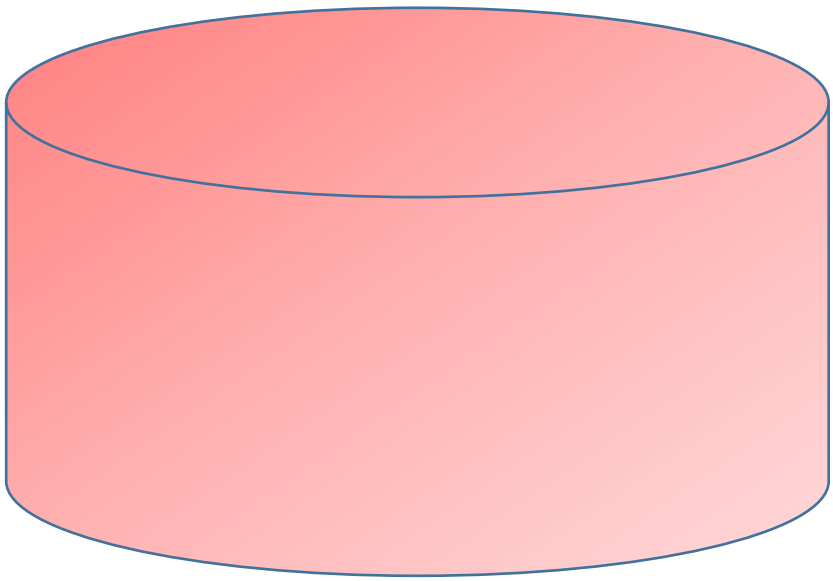


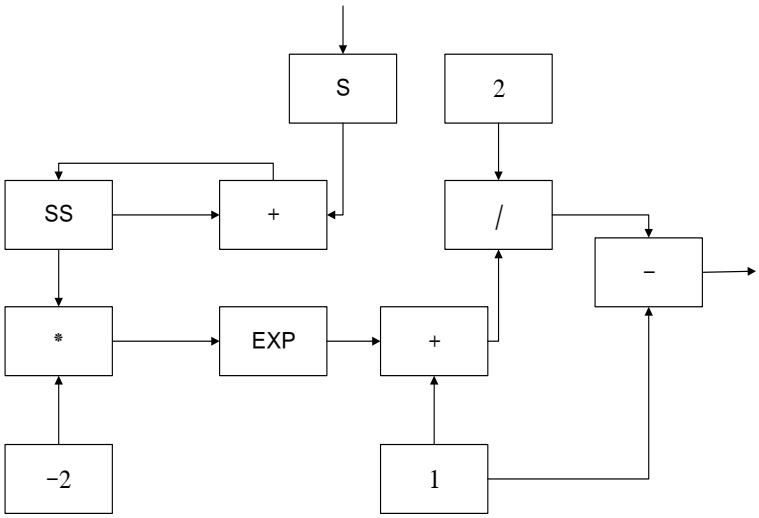
الشكل(9) بنية الخلية الرابعة

النوع الرابع:

$$SS=SS+S \quad (7)$$

$$R= 2 / (1 + \exp(-2*ss)) - 1 \quad (8)$$





الشكل(10) بنية الخلية الخامسة

حيث أن:

pp عبارة عن بيانات دخل النظام والتي هي 80 ميزة في بيانات التدفق ، أما بالنسبة للبارامترات الأخرى (xoffset ، B ، D ، gain ، ymin) يتم إيجاد القيم المثلى لها باستخدام خوارزميات الأدلة العليا metaururistics –في علوم الحاسب والأمثلة الرياضية– والتي هي إجراءات أو إرشادات عالية المستوى مصممه لإيجاد أو ابتكار أو اختيار طرق بحث خوارزميه نحصل من خلالها على حلول عالية الجودة لمسألة الأمثلة خاصه إذا كانت المعلومات غير كافيه أو غير كامله أو إذا كانت السعه الحسابية محدودة .الأدلة العليا تضع نماذج للحلول التي تكون كبيرة جدا لأخذ امثله منها وهي أيضا (الأدلة العليا) تقدم بعض الافتراضات الخاصة بمشكله الأمثلة التي نقوم بحلها كي نستطيع إعادة استخدامها في حل العديد من المشكلات .بالمقارنة بالخوارزميات الخاصة بالأمثلة والطرق التكرارية فان الأدلة العليا لا تضمن إيجاد أفضل حل عامه على مستوى قطاع معين من

مسائل (مشكلات) الأمثلة. العديد من طرق الأدلة العليا تنفذ بعض عمليات الأمثلة العشوائية حتى يكون الحل الناتج معتمدا على المتغيرات العشوائية المولدة وبالبحث في مجموعه كبيرة من الحلول الممكنة، عمليا فان الأدلة العليا يمكنها غالبا إيجاد حلول جيده بمجهود حسابي اقل من الطرق التكرارية والخوارزميات ولذلك فهي (الأدلة العليا) نهج مفيد في حل مشكلات الأمثلة. الخوارزمية المعتمدة لأمثلة البارامترات:

الخطوة الأولى: تهيئة القيم البدائية لخوارزمية

L=الحد الأدنى, H= الحد الأعلى

$$X_{ij}=L+(L-H) \qquad (9)$$

الخطوة الثانية: توليد ارقام عشوائية r_1, r_2, r_3 حيث $r_1 \neq r_2 \neq r_3$ وتقع ضمن المجال.

الخطوة الثالثة: توليد الشعاع v

$$v_j = X_{r3} + F.(X_{r1} - X_{r2}) \qquad (10)$$

حيث أن F هو الوزن المطبق على الفرق العشوائي (عامل التحجيم)

الخطوة الرابعة: تطبيق معامل العبور

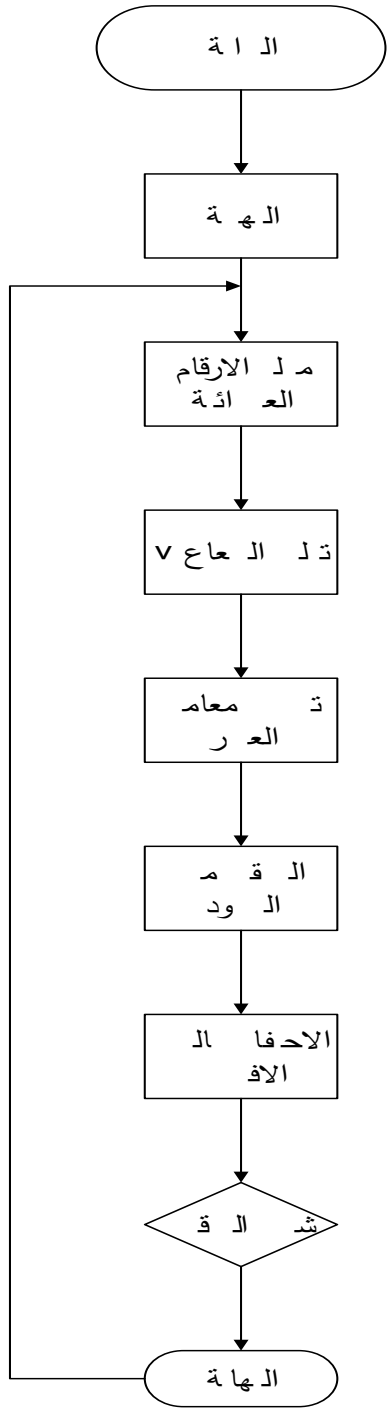
$$U_j = \begin{cases} v_j & if\ rand[0\ 1] \leq CR \\ & \text{او} \\ X_j \end{cases} \qquad (11)$$

CR هو ثابت العبور

الخطوة الخامسة: التحقق من الحدود

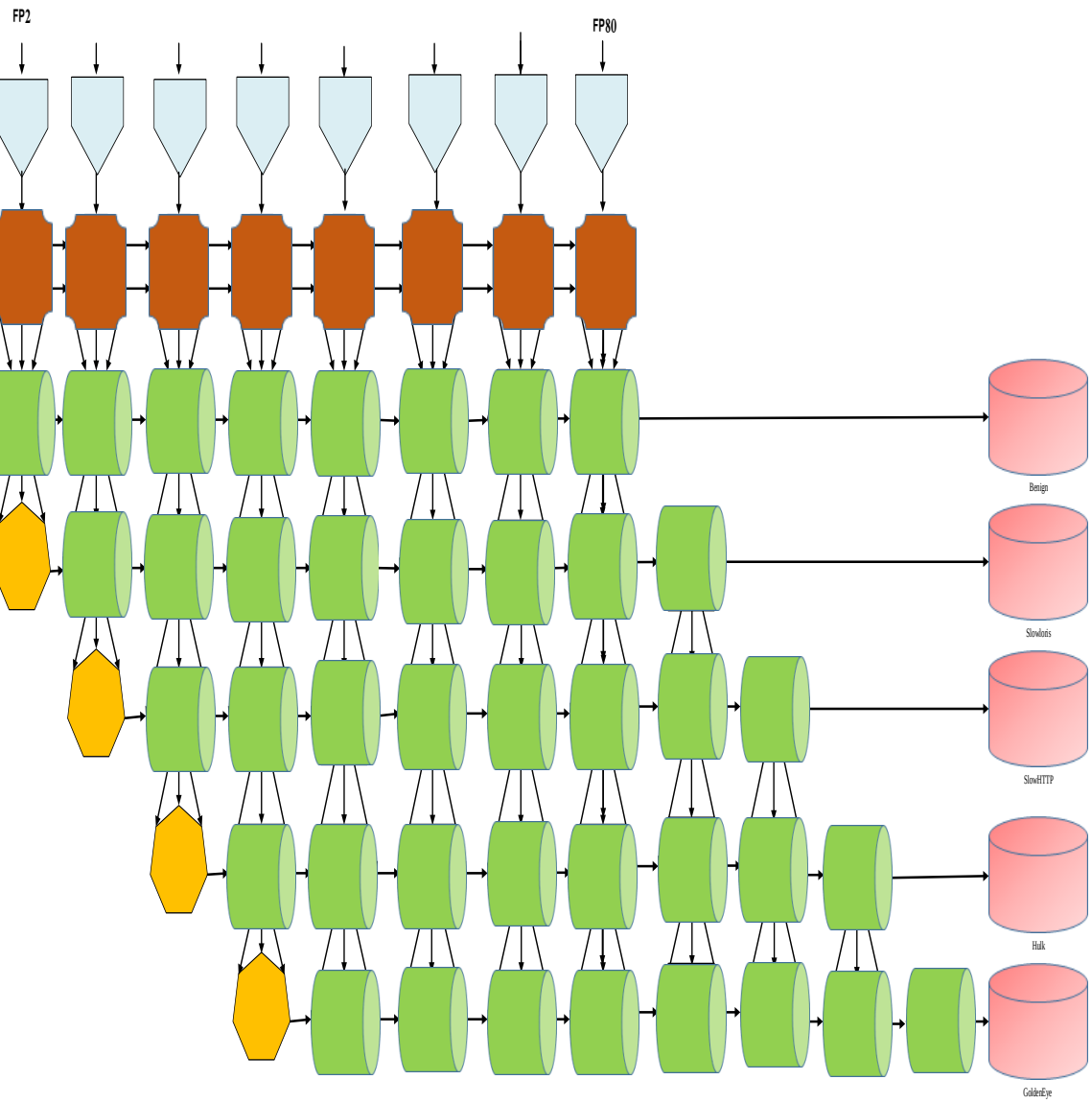
If ($U_j \neq$[L, H])? U_j= L+(L−H)

الخطوة السادسة: حفظ الحل الأفضل



الشكل(11) خوارزمية امثلة البارامترات

وبعد تصميم الخلايا المكونة للمصفوفة الانقباضية يمكن تصميم المصفوفة بشكل كامل حيث أن بيانات النظام هي مداخل للخلايا من النوع الأول والتي تأخذ بيانات إضافية كدخل لها ، ومن المهم ملاحظة أن عملية تطبيق بيانات الدخل لا يتم بشكل مباشرة ، أي انه لا تطبق كل البيانات معا في نفس الوقت ، وإنما يتم تطبيقها بشكل تدريجي ، حيث أن شكل عملية تطبيق الدخل وخرج هذه الخلايا ينتشر بشكل مشابه لسريان الدم في الكائنات الحية ضمن الخلايا من النوع الثاني والتي تأخذ بيانات إضافية كمداخل أيضا ، وخرج الخلايا من النوع الثاني ينتشر بنفس الأسلوب ليصل لخلايا النوع الثالث والتي تمثل خرج النظام ، لذلك يوجد 5 خلايا في الخرج وهذه الخلايا مرقمة من الواحد الى خمسة، عند تطبيق بيانات دخل للنظام فإن خلايا الخرج قيمتها إما تكون صفر أو واحد ، والمصفوفة الانقباضية الكاملة:



الشكل(12) المصفوفة الانقباضية كاملة

ويتم بناء خلايا المصفوفة الانقباضية برمجياً باستخدام الماتلاب :

```
for i=1:80
    A(i)= (2 / (1 + exp(−2*(B(i)+D (i, :)*Q')))−1);
for j=1:5
  S (j, i) =B2(j)+D2(j, :)*A';
End
end
for j=1:5
    for i=1:80
        SS (1, j) =SS (1, j) +S (j, i);
    End
End
for j=1:5
  ss2(j)= 2. / (1 + exp(−2*SS(j))) − 1;
end
```

7. النتائج

تظهر النتائج التي تم الحصول عليها من تصنيف DoS البطيء أن النموذج قادر على تحقيق دقة إجمالية بنسبة 99.8٪. مصفوفة الارتباك للنموذج الذي حصل على هذه الدقة موضحة في الشكل(13). يُظهر المحور "x" لمصفوفة الارتباك التسمية المتوقعة ويظهر المحور "y" التسمية الحقيقية. من خلال مقارنة عدد السجلات في كل صنف، يمكننا ملاحظة أن السجلات في كل صنف لا يتم توزيعها بشكل موحد. ومن ثم قمنا بحساب F1 score كمقياس للأداء بالإضافة إلى precision و recall. يظهر ملخص دقة التصنيف precision التي تم الحصول عليها و recall و F1 score في الجدول 2.

القيم الحقيقية						
	Benign	1996	1	0	1	1
	Slowloris	1	821	1	0	0
	SlowHTTP	0	1	485	0	0
	Hulk	0	0	0	1553	0
	GoldenEye	0	0	0	0	1567
		Benign	Slowloris	SlowHTTP	Hulk	GoldenEye
	القيم المتوقعة					

الشكل(13) مصفوفة الارتباك لخرج المصنف.

Traffic type	Precision	Recall	F1 score
Benign	0.99	1.00	1.00
Slowloris	1.00	0.99	0.99
Slowhttptest	1.00	0.99	0.99
Hulk	1.00	1.00	1.00
GoldenEye	1.00	1.00	1.00

الجدول 2: ملخص نتيجة التصنيف

ويوضح الجدول 3 مقارنة النتائج من حيث الدقة مع أحدث وأهم الدراسات السابقة.

الخوارزمية المستخدمة	قاعدة البيانات	رقم المرجع	الدقة
الخوارزمية المستخدمة	CICIDS2017	–	99.9952
ML	CICIDS2017	[22]	99.9920
DL	CICIDS2017	[21]	99.6100
SVM	CICIDS2017	[23]	82.1000

الجدول 3: مقارنة النتائج

يلاحظ من مقارنة النتائج السابقة تفوق النموذج المقترح على الدراسات المرجعية السابقة، يرجع ذلك التفوق الى بنية المصفوفة الانقباضية والتي تتميز بالمعالجة التفرعية للبيانات.

8. التوصيات المستقبلية

تم تقديم مصنف قائم على التعلم العميق والمصفوفات الانقباضية لهجوم HTTP DoS البطيء. تم تقييم المصنف باستخدام مجموعة بيانات CICIDS2017. أظهرت النتائج التي تم الحصول عليها أن المصنف يمكنه تصنيف الهجوم بدقة 99.9952٪. على الرغم من أن المصنف قد حقق دقة أعلى، إلا أنه من المهم تقييم المصنف وقياس أدائه مع حركة المرور الحقيقية.

المراجع

[1] S.T. Zargar, J. Joshi, D. Tipper, A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks, IEEE Commun. Surv. Tutor. 15 (4) (2013) 2046–2069.

[2] A. Almomani, M. Alauthman, F. Albalas, O. Dorgham, A. Obeidat, An online intrusion detection system to cloud computing based on neucube algorithms, Int. J. Cloud Appl. Comput. 8 (2) (2018) 96–112.

[3] A. Bhardwaj, S. Goundar, Comparing single tier and three tier infrastructure designs against DDoS attacks, Int. J. Cloud Appl. Comput. 7 (3) (2017) 59–75.

[4] K. Bhushan, B.B. Gupta, Distributed denial of service (ddos) attack mitigation in software defined network (SDN)-based cloud computing environment, J. Ambient Intell. Humaniz. Comput. 10 (5) (2019) 1985–1997.

[5] F.S. d. Lima Filho, F.A. Silveira, A. de Medeiros Brito Junior, G. Vargas-Solar, L.F. Silveira, Smart detection: An online approach for DoS/DDoS attack detection using machine learning, Secur. Commun. Netw. (2019).

[6] M. Latah, L. Toker, Minimizing false positive rate for DoS attack detection: A hybrid SDN-based approach, ICT Express 6 (2) (2020) 125–127.

[7] E. Cambiaso, G. Papaleo, M. Aiello, Taxonomy of slow DoS attacks to web applications, in: International Conference on Security in Computer Networks and Distributed Systems, Springer, Berlin, Heidelberg, 2012, pp. 195–204.

[8] Muraleedharan, N., and B. Janet. "A deep learning based HTTP slow DoS classification approach using flow data." *ICT Express* 7.2 (2021): 210-214.

[9] Nugraha, Beny, and Rathan Narasimha Murthy. "Deep learning-based slow DDoS attack detection in SDN-based networks." *2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*. IEEE, 2020.

[10] M. Aamir and S. M. A. Zaidi, “Clustering based semi-supervised
machine learning for DDoS attack classification,” Journal of
King Saud University—Computer and Information Sciences,

2019.

[11] R. K. C. Chang, “Defending against flooding-based distributed denial-of-service attacks: a tutorial,” IEEE Communications Magazine, vol. 40, no. 10, pp. 42–51, 2002.

[12] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, “Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data,” IEEE Access, vol. 6, pp. 7234–7243, 2017.

[13] B. Pfaff, J. Pettit, T. Koponen et al., “The design and implementation of Open vSwitch,” in 12th USENIX Symposium on Networked Systems Design and Implementation (NSDI 15), pp. 117–130, USENIX Association, Oakland, CA, USA, 2015,

[14] J. Le, R. Giller, Y. Tatsumi, H. Huang, J. Ma, and N. Mori, Case Study Developing DPDK-Accelerated Virtual Switch Solutions for Cloud Service Providers, Intel Corporation, Santa Clara, CA, USA, 2019,

[15] R. Panigrahi and S. Borah, “A detailed analysis of CICIDS2017 dataset for designing intrusion detection Systems,” International Journal of Engineering & Technology, vol. 7, no. December, pp. 479–482, 2018,

[16] N. Tripathi, N. Hubballi, Slow rate denial of service attacks against HTTP/2 and detection, Comput. Secur. 72 (2018) 255–272.

[17] M.M. Najafabadi, T.M. Khoshgoftaar, A. Napolitano, C. Wheelus, RUDY Attack: Detection at the Network Level and Its Important Features., in: FLAIRS Conference, 2016, pp. 288– 293.

[18] J. Park, K. Iwai, H. Tanak, T. Kurokawa, Analysis of Slow Read DoS Attack and Countermeasures, in: The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014), The Society of Digital Information and Wireless Communication, 2014, pp. 37–49.

[19] R. Hofstede, P. Celeda, B. Trammell, I. Drago, R. Sadre, A. Sperotto,

A. Pras, Flow monitoring explained: From packet capture to data analysis with NetFlow and IPFIX, IEEE Commun. Surv. Tutor. 16 (4) (2014) 2037–2064.

[20] Keras: The Python Deep Learning library, [Online]. Available: https:/

/keras.io/.

[21] scikit-learn: Machine Learning in Python, [Online]. Available: https:// scikit-learn.org/stable/index.html.

[22] P. Phaal and M. Lavine, sFlow version 5, InMon Corp, San Francisco, CA, USA, 1981, https://sflow.org/sflow_version_5.txt.

[23] S. Simpson, S. N. Shirazi, A. Marnerides, S. Jouet, D. Pezaros, and D. Hutchison, "An inter-domain collaboration scheme to remedy DDoS attacks in computer networks," IEEE Transactions on Network and Service Management, vol. 15, no. 3, pp. 879–893, 2018.