مجلة جامعة دمشق للعلوم الهندسية
المجلد42 العدد (1) – 2025: 221-231

Damascus University Journal for engineering sciences
Vo 42 number (1) -2025: 221-231

تخفيف أثر هجمات الحرمان من الخدمة باستخدام طريقة تعاونية بين مزودات خدمة الانترنت

سامر ممتاز سليمان*[1] وسيم السمارة[2] رأفة خازم[3]

*[1]. طالب دكتوراه، جامعة دمشق، هندسة الحواسيب وشبكاتها، samer.sulaiman@damascusuniversity.edu.sy

[2]. أستاذ مساعد ،دكتور، مهندس، جامعة دمشق، شبكات ومراكز التحويل وتوزيع المعطيات . wasim.alsamara@damascusuniversity.edu.sy

[3]. مدرس، دكتور، مهندس، جامعة دمشق، القيادة والقياس عن بعد، Raafah.Khazem@damascusuniversity.edu.sy

الملخص:

تطورت وسائل التصدي لهجمات الحرمان من الخدمة خلال السنوات الماضية وقد تم الاعتماد على العديد من التقنيات الحديثة في تطوير آليات حماية محلية تساعد في التخفيف من شدة هذه الهجمات وتعزز من أمن الشبكات بشكل عام. على الرغم من أنّ استخدام التقنيات الحديثة ساهم في تخفيف الآثار السلبية لبعض أنواع الهجمات إلا أنّ هذه المحاولات الإفرادية قد لا تثمر حلًا فعالًا للتصدي للهجمات وإنما يجب العمل على تطوير حلول تعاونية بين عدة جهات للتخفيف من أثر هذه الهجمات. تم في هذه الدراسة استخدام بنية معطيات يتم تبادلها بين أجهزة الشبكات المختلفة والتي تتضمن معلومات خاصة بالهجمات التي يتم اكتشافها وتعميمها على جميع الأجهزة ضمن الشبكة وكأنها عملية وشاية، تحقق الطريقة المقترحة حلًا رادعًا عن طريق عزل كامل التجهيزات الشبكية التي تشارك بهجمات الحرمان من الخدمة حتى ولو لم تتعاون جميع التجهيزات في التصدي للهجمات وذلك عبر تبادل بنية معطيات DoSGoS بين التجهيزات المختلفة. أظهرت النتائج تحسنًا في تخفيف أثر هجمات الحرمان من الخدمة عبر عزل المهاجمين مهما كان نوع الهجمة المستخدمة وضمن وقت مقبول انطلاقًا من بدء الهجمة.

الكلمات المفتاحية: هجمات الحرمان من الخدمة، أمن الشبكات، الوشاية

تاريخ الإيداع: 2023/5/16
تاريخ القبول: 2023/6/21

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

Reducing the effects of Denial of Service attacks using a cooperative method between ISP's

Samer Momtaz Sulaiman*[1] Wassim Alsamara[2] Raafah Khazem[3]

*[1]. PhD Student, Damascus University, Computer and networks engineering, samer.sulaiman@damascusuniversity.edu.sy

[2]. Assistant Professor, Dr, Damascus University. Networks and centers of data transformation and distribution wasim.alsamara@damascusuniversity.edu.sy

[3]. Dr, Eng, Lecturer, Damascus University, Remote measurement and driving, Raafah.Khazem@damascusuniversity.edu.sy

Received: 16/5/2023
Accepted: 21/6/2023

Abstract:

Methods for mitigating Denial of Service attacks have improved during the past years and these methods used several modern techniques for developing local protection mechanisms to help reduce the severity of these attacks and enhance network security in general. Despite the fact that using modern techniques reduced the negative effects of some types of attacks but standalone solutions might not result effective solutions, hence work must be done on developing cooperative solutions among several entities to reduce the effects of such attacks. This study includes the usage of a data structure that is exchanged between different network devices which includes attack-related information which is detected and broadcasted among all devices within a network as if it was a gossip, this implements a deterrent solution by isolating the whole network devices that are participating in DoS attacks even if they were not cooperating in fighting these attacks and this is done by exchanging the DoSGoS Data structure among different devices. Results has shown an improvement in reducing the effects of Denial-of-Service attacks by isolating the attackers whatever the type of attack used and within an acceptable time after the beginning of the attack.

Keywords: Denial of Service attacks, Network Security, Gossip.

المقدمة:

تعد هجمات الحرمان من الخدمة Denial of Service من أهم الأخطار الإلكترونية التي لاتزال تهدد شبكة الانترنت والشركات حول العالم لغاية يومنا هذا. تطورت هذه الهجمات عبر السنين وازدادت حدتها وخصوصًا عند حدوث هجمات الحرمان من الخدمة الموزّعة والتي يشارك فيها عدد كبير من المهاجمين وفي الكثير من الأحيان دون إدراكهم أنهم مشاركين في هذه الهجمة وذلك بعد تعرضهم لبرمجية خبيثة ما. أعلنت عدة شركات متخصصة في حماية المخدمات حول العالم تصديها لهجمات حرمان من الخدمة موزّعة غير مسبوقة خلال الفترة الماضية وقد كان آخرها في شهر أيلول من عام 2022 حيث تصدّت شركة Akamai العاملة في مجال التصدي لهجمات الحرمان من الخدمة لأكبر هجمة حرمان من الخدمة ضمن قارة أوروبا (Sparling, 2022) والتي وصل فيها معدل معطيات الهجوم Attack Rate إلى قرابة Mpps704.8 من ستة مواقع جغرافية مختلفة إضافة إلى وجود العديد من حالات سابقة سببت فيها هذه الهجمات انقطاع الانترنت عن دول بأكملها. تركز العديد من الأبحاث على كشف هجمات الحرمان من الخدمة وتوظيف آليات مناسبة من طرف الضحية للتصدي لهذه الهجمة ويكون هذا التصدي عن طريق الحفاظ على الخدمة للمستخدمين الشرعيين من جهة ومحاولة إبلاغ مزود خدمة الانترنت من أجل تتبع نقطة الهجوم واتخاذ فعل قانوني مناسب. تعد اليوم الطريقة الأكثر شيوعًا للتصدي لهذه الهجمات الاعتماد على شبكة إتاحة المحتوى Content Delivery Network (CDN) والتي تحاول تخفيف أثر الهجمة عن طريق التضحية بالموارد المتاحة لدى شركة الحماية وتعد هذه الطريقة مكلفة وعلى الرغم من نجاحها في الوقت الراهن إلا أنّ تزايد شدة وأعداد الهجمات قد تجعل من هذه الطريقة غير فعالة. لا يجب الاكتفاء بتطبيق آليات الحماية من طرف الضحية وإنما يمكن لمزودات الخدمة أن تلعب دورًا فعالًا في مكافحة هذه الهجمات، يجب تطوير طرائق من قبل مزود الخدمة لكبح انتشار هجمات الحرمان من الخدمة ويجب الأخذ بالاعتبار حالتين أساسيتين عند تطوير مثل هذه الطرق وهي تعاون جميع مزودات الخدمة في مواجهة الهجمة أو وجود بعض المزودات والتي لا توظف أية آليات لإيقاف مثل هذه الهجمات. يمكن عند وصول معلومة مناسبة لجميع التجهيزات المختصة بالحماية أن يتم اتخاذ الأفعال المناسبة لعزل المهاجم إما عن طريق عرقلة جميع الرزم الواردة من الجهة المشبوهة والتي تمر عن طريقها الهجمة أو عند انقضاء زمن كافٍ وعدم اتخاذ مزودات الخدمة المعنية أية تدابير لحد هذه الهجمة فيبقى لدى مزود الخدمة خيارًا وحيدًا وهو حظر الجهة غير المتعاونة فعندما يتم ذلك من قبل عدة مزودات خدمة فيصبح مزود الخدمة الذي مرر الهجمة مضطرًا لاتخاذ أفعال تصحيحية وإلا فسيصبح هو الخاسر الأكبر نتيجة تمريره للهجمة. يمكن التعبير عن هذه الطريقة على أنها طريقة رادعة deterrent method إذ يعرف الردع في مجال أمن المعلومات على أنه اتخاذ أفعال تسهم في جعل تكلفة الهجوم أكبر بكثير من الفائدة المرجوة منه وبالتالي عندما يُجبر مزود الخدمة على حظر المهاجمين فإن المهاجم سيضطر إلى محاولة الاتصال بمزودات خدمة إضافية وحجز عناوين منها وعندما يتم حظر أجزاء كبيرة منها فإن استمرار الهجوم دون تمكنه من حرمان الخدمة فعليًا يعد خسارة بشكل كامل بالنسبة للمهاجم ولهذا يمكن وصف مثل هذه الطريقة التي يتعاون فيها عدة مزودات خدمة للتصدي لهذه الهجمات على أنها طرق رادعة. نفرض وجود مزود خدمة يتيح خدمة ما سواء كانت موزّعة Distributed أو منفردة Standalone لمجموعة من المستخدمين u والذين ينفذون للخدمة بأوقات عشوائية. يريد مهاجم إرسال مجموعة من الطلبات الوهمية بشكل يجعل المخدم الذي يتيح الخدمة غير قادرًا على تقديم الخدمة لجميع المستخدمين. يمكن تصنيف المستخدمين إلى مستخدمين

شرعيين vu ومستخدمين غير شرعيين iu حيث يمكن أن يكون المستخدم غير الشرعي مستخدمًا تم خداعه للمشاركة في الهجمة عبر تثبيت برمجية خبيثة malware قام المهاجم بإعدادها على حاسبه بطريقة ما أو يكون هذا المستخدم عبارة عن حاسب أعدّه المهاجم ليبدو على أنه مستخدم طبيعي ويشارك في الهجمة المختارة بكامل موارده المتاحة. إذا كانت قدرة المخدمات C_s على إتاحة الخدمة فنعرف هجمة الحرمان من الخدمة بالشكل الرياضي التالي مع الأخذ بعين الاعتبار أن الخدمة منفردة وليست موزّعة وذلك للتبسيط:

$$C_s < \sum_{i=0}^{u} C_i$$

حيث أنّ C_i تمثل كلفة معالجة الطلبات القادمة من مستخدم واحد. يمكن تحديد الشرط اللازم لضمان فشل هجمة الحرمان من الخدمة مهما يكن شكلها بأنه:

$$C_s \gg \sum_{i=0}^{u} C_i$$

وبما أنه يمكن التمييز بين أنواع المستخدمين وفق التصنيف السابق يصبح الشرط السابق بالشكل

$$C_s \gg \sum_{i=0}^{vu} C_i + \sum_{j=0}^{iu} C_j$$

يعبر هذا الشرط عن حلّ مشكلة هجمة الحرمان من الخدمة عن طريق CDN عبر زيادة قدرة المخدمات على إتاحة الخدمة وبما أنّ عدد المستخدمين الشرعيين يتغير بشكل بسيط مع الزمن إلا في بعض الحالات الخاصة فيمكن الحفاظ على صحة الشرط السابق عبر تقليل قيمة الحد $\sum_{j=0}^{iu} C_j$ وعليه يمكن الاستعاضة عن زيادة قدرة المخدمات على تقديم الخدمة للمستخدمين. ليس من الضروري لحل المشكلة دومًا الوصول إلى المهاجم بشكل مباشر لإيقاف الهجمة وخصوصًا إذا استخدم المهاجم بعض الآليات للتخفي. تستطيع مختلف العقد في الشبكة أن تتفق فيما بينها على آلية تؤدي إلى عزل عقدة مهاجمة نرمز لها بالمحرف A وذلك عن طريق مخاطبة العقد الوسيطة والتي نرمز لها بالمحرف R حيث أنّ هذه العقد الوسيطة تمثل جميع الموجهات التي يمكن أن يمر بها تدفق المعطيات بين المهاجم والجهاز، ففي حال استجابت هذه العقد الوسيطة تبقى الشبكة كما هي ولا يوجد تعديلات أما في حال عدم تجاوبها فتقوم العقد أولًا بفرض كلفة إضافية على الاتصال بهذه العقد الوسيطة مما يعرقل عملها ويخفف بآن واحد من شدة الهجوم الواردة منها. وفي حال استمرار هذا الهجوم ومع استمرار عدم تعاون العقد الوسيطة فالحل النهائي هو حظر الطرقات إلى العقد الوسيطة للحفاظ على استقرار الشبكة.

الشكل(1) بنية شبكة اتصال بوجود مهاجم وعقدتين وسيطتين للهجوم.

2 . الدراسات المرجعية (Literature Review):

توجد العديد من الدراسات المرجعية التي درست هجمات الحرمان من الخدمة سواء من ناحية كشف الهجمة أو محاولة التصدي لها. نجد في (Sudip Misra، 2010) دراسة تتضمن إيجاد بروتوكول لكشف والوقاية من هجمات الحرمان من الخدمة في الشبكات اللاسلكية حيث يتم تعريف رسائل توجيهية على هيئة رزم تتضمن معلومات عن مقدرة المخدمات وفي حال تم كشف حدوث هجمة حرمان من الخدمة فإنه يتم إرسال عنوان المهاجم وتعميمه وتعديل جداول التوجيه لصد هذه الهجمة. أما في المقالة (Alaeddine Mihoub، 2022) فنجد طريقة مبتكرة تعتمد على تعلم الآلة من أجل كشف هجمة الحرمان من الخدمة ضمن شبكات انترنت الأشياء حيث يتم اعتماد مقاربتين لكشف الهجمة إحداهما هي المقاربة البسيطة والتي تعتمد على أفضل المزايا Features الموجودة ضمن مجموعة المعطيات Data Set المستخدمة في البحث المذكور وهي مجموعة المعطيات "IOT-BOT" وتختار عشرة مزايا منها وفقًا للدراسة المرجعية (Koroniotis N، 2019) والتي صممت قاعدة معطيات واقعية باستخدام بيئة اختبار testbed عملية. أما المقالة (Sreejesh N. G، 2022) فتقدم طريقة للحماية من هجمات الحرمان من الخدمة ضمن الشبكات المعرّفة برمجيًا Software Defined Networks والتي لا تعتمد على معلومات من الرزم التي تمر عبرها وإنما على ما

قام الجهاز الشبكي بتمريره أثناء عمله وتعرف هذه الطريقة حدًا Limit واحدًا للحكم على وجود هجوم من عدمه وعليه فإن الطريقة تسبب ظهور معدل خطأ كبير في بعض التصنيفات وهو معدل أشار إليه الباحثون باسم معدل الأخطاء الكاذبة False Positive rate والذي يحد من فعالية تطبيق مثل هذه الطريقة عمليًا. تبين الدراسة (Marta Catillo، 2022) إلى أنّه لا يوجد حل وحيد وفعال للتصدي لهجمات الحرمان من الخدمة حيث تقدم الدراسة نتائج تقييم مجتزأين Modules خاصين بالحماية ضمن مخدم ويب Apache وتخلص الدراسة إلى أنّ استخدام مجتزآت الحماية الجاهزة غير فعالة في التصدي للهجمات ويجب اعتماد وسائل أكثر فعالية للحماية وقياس هذه الفعالية بشكل دقيق. أما الدراسة (John Kafke, 2022) فتقدم طريقة للتخفيف من آثار هجمات الحرمان من الخدمة في أنظمة الاتصالات الصوتية عبر عناوين الانترنت VOIP عن طريق تبديل البروتوكولات بشكل ديناميكي عند اكتشاف الهجمات والاعتماد على زمن العطالة latency في كشف الهجمة حيث تم تقديم إطار عمل يدعى "Call me Maybe" والذي أظهر تحسنًا كبيرًا في أداء منظومة VOIP في حال التعرض لهجمة الحرمان من الخدمة.

3- الطريقة المقترحة (Proposed Method)

نجد إضافة إلى الدراسات المرجعية السابقة عددًا كبيرًا من الأبحاث التي تهتم بحل مشكلة الهجمات بشكل إفرادي ولكن قلّما نجد أبحاثًا في إيجاد بيئة متكاملة تحارب هذه الهجمات. لذا يجب إيجاد آلية تتيح للأجهزة الشبكية المختلفة سواء كانت موجهات أو حتى تجهيزات حماية شبكية أن تتخذ أفعالًا مناسبة عند التحسس لوجود هجمة حرمان من الخدمة وتحديدًا عندما تكون هذه الهجمة موزّعة. لا يركز البحث الحالي على كشف حدوث هجمة الحرمان من الخدمة فالكثير من الدراسات تضمنت مثل هذه الطرق وإنما يركّز البحث على نشر المعلومات الخاصة بالهجمات ضمن إطار زمني مناسب. تفيد مثل هذه الآلية في عملية التخفيف من أثر هجمة الحرمان من الخدمة وتحديدًا الهجمات من مستوى طبقة الشبكة Network Layer والتي يمكن معالجتها من قبل مزود خدمة الانترنت، أما الهجمات على مستوى طبقة التطبيقات والتي قد تتضمن بعض العمليات التي لا يستطيع مزود الخدمة فهمها أو التحكم بها فقد لا يكون التصرف بخصوصها من قبل مزود خدمة الانترنت حلًا سليمًا في جميع الحالات. تركز معظم الأبحاث السابقة على كشف هجمة الحرمان من الخدمة ومحاولة تجنب آثارها وتقتصر عمليات التصدي هذه على العمل ضمن النطاق المحلي أي لدى مكان استضافة الخدمة فقط باستثناء بعض الآليات التي تعتمد على تعقب عناوين IP. يمكن تصميم آلية تخاطب بين موجهات مزودات خدمة الانترنت للتنبيه إلى وجود هجمة الحرمان من الخدمة واتخاذ مجموعة من الأفعال تضمن حماية المستخدمين بالحد الأدنى كما يمكن تطوير بعض هذه الإجرائيات لتكون رادعة لبعض المشاركين في هذه الهجمات. يتحقق كل ما سبق عبر تبادل بنية معطيات مناسبة تضمن المعلومات المتعلقة بالهجوم من حيث مصدره والإطار الزمني الذي تم فيه. تجدر الإشارة إلى أنه يتم اعتماد مصطلح موجه الشبكة أو الجهاز الشبكي بشكل متداخل نظرًا للتداخل الفعلي بالوظائف بين بعض الأجهزة الشبكية والمقصود هو الجهاز الذي يتولى وظائف التوجيه والقادر على تنفيذ بعض الوظائف الإضافية المتعلّقة بالأمان. يبين الشكل (2) بنية المعطيات المقترحة والمسماة DoSGoS اختصارًا لمصطلح الوشاية الخاصة بهجمة الحرمان من الخدمة DoS Gossip والتي يمكن اعتمادها للتخاطب بين الموجهات للإخبار عن هجمة الحرمان من الخدمة وتتألف هذه البنية من الحقول التالية:

الشكل(2) بنية المعطيات DoSGoS

Status	Options	Denial of service attack type

Current Timestamp	
Attack Begin Timestamp	
Attack End Timestamp	
Attack source IP	Attack destination IP

يفيد حقل الحالة Status في تحديد حالة الرسالة التي يستقبلها أو يرسلها الموجه إذ أنه يجب تجنّب رسائل الإنذار المبالغ فيها فلا يجب استنفار آليات الحماية بأقصى أشكالها من أجل أية تحذير بسيط ولهذا فإن هذا الحقل يأخذ القيمة 0 عندما تكون الرسالة تهدف إلى التحذير ولا يطلب في هذه الحالة من جهاز الشبكة اتخاذ أفعال وإنما هي رسالة إخطار فقط. أو يأخذ القيمة 1 عندما تكون الرسالة إنذارًا فعليًا ويجب عندها على جهاز الشبكة التصرف. يتضمن حقل الخيارات Options بعض المعلومات المرتبطة بالحالة. أما الحقل نوع هجمة الحرمان من الخدمة فهو بطول 48 بت يمثل نوع هجمة الحرمان من الخدمة وفق جدول محدد يتم فيه التعبير عن كل نوع من أنواع الهجمات بقيمة ثابتة، نظرًا لأن عدد البتات كبير مقارنة بعدد الهجمات المعروفة اليوم فكان من الممكن إنشاء تمثيل للهجمات المختلفة حتى لو وردت معًا وهو ما يعرف باسم الهجمة متعددة الأشعة Multi-vector attack حيث يستخدم المهاجم نوعين أو أكثر من أنواع الهجمات إلا أن التصميم المقترح يفضّل إرسال بنية المعطيات مرة لكل هجوم وذلك للاستفادة منها في التحسين المستقبلي لتعلم الآلة ولحل أية مشاكل يمكن أن تظهر في حالة تعدد العناوين المستخدمة. تم استخدام ثلاث كلمات متتالية كل منها بطول 64 بت والتي تحدد بالترتيب الطابع الزمني الحالي Current Timestamp والطابع الزمني عند بداية الهجوم Attack Begin Timestamp والطابع الزمني عند نهاية الهجوم Attack End Timestamp ويفيد استخدام الطابع الزمني الحالي في ضمان عدم اتخاذ أفعال بناءً على معلومات قديمة إلا أنّ هذا الحقل له أهمية كبيرة من حيث تقييم الأداء الخاص بالطريقة المقترحة ومنظومات الحماية المستخدمة في مواجهة هجمات الحرمان من الخدمة. أما حقل الطابع الزمني عند نهاية الهجوم فيتم ضبطه إلى القيمة 0 للإشارة إلى أنّ الهجمة مازالت مستمرة. تم تخصيص 64 بت لكل طابع زمني وذلك للحصول على أدق قيمة ممكنة للحظة بدء ونهاية الهجوم لأن معظم هجمات الحرمان من الخدمة لا تستمر لفترة زمنية طويلة كما أوجدت الدراسة (Denial of Service: How Businesses evaluate the threat of DDoS Attacks، 2018). في النهاية يوجد حقلين مخصصين للعنوان الذي انطلق منه الهجوم وعنوان الضحية.

يمكن أن يتم تضمين هذه البنية ضمن البروتوكولات الأخرى حاليًا، إلا انه يمكن لاحقًا تطوير بروتوكول متكامل يتضمن عمليات المصادقة وعمليات الأمان المختلفة بحيث يمنع إساءة استخدام مثل هذه الرسائل في تنفيذ هجمات حرمان من الخدمة. عندما يستلم موجه بنية معطيات DoS GoS يبدأ بتنفيذ وظيفتين أساسيتين وهما:

1- تسجيلها ضمن السجل للاستفادة منها لاحقًا.

2- اتخاذ القرار.

أولًا: تسجيل الرسالة في السجل

يتم تسجيل بنية المعطيات في ملف سجل خاص ويتم تخزينه على الموجه ذاته أو إرساله إلى مخزن سجلات مركزي والاستفادة منه في عملية مراقبة الشبكة. كما أنّه من الممكن الاستفادة من تراكم المعلومات هذه في تعلم الآلة وذلك لتنفيذ آليات توقع لأوقات حدوث الهجمات أو في عملية التتبع العكسي للعناوين التي تنطلق منها الهجمات.

ثانيًا: اتخاذ القرار:

يجب أنْ يقوم الموجّه باتخاذ القرار المناسب وذلك بالاعتماد على عدد رسائل الإنذار التي وصلته والطابع الزمني الخاص بنهاية الهجوم وعليه تم تصميم خوارزمية اتخاذ قرار والتي نعبر عنها بواسطة الكود الزائف التالي:

Algorithm(1) DoS Gossip.

1. Initialize queue for DoSSnitch data
2. Initialize numberofthrottledata, numberofblockdata
3. OnReceive (DoSSnitch data) do
4. if dataTimestamp < RouterTimestamp – 1 days do
5. Log(DoSSnitch)
6. else do
7. Check internal queue for similar entries
8. if found do
9. if numberofactivematches == numberofblockdata
10. Block Routes to attacker
11. else if numberofactivematches == numberofthrottle-data
12. Throttle the route to attacker
13. end if
14. Set received flag and detected flag
15. else do
16. Set received flag and reset detected flag
17. end if
18. for counter=1 to DirectlyConnectedRoutersCount-1 do
19. Construct newDoSSnitch data
20. send newDoSSnitch data
21. Log(newDoSSnitch)
22. end for
23. end if

يعد اختيار القيمتين الخاصتين بالعتبتين numberofthrottledata و numberofblockdata ذات تأثير هام على استقرار الشبكة إذ تتحكم هذه القيم بسرعة حظر المهاجم ولكن بذات الوقت يجب الأخذ بعين الاعتبار أنّ اختيار قيمة صغيرة يسبب عرقلة الشبكة وحظرها بشكل متكرر كما أنّ استخدام قيمة كبيرة تسبب تأخيرًا في الوشاية عن هجمة الحرمان من الخدمة لذلك تم اعتماد القيمتين 5 و10 بالترتيب تجريبيًا.

4- الاختبار (Testing):

تم اختبار الطريقة المقترحة بشكل أولي بالاعتماد على الشبكة البسيطة الموضّحة في الشكل(3) حيث أن الشبكة المقترحة تحاكي الشبكات البسيطة الموجودة في العالم الحقيقي إذ أنه عادة ما يوجد حاسب واحد أو أكثر ومتصلين عبر مبدل واحد أو أكثر ومن ثم نجد الموجه الذي يتصل بموجهات مزودات خدمة الانترنت المختلفة. وقد تم الاعتماد في التجارب على محاكي الشبكة الشهير OMNET++ نظرًا لجودة أدائه وخصوصًا عند استخدام إطار العمل INET الذي تتم إضافته إليه. لاختبار الطريقة المقترحة قمنا بمحاكاة حدوث عدة هجمات حرمان من الخدمة وقمنا باعتماد مجموعة من طرق التقييم للطريقة المقترحة. بالعودة إلى الدراسة المرجعية نجد أن بعض التجارب المنفّذة في (Sudip Misra، 2010) تناسب طريقتنا المقترحة وهي تأثير نمو الشبكة وتحليل مستوى إهمال الرزم إلا أننا نقترح معيارًا هامًا وهو الزمن اللازم لعزل جزء الشبكة المنخرط في الهجمة.

الشكل (2) بنية الأختبار لاستخدام بنية المعطياتDosGos

1.4 الزمن اللازم لعزل جزء الهجمة

يتيح المحاكي OMNET++ تحكمًا كاملًا بالإطار الزمني للمحاكاة وعليه تم تحديد مواعيد بدء الهجمات وتحديد لحظة تشكيل الرزم والرسائل ضمنها بسهولة مما يتيح تحديد الزمن اللازم لعزل الهجمة. تم تعريف هذا الزمن على أنه فارق الزمن

بين لحظة إشـــعار الموجه بحدوث الهجمة ولحظة قيام آخر موجه بحظر الطرقات إلى الموجه المسؤول عن الهجمة.

تم تكرار المحاكاة عشر مرات وتم حساب الزمن الوسطي لعزل جزء الهجمة والذي بلغ عند تعيين زمن محاكاة 300 ثانية حوالي 34.5 ثانية. وقد تم اعتماد قيمة زمن المحاكاة كما في (Sudip Misra، 2010)

2.4 تأثير نمو الشبكة

يعد معيار التقييم هذا أمرًا هامًا والسبب في ذلك هو تجنب غمر الشبكة بالرسائل الخاصة بالوشاية. يمكن النظر لهذا المعيار بأنه عدد الرسائل اللازمة حتى عزل جزء الهجمة. بالاعتماد على دراسة أسوأ حالة وهي حالة وجود شبكة كاملة mesh network وكان عدد العقد في الشبكة n فإن كل موجه يرسل (n-2) رسالة وبالتالي إجمالي عدد الرسائل هو n(n-2) إذ أنّ الموجه لن يرسل الرسالة إلى نفسه أو إلى الموجه الذي أرسل له الرسالة. وعلى الرغم من أنّ هذا النوع من الشبكات هو الأصعب إلا أنّه لا يوجد بشكل عملي ولكن قمنا بدراستها لأنها تمثل أسوأ حالة ممكنة.

لا ينعكس عدد الرسائل الكبير بشكل سلبي فقط على الشبكة وإنما يؤثر على الزمن اللازم لعزل جزء الهجمة. وانطلاقًا من الشبكة السابقة قمنا بالتجربة بزيادة عدد الموجهات ويبين الشكل (4) العلاقة بين عدد العقد وعدد الرسائل المتبادلة ضمن الشبكة.

الشكل (3) العلاقة بين ازدياد عدد العقد وعدد الرسائل ضمن الشبكة.

الشكل(4) العلاقة بين ازدياد عدد العقد الزمن اللازم لعزل المهاجم.

من الواضح أنه يمكن تقريب العلاقة بين عدد الرسائل والعقد إلى علاقة تربيعية. ويبين الشكل(5) العلاقة بين ازدياد عدد العقد والزمن اللازم لعزل جزء الشبكة المشارك في الهجمات.

5- النتائج والمناقشة(Results & Discussion):

تحقق البنية المقترحة بالنسبة للشبكات البسيطة مثل المعتمدة في هذا البحث أداءً جيدًا وذلك بمعزل عن الهجوم المستخدم وذلك لأن هذه البنية تعمل ضمن طبقة مزودات الخدمة فهي معزولة عن المستخدمين النهائيين سواء كانوا مستخدمين طبيعيين أم مهاجمين وإن الزمن اللازم لتعميم حدوث الهجمة مقبول وبالعودة إلى المعايير الخاصة ببروتوكولات التطبيقات المستخدمة في الخدمات العامة مثل الاتصال الصوتي أو الفيديوي وغيرها، نجد أن هذا الزمن مقبول لعدم معرفة المستخدم بحدوث انقطاع في أي من خدماته وذلك مقارنة بالقيم المقترحة من معايير الاتصال المختلفة والتي تم جمعها في الدراسة (Jelena Mirkovic، 2006). يعد عدد الرسائل المتبادلة ضمن الشبكة كبيرًا وذلك بأخذ تحليل أسوأ حالة ممكنة ولكن تجدر الإشارة إلى أن الدراسة تقترح بنية رسالة معطيات ولا تقترح بنية رزمة شبكة وبالتالي يوجد العديد من الوسائل التي يمكن استخدامها لأمثلة عدد الرزم التي ستحوي هذه الرسائل وهذا من أهم الدوافع إلى عدم العمل على تطوير بروتوكول متكامل مثل الدراسة (Sudip Misra، 2010) إلا أنّ ذلك ليس مستحيلًا. بمقارنة البنية المقترحة مع مثيلتها فإن أبرز نقاط الاختلاف هي استخدام عتبتين للتحسس وذلك عند اتخاذ قرار يخص هجمة الحرمان من الخدمة مقارنة بعتبة واحدة في الدراسة المذكورة وأننا نقترح بنية معطيات وحيدة تتضمن جميع المعطيات اللازمة مقابل رزمتين في الدراسة المذكورة يمكن عند تطوير البنية المقترحة وتوسعتها لتصبح بروتوكولًا أن تتم عمليات المصادقة ضمن رزم خاصة مشفرة لتضمن عدم

استغلال معلومات البروتوكول المقترح في توليد آثار سلبية إلا أنّ المعلومات المضمنة في بنية المعطيات DoSGoS ليست خطيرة وعلى الرغم من ذلك يمكن أن يستغلها مهاجم في توقع الإجراء القادم من وسيلة الحماية وتعديل هجومه بشكل ديناميكي ولهذا يجب حمايته. كما أنّه يمكن إدخال الكثير من التعديلات على بنية المعطيات المقترحة وأمثلتها لتحقيق الفائدة منها. مقارنة مع الدراسات المرجعية التي تمت مناقشتها فإن الطريقة المقترحة لها العديد من المميزات وأهمها:

1- استخدام عتبتين للمقارنة عند اتخاذ القرار مما يساهم في تخفيف معدّل الأخطاء الكاذبة حيث لا يتم حظر الاتصال بالاعتماد على عتبة واحدة فقط.

2- لا تتضمن بنية المعطيات المقترحة معلومات يمكن استخدامها في شن هجمة بحد ذاتها.

3- تتم عملية الحظر وعزل موجّه ما يمرر رزم خاصة بالهجوم ضمن قرار جماعي وليس من جهة واحدة مما يشكل خطوة رادعة لانطلاق هجمات الحرمان من الخدمة من أي جهة كانت.

4- تعمل الطريقة المقترحة ضمن الشبكات التقليدية وضمن أي شبكة لا تفرض قيودًا على حجوم تبادل المعطيات إذ أنّ البنية المقترحة تتضمن بعض الحقول كبيرة الحجم نسبيًا والتي قد لا تكون مناسبة في بعض أنواع الشبكات الخاصة.

توجد العديد من التحسينات التي يمكن إضافتها في المستقبل ومنها تقليل حجم بنية المعطيات دون فقدان المعلومات الخاصة بالطابع الزمني. كما يمكن العمل على تقليل عدد الرسائل المتبادلة من أجل كشف هجمة الحرمان من الخدمة.

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

References:

[1] Alaeddine Mihoub, O. B. (2022). Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Computers and Electrical Engineering.

[2] (2018). Denial of Service: How Businesses evaluate the threat of DDoS Attacks. Kaspersky Lab.

[3] Jelena Mirkovic, P. R. (2006). Measuring denial Of service. 2nd ACM workshop on Quality of protection (pp. 53-58). ACM.

[4] John Kafke, T. V. (2022, 10 18). Call Me Maybe: Using Dynamic Protocol Switching to Mitigate Denial-of-Service Attacks on VoIP Systems. Network, pp. 545-567.

[5] Koroniotis N, M. N. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: bot-IoT dataset. Future Generation Computer Systems, pp. 779-796.

[6] Marta Catillo, A. P. (2022, 2 16). No More DoS? An Empirical Study on Defense Techniques for WebServer Denial of Service Mitigation. Journal of Network and Computer Applications.

[7] Sparling, C. (2022, 9 15). Record-Breaking DDoS Attack in Europe. Retrieved 10 21, 2022, fromakamai://www.akamai.com/blog/security/record-breaking-ddos-attack-in-europe

[8] Sreejesh N. G, S. M. (2022). DoSMit: A Novel Way for the Mitigation of Denial of Service Attacks in Software Defined Networking. International Journal for Research in Applied Science & Engineering Technology (IJRASET).

[9]Sudip Misra, P. V. (2010). An adaptive learning routing protocol for the prevention of distributed denial of service attacks in wireless mesh networks. Computers and Mathematics with Applications, pp. 294-306.