Study and Analysis of the Impact of Man-in-the-Middle (MITM) Attacks on the Software-Defined Network

Dr. Mohammed Sobih *
Abeer Hasan **

(Received 18 / 11 / 2021. Accepted 12 / 6 / 2022)

□ ABSTRACT □

Software Defined Networks SDN is a new technology in managing computer networks, and it is the most studied topic in recent years, as it has provided many features and contributed to solving many problems experienced by traditional networks. However, what has not changed is the need to understand the network topology and stay informed about how network elements perform across the topology. This factor continues to be a key factor in achieving performance and security goals.

The SDN architecture offers a lot of advantages to the networking field, but its weaknesses mostly lie in the lack of security. However, it provides support for security solutions, an area that is currently being explored by many researchers, and this is what made the study of the security aspect by achieving the man-in-the-middle attack in several forms and studying its impact on the network and studying security solutions and proposing a new structure that specializes in detecting and repelling these attacks . Therefore, in this paper, we will study the security issues of a number of widely used controllers specifically regarding man-in-the-middle attacks, and we will study the most important attack detection and blocking algorithms.

Keywords : Controller, Software Defined Networks, (Man-in-the-Middle) MITM, ARP spoofing, TCP-attack, SSL-attack.

* **Associate Professor, Department of Networks and Operating Systems. Faculty of Information Technology, Tishreen University, Lattakia, Syria.** msobeihy@gmail.com.

** **Postgraduate Student (MSc), Department of Networks and Opeating Systems. Faculty of Information Technology, Tishreen University, Lattakia, Syria.** Eng.abeer.a.hassan@gmail.com.

دراسة وتحليل أثر هجمات الرجل في المنتصف (MITM) على الشبكة المعرّفة بالبرمجيات

د. محمد صبيح*

عبير حسن**

(تاريخ الإيداع 18 / 11 / 2021. قُبِل للنشر في 12/ 6 / 2022)

□ ملخّص □

الشَّبكات المعرَّفة بالبرمجيات SDN (Software Defined Network) هي تقنية جديد في إدارة شبكات الحاسب، وهي من أكثر المواضيع دراسةً في السنوات الأخيرة، فقد قدَّمت العديد من الميزات وساهمت في حل العديد من المشاكل التي عانت منها الشبكات التقليدية. ومع ذلك، فإن الذي لم يتغير هو الحاجة إلى فهم طوبولوجيا الشبكة والبقاء على اطلاع حول كيفية أداء عناصر الشبكة عبر الطوبولوجيا. ولا يزال هذا العامل عاملاً رئيسياً في تحقيق أهداف الأداء والأمن.

تقدم بنية SDN الكثير من المزايا لمجال الشبكات، ولكن نقاط ضعفها تكمن في الغالب في نقص الأمن. ومع ذلك، فإنها تقدم الدعم للحلول الأمنية، وهو مجال يجري استكشافه حالياً من قبل العديد من الباحثين، وهذا ما جعل دراسة الجانب الأمني من خلال تحقيق هجمة الرجل في المنتصف بعدة أشكال ودراسة أثرها على الشبكة ودراسة الحلول الأمنية واقتراح بنية جديدة تتخصص بكشف هذه الهجمات وصدها، لها أهمية كبيرة. لذلك سنقوم في هذه البحث بدراسة القضايا الأمنية لعدد من المتحكمات المستخدمة على نطاق واسع بما يخص هجمات الرجل في المنتصف على وجه التحديد كما سنقوم بدراسة أهم خوارزميات كشف الهجوم وصدّه.

الكلمات المفتاحية: المتحكم، الشبكات المعرفة بالبرمجيات،MITM (Man–in–the–Middle)، ARP spoofing، SSL– attack ،TCP– attack

* أستاذ مساعد –قسم النظم والشبكات الحاسوبية –كلية الهندسة المعلوماتية– جامعة تشرين –اللاذقية – سورية.msobeihy@gmail.com

** طالب دراسات عليا (ماجستير)– قسم النظم والشبكات الحاسوبية –كلية الهندسة المعلوماتية–جامعة تشرين –اللاذقية –سورية. Eng.abeer.a.hassan@gmail.com

مقدمة:

مع أي تقنية جديدة، ستكون هناك مخاطر سواء كانت هذه التكنولوجيا الجديدة تزدهر أم لا. وفي عالم شبكات الكمبيوتر، يمكن تضخيم هذه المخاطر بسبب طبيعة البيئة. فلا يمكن للشبكات التي نبنيها أن تكون سريعة أو محسّنة فقط، بل يجب أن تكون آمنة أيضًا. منذ بداية تطوير SDN، كان التركيز الأساسي للأبحاث على فصل مستوى التحكم عن مستوى البيانات عن طريق الحفاظ على الأداء والمرونة التشغيلية دون تغيير، بينما الجوانب الأمنية لشبكة SDN بقيت من الجوانب الغير مدروسة لهذه التقنية. على الرغم من أن فصل مستوى التحكم عن مستوى البيانات يعد خطوة كبيرة نحو تبسيط إدارة الشبكة، فإنه يخضع الشبكة إلى هدف محتمل للمتسللين للوصول إلى السيطرة عليها. نظرًا للتصميم المركزي لشبكات SDN، فإن أمن وحدة التحكم قد يؤدي إلى تعريض أمن شبكة كاملة للخطر. الشركات التي تتحرك نحو تكييف SDN تشعر بالقلق إزاء القضايا الأمنية والمشاكل الناجمة عنها. لذلك سنقوم في هذه البحث بدراسة القضايا الأمنية لعدد من المتحكمات المستخدمة على نطاق واسع بما يخص هجمات MITM –Man–in–the (Middle) الرجل في المنتصف على وجه التحديد. حيث تعد هذه الهجمات من أخطر التهديدات الأمنية التي تستهدف أي نوع من الشبكات، ولا سيما الشبكات المعرفة بالبرمجيات التي تتميز بمركزية التحكم، الأمر الذي يجعلها هدفاً لهذا النوع من الهجمات وعواقب الهجوم تكون ببساطة مدمرة.

أهمية البحث وأهدافه:

اعتماد الشركات والمؤسسات على الشبكات المعرفة بالبرمجيات يترتب عليه الكثير من التحديات. حيث تتشابه التحديات الأمنية في شبكات SDN تماماً مع الشبكات التقليدية حيث تحدث العديد من الهجمات في طبقة التحكم. وتتصاعد هذه المشكلة من خلال حقيقة أن المعلومات متزامنة بين طبقة البيانات، التي تضم أجهزة الشبكة؛ وطبقة التحكم، التي تعمل فيها وحدة تحكم SDN. تحتوي طبقة التحكم على سياسات لتشغيل طبقة البيانات، مما يوفر نقطة واحدة للفشل على الشبكة ككل، ومع زيادة الاعتماد على شبكات SDN كبنية في العديد من الشبكات ومنها انترنيت الأشياء، أصبحت المشكلات الأمنية أكثر أهمية ويجب تسليط الضوء عليها أكثر.

يعتبر هجوم MITM الذي يستهدف وحدة تحكم SDN هو إحدى القضايا التي قد تتسبب في حدوث مشكلات خطيرة بالنسبة إلى تطوير شبكات SDN. في الواقع، كانت هناك محاولات ناجحة في تنفيذ مثل هذا الهجوم ومما قد يتسبب بنتائج مدمّرة: مثلاً سيكون المهاجم قادراً على تشفير بيانات اعتماد تسجيل الدخول إلى إمكانية السيطرة الكاملة على الشبكة بالكامل.

لذلك تكمن أهمية البحث، في ضرورة دراسة هذا النوع من الهجمات ومعرفة الأساليب المستخدمة للقيام بكشفها وصدها. يهدف البحث إلى تنفيذ عدة أنواع من هجوم MITM على شبكة SDN وكشفها وصده وتحسين خوارزمية كشف الهجوم ودراسة مدى تأثيره على أداء الشبكة على اختلاف الطبولوجيا المستخدمة.

1- الدراسات المرجعية:

نتيجة التطورات الكبيرة في الشبكات اللاسلكية واعتمادها على تقنية إنترنت الأشياء مع شبكات الجيل الخامس ومابعدها، والتي ستعتمد بشكل أساسي على الشبكات المعرفة بالبرمجيات (SDN) لتحقيق جودة الخدمة الموعودة. كان لا بدّا من التركيز على إيجاد حلول أمنية ذكية قائمة على SDN والتي تتحقق في الزمن الحقيقي، وكشف التسلل

والتخفيف من حدته بالاعتماد على التعلم الآلي. درس [1]، باقتراح حلاً لاكتشاف التسلل وتخفيفه في الزمن الحقيقي لـ SDN، النهج المقترح مبني على استخراج ميزة التدفق الآلي وتصنيف التدفقات من خلال استخدام مصنفات الغابات العشوائية (random forest classifiers) في طبقة تطبيق SDN. وقدمو نتائج حول دقة اكتشاف التسلل بالإضافة إلى نتائج الأداء في وجود وغياب آلية الأمن المقترحة.

وفي [2] تمت نمذجة الهجوم MITM وتنفيذه في SDN باستخدام المحاكي Mininet حيث ناقش الباحثون محور الكشف عن آليات الهجوم على MITM، ونفّذ هجوم الرجل في المنتصف باستخدام تقنية ARP Flooding في Mininet وذلك بغض النظر عن وحدة التحكم المستخدمة.

وقام الباحثون في [3] بدراسة المتحكم OpenDayLight حيث استخدمت الأداة ettercap من أجل تنفيذ هجوم MITM على وحدة تحكم، والتقاط حركة المرور ومحاولة الحصول على بيانات تسجيل الدخول إلى واجهة الويب DLUX. كان الهدف من هذا السيناريو هو التقاط حركة المرور، وبالتالي إمكانية السيطرة على المتحكم. ولكن لم يتم استخدام ألية للكشف عن الهجوم ودراسة أثره على المتحكم ODL.

قام الباحثون في [4] بإنشاء مصفوفة تهديد فردية من STRIDE لتلخيص نشاط كل متحكم ضد فئات الهجوم المعروفة. يعتبر "STRIDE" بحد ذاته اختصارًا لستة فئات تهديد، مثل: الانتحال، والتلاعب، والنبذ، وكشف المعلومات، وحجب الخدمة (DoS)، ورفع الامتيازات. تمت المقارنة بين مصفوفات التهديدات الناتجة للمتحكمات واستعراض جدول للتهديدات التي تتعرض لها المتحكمات وأسبابها.

وظهرت الدراسة [5] لمحاكاة هجوم ARP spoofing ضد المتحكم. بمجرد بدء الهجوم MITM، تفقد وحدة تحكم ONOS اتصالها. بعدها أنشئت المصادقة للنظام البعيد للوصول إلى ONOS GUI، أي أضيف مستخدم جديد عبر المهاجم .

في [6] يعتقد الكثيرون أن مستقبل إنترنت الأشياء سيعتمد على SDN. ولكن تبقى المشكلات الأمنية لا مهرب منها ركزوا بشكل رئيسي في هذا البحث على القضايا الأمنية لقنوات البرتوكول OpenFlow ، وخاصة هجمات MITM. اقترحوا أيضاً إجراء مضاد للكشف عن هجمات MITM عن طريق الاستفادة من مرشح Bloom حيث قاموا بتطبيق نظام نموذجي للكشف عن تعديل الحزمة مع مرشحات Bloom القائمة على SDN وتوسيع بروتوكول OpenFlow. استخدم الباحثون Floodlight كوحدة تحكم SDN مفتوحة المصدر، واستخدموا المحاكي Mininet لمحاكاة الشبكة. قاموا بتقييم أداء طريقة مرشح Bloom من حيث الزمن المستغرق لاكتشاف الهجوم والتأخير. بعد ذلك، اختبروا دقة هذه الطريقة.

وفي [7] اقترح الباحثون آلية مقنعة للكشف عن هجوم الرجل في المنتصف في شبكات SDN تسمى (Convincing Mechanism for MITM Detection) CMD. إلى جانب ذلك، يمكن لـ CMD تقديم تفاصيل عن موقع المهاجم من أجل إيقاف الهجوم من المصدر. يتم استخدام ميزات مثل التحكم المركزي وقدرات واجهة مفتوحة من SDN بواسطة CMD للكشف عن هجمات MITM.

قاموا بتقييم أداء خوارزمية CMD في الكشف عن الهجوم حيث استخدام الـ Floodlight كوحدة تحكم SDN. استُخدام الجهاز OpenvSwitch و KVM لبناء عملية الهجوم MITM في بيئة SDN. نظام التشغيل للمهاجم هو kali، واستخدموا Ettercap لتشغيل هجمات MITM. نظام تشغيل الضحايا هو Ubuntu 16.04. قاموا بتنفيذ الهجوم ولكن لم يتم استخدام ألية للكشف عن الهجوم ودراسة أثره على الشبكة.

و في البحثين [9] و[10] قام الباحثون بدراسة الخوارزميتين:

NetWatch (Network Watch) , ARP-Packet Analysis للكشف عن الهجوم وصده وتقييم أداء إنتاجية الشبكة أثناء إجراء اتصال TCP قبل الهجوم وخلاله وبعد كشفه وصده من قبل الخوارزمية.

وفي الدراسات [13] ,[11],[12] تمت دراسة البرتوكول الأساسي OpenFlow الذي تعمل به الشبكات المعرفة بالبرمجيات ومراقبة الرسائل المتبادلة في الشبكة في حالتها الطبيعة الآمنة، وكلك قيّم أداء المتحكمات في الشبكة وذلك دون تطبيق هجوم.

طرائق البحث ومواده:

اتُبعت المنهجية الآتية:

1 دراسة نظرية تناولت مايلي:

التعريف بالشبكات المعرفة بالبرمجيات و تسليط الضوء على الثغرات الأمنية فيها.

التعريف بأشهر الهجمات التي تتعرض لها الشبكات المعرفة بالبرمجيات والتركيز على دراسة أهم أنواع هجمات الرجل في المنتصف التي قد تهدد الشبكة.

2- الدراسة العملية:

المحاكي المستخدم:

استُخدام المحاكي Mininet لبناء طوبولوجيا الشبكة وتنفيذ السيناريوهات. و استخدام أداة توليد الهجوم وهي ettercap والأداة Gnuplot لرسم النتائج.

السيناريوهات المدروسة:

في البداية تنفيذ هجوم Man-in-the-Middle على شبكة SDN بعدة أنواع له وهي ,ARP spoofing TCP- attack, SSH-attack والمقارنة بين الأنواع الثلاثة من حيث التأثير على الشبكة. وتجدر الإشارة إلى أن الهجوم SSH-attack هو الأخطر كونه حصل على بيانات مشفرة وقد فُك تشفيرها والحصول على كلمة السر واسم المستخدم.

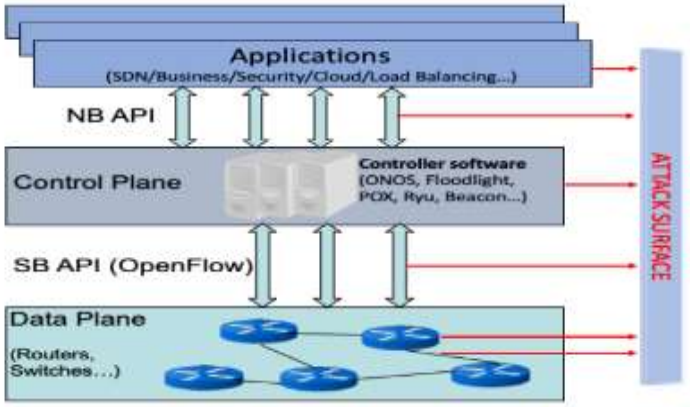
والعمل على دراسة خوارزميات لكشف الهجوم وصده وتقييم أداء هذه الخوارزميات كما تم اقتراح تحسين لهذه الخوارزميات.

الدراسة النظرية:

1 الشبكات المعرفة بالبرمجيات SDN:

هي اختصار لـ (Software Defined Networking) وفقاً للتعريف الرسمي من Open Networking Foundation، فإن " الشبكات المعرفة بالبرمجيات (SDN) هي بنية شبكة ناشئة يتم فيها فصل التحكم في الشبكة عن إعادة التوجيه ويمكن برمجته بشكل مباشر. هذا التحكم، كان مرتبطاً سابقاً بإحكام في أجهزة الشبكة الفردية، التي يمكن الوصول إليها. تمكّن التقنية الأجهزة من تجريد البنية التحتية الأساسية للتطبيقات وخدمات الشبكة، والتي يمكن أن تعامل الشبكة ككيان منطقي أو افتراضي. "

في الشبكات التقليدية، تكون عمليتي تمرير البيانات و تقرير وجهة البيانات (التوجيه) متضمنتان ضمن نفس الجهاز وهذا ما جعلها تبدو معقدة .أما في الشبكات المعرفة بالبرميجيات تم فصل مستوى البيانات Data plane عن مستوى التحكم control plane في أجهزة الشبكة، ليصبح دور هذه الأجهزة مقتصراً على تمرير البيانات، أما الإدارة والتحكم ستصبح في طبقات جديدة كما هو موضح في الشكل (5-1) بنية شبكات الـ SDN [12] :



الشكل (5-1) بنية شبكات ال sdn

2 المتحكمات controllers [10]:

يعتبر المتحكم عقل الـ SDN لأننا جمعنا فيه وظيفة control plane المسؤولة عن الخدمات والتطبيقات المطلوبة والتي تم برمجتها من قبل مهندس الشبكات بواسطة API لتنتقل بشكل إعدادات إلى أجهزة الشبكة الأخرى. ومن أهم أنواع هذه المتحكمات: NOX [13]، Floodlight [15]، Ryu [14] .

يتواصل المتحكم controller مع باقي أجهزة الشبكة التي نُزعت منها وظيفة التحكم لينقل لها الخدمات والتطبيقات، وذلك باستخدام لغة مشتركة بينهما تسمى البروتوكول openflow .

3 الثغرات الأمنية في شبكة SDN :

نظرًا للتصميم المركزي لشبكات SDN، فإن أمن وحدة التحكم قد يؤدي إلى تعريض أمن شبكة كاملة للخطر. الشركات التي تتحرك نحو تقنية الـ SDN تشعر بالقلق إزاء القضايا الأمنية.

ومن مشكلات الأمان في شبكات SDN تعرضها لهجمات مثل DDOS و MITM.

3-1 هجمات MITM:

تحدث MITM بسهولة في شبكات SDN بسبب عدم وجود مصادقة في حزم OpenFlow التي تتدفق عبر المبدل. إذا كان المهاجم يتنصت على جزء الشبكة الموجود بين وحدة التحكم والمبدل، فيمكن للمهاجم إجراء حركة مرور مكررة إلى مضيفه وتفريغ التدفقات في شبكات SDN مع القواعد للسيطرة على المبدلات والتقاط حركة المرور المتدفقة من خلالها. وقد يطلق هؤلاء مهاجمين آخرين لمهاجمة شبكات SDN. سيؤثر ذلك على أداء ومصداقية شبكات SDN.

من أنواعه ARP spoofing و TCP- attack, SSL- attack .

لماذا يعتبر هجوم "الرجل في المنتصف" خطراً ؟ وماذا يمكن للمهاجم أن يفعله في حال إتمام الهجوم بنجاح؟

أ- **سرقة ملفات الـ "cookies"**

باختصار، يحتوي ملف الـ "cookies" على بيانات المستخدم حين يسجل دخوله إلى حساب على الإنترنت، لإبقاء الجلسة الحالية مفتوحة عندما يتنقّل بين صفحات الموقع. تشفّر هذه البيانات بمفتاح يتم توليده عشوائياً ويخزّن في قاعدة بيانات الموقع. وعند تطابق المفتاح الموجود في قاعدة البيانات والمفتاح الموجود في ملف الـ "cookies" يتم التعرف على المستخدم.

توجد مشكلة تتعلق بملفات الـ "cookies" وهي أن العديد من المواقع تستخدم برتوكول SSL للتشفير على صفحة تسجيل الدخول فقط، فيما بقيّة صفحات الموقع تستخدم بروتوكول HTTP نتيجة ذلك، سيكون ملف الـ "cookies"غير

مشفر، وبالتالي سيستطيع المهاجم عند حصوله على هذا الملف ونسخه إلى جهازه، الدخول إلى حسابكم دون الحاجة إلى إدخال أية بيانات.

ب- **هجوم (SSL-Strip)** (Secure Sockets Layer):

يسود اعتقاد بأن اللجوء إلى بروتوكول SSL وحده في المواقع التي تدعمه كفيل بتأمين الحماية، ولكن وجود هجوم MITMأثبت عكس ذلك، حيث يمكن للمهاجم أن يتحكم بالطلبات التي يتم تُرسل عبر بروتوكول SSL وفك تشفيرها، مما يجعل كافة كلمات السر والبيانات التي نرسلها مكشوفة له.

ت- **اختراق نظام أسماء النطاقات (DNS)**

يعمل نظام أسماء النطاقات على النحو التالي:

عندما نكتب اسم موقع (على سبيل المثال: google.com) في المتصفح، يتواصل الحاسب مع مخدّم يسمى "مخدّم نظام أسماء النطاقات" (DNS) لسؤاله عن عنوان الموقع الذي طلبناها. ولأن الحاسب لا يعرف ماذا تعني عبارة "google.com" أو أين يجد الموقع، تأتي مهمّة مخدّم نظام أسماء النطاقات في ربط عنوان الموقع المطلوب مع رقم الـ IP الخاص به.

على سبيل المثال، في حال طلبنا الموقع Facebook.com بإمكان المهاجم تحويلنا إلى موقع مليء بالملفات الخبيثة. يمكنه أيضاً تحويلنا إلى صفحة مزورة شبيهة تماماً بموقع Facebook ولكن تحت سيطرته، لسرقة بيانات دخولنا إلى حسابنا على Facebook وهذه العملية الأخيرة تسمّى بالتصيّد (Phishing) .

ث- **الحقن الخبيث للرمز البرمجي (Code Injection)**

بإمكان منفّذ هجوم "MITM" تغيير المحتوى الذي نفتحه عبر الانترنت، عبر إضافة رمز برمجي خبيث إلى لعبة أو برنامج نقوم بتحميلها ، أو حتى صفحة نزورها، وهذا يضعنا أمام احتمالات عديدة يستطيع المهاجم القيام بها، ولعلّ أهمها هو اختراق جهازنا والسيطرة التامة عليه، أو سرقة حساباتنا.

4 بروتوكول ARP (Address resolution protocol):

هو بروتوكول يستخدم من قبل الأجهزة الموجودة في شبكة الـ SDN لربط عناوين الـ IP بالـ AC Address الخاص بكل جهاز أي أنه يقوم بعملية تحديد العنوان الفيزيائي (MAC Address) لـ IP معلوم عندنا مما يمكن هذه الأجهزة من الإتصال ببعضها و تناقل المعلومات بينها.ويتم الاحتفاظ بهذا الربط بجدول ضمن الذاكرة المخبئية.

5-4-1هجوم تزييف **ARP spoofing ARP**:

في هذا الهجوم، يقوم المهاجم بإرسال رسائل بروتوكول تحليل عنوان (ARP) وهمية عبر شبكة محلية، ويتم ذلك عندما يربط المهاجم عنوان MAC الضار بعنوان IP الخاص بخادم المستخدم وجهاز الحاسب على الشبكة. بمجرد الاتصال، يبدأ المهاجم تلقائيًا في تلقي البيانات التي تدخل وتخرج من عنوان IP المحدد. حيث أنه يمنح المهاجمين إمكانية تغيير أو اعتراض البيانات العابرة. يتم تحديث ذاكرة التخزين المؤقت لـ ARP، وبالتالي يواصل الحاسب والموجه الاتصال بالمهاجم. يرى المضيفون الآخرون إدخالات ذاكرة التخزين المؤقت ARP المخادعة ممايجعلهم ينتقلون البيانات إلى المهاجم.

هجوم ARP spoofing هو الأكثر شيوعًا في شبكات المناطق المحلية التي تنفذ بروتوكول تحليل العنوان كما هو موضح في الشكل (5-2). يستخدم المهاجم أداة انتحال ، مثل Driftnet أو ettercap وبعد تنفيذ الهجوم يصبح المهاجم قادراً على تغيير أو اعتراض البيانات المرسلة بين الطرفين.

الشكل (5-2) هجوم تزييفARP ARP spoofing attack [1]

2-4 المخاطر الناتجة عن هجوم ARP spoofing:

بمجرد أن ينجح المهاجم في تنفيذ هجوم تزييف ARP، فإنه يكون قادراً على الانتقال بسهولة إلى التنفيذ:

1. **هجمات DDoS** بدلاً من عنوان MAC الخاص به، يمكن للمهاجم استخدام عنوان الخادم الذي يرغب في مهاجمته من أجل تنفيذ هجوم DDoS. من خلال تكرار هذا لعدد كبير من عناوين IP، ستغرق الضحية بحركة المرور.
2. **Session hijacking** اختطاف الجلسة – يمكن للمهاجم الحصول على معرف الجلسة الخاص بك عبر تزييف ARP ثم استخدامه للوصول إلى الحسابات التي تم تسجيل دخول الضحية إليها.
3. **Continued packet theft** سرقة الرزم المستمرة أي سرقة الرزم وبياناتك الخاصة.
4. **Altering communications** تغيير الاتصالات – وهو مايسمى MITM هجوم رجل في المنتصف.

5 الخوارزميات المستخدمة لاكتشاف الهجوم وصده في الشبكات المعرفة بالبرمجيات:

5-1 الخوارزمية ARP-Packet Analysis [9]:

تقوم هذه الخوارزمية بمراقبة الرزم على المنفذ لاكتشاف قدوم رسائل من عنوان IP ليس موجوداً في الجدول. ومراقبة عدد حزم ARP على المنفذ، لاكتشاف التدفق الكبير للحزم الضارة وإيقافها عبر قواعد البرتوكول Openflow وتجنب الحمل الزائد على وحدة التحكم عبر إسقاط الحزم القادمة نحو وحدة التحكم ، في حالة محاولة المهاجم إسقاط وحدة التحكم.

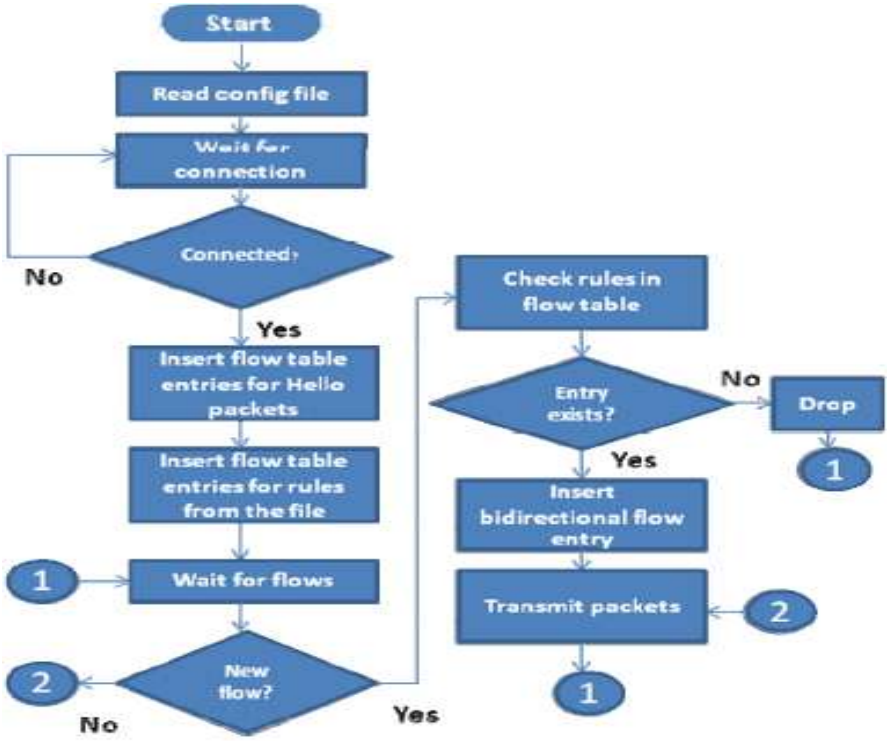
5-1-1 مبدأ عمل الخوارزمية:

1. يبني المتحكم جدول لتعيين العناوين الموجودة في الشبكة وربطها إلى المنافذ.
2. يملأ المتحكم الجدول من خلال مراقبة حركة المرور.
3. عندما يريد المتحكم إعادة توجيه حركة المرور، فإنه يبحث عن المسار في الجدول. إذا كان المنفذ غير موجود، يرسل الرسالة إلى جميع المنافذ باستثناء المنفذ الذي جاءت منه. أما إذا كان المنفذ موجود يتم إرسال الرسالة إلى الوجهة المطلوبة.
4. إذا كان عنوان الوجهة هو عنوان مسار تمت تصفيته (أي كشفه أنه من مهاجم) يتم إسقاط الحزمة. حيث تعتمد الخوارزمية على عدد الرزم الكبير القادمة من المهاجم للكشف عن الهجوم.

5-2 الخوارزمية NetWatch:

نظراً لكون بنية الشبكات المعرفة بالبرمجيات توفر إمكانية جمع الإحصائيات من الشبكة وبرمجة أجهزة إعادة التوجيه المتصلة بالشبكة. NetWatch تعتمد على الجمع الدوري لإحصائيات التدفق من المبدلات المتصلة من خلال رسائل OpenFlow Control المتبادلة، والتي يتم تحليلها لاحتمال حدوث هجوم من قبل مضيف مهاجم. وتعتبر هذه

الخوارزمية تطوير لنموزج جدار حماية حيث يحتاج تنفيذها إلى ملف قواعد يتم تضمينه ضمن المتحكم. يوضح الشكل (3-5) مبدأ عمل الخوارزمية NetWatch [10] :



الشكل (5-3) مبدأ عمل الخوارزمية NetWatch

5-2-1 مبدأ عمل الخوارزمية:

1. عند تنفيذ التطبيق من قبل المتحكم يقوم بجمع المعلومات من الشبكة من خلال رسائل OpenFlow Control المتبادلة. ثم يقرأ ملف القواعد الذي تم إنشاؤه ووضعه ضمن المتحكم وتُثبت إدخالات جدول التدفق في المبدلات بناءً على القواعد المحددة.
2. يوجه المبدلات المتصلة لإرسال رزم ARP إلى وحدة التحكم وذلك للحصول على التعيين بين عناوين IP وعناوين MAC للمضيفين.
3. بعد جمع معلومات السابقة، يلغي التطبيق التعليمات السابقة التي تتضمن إرسال رزم ARP إلى وحدة التحكم ويركز التطبيق على إحصائيات التدفق. هذا يساعد في تجنب الاختناق المروري على مستوى وحدة التحكم.
4. يعيد التطبيق إصدار تعليمات إعادة توجيه الرزم إلى وحدة التحكم فقط في حالة ملاحظة قدر غير عادي من حركة حزم ARP. هنا يستخدم المتحكم المعلومات التي جمعها في المرحلة الأولى لتحديد عدم التطابق ثم يثبيت إدخال في المبدلات لإسقاط رزم ARP المزيفة لفترة زمنية محددة من قبل التطبيق ويصدر تنبيهاً بعنوان المهاجم ليتم إزالته من الشبكة.

نظرًا لأنه لا يمكن تحديد ما إذا كان المهاجم قد تم إزالته ديناميكيًا ، تعمل NetWatch على افتراض أنه سيتم حظر المضيف الضار خلال مدة معينة بمجرد إصدار التنبيه.

5-3 الخوارزمية المقترحة:

هذه الخوارزمية عبارة عن تحسين للخوارزمية NetWatch بصرف النظر عن إصدار التنبيه وحظر المهاجم، التحسين الذي اقترحته أنه إعادة الرابط التالف بين الضحية والأجهزة الأخرى حتى لا يؤثر ذلك على عمل الشبكة بحيث لاتتوقف الشبكة عن العمل. عند تنفيذ التطبيق من قبل المتحكم يقوم بجمع المعلومات من الشبكة وبناء قاعدة البيانات و الحصول على التعيين بين عناوين IP وعناوين MAC للمضيفين كما في خوارزمية NetWatch ويعيد التطبيق إصدار تعليمات إعادة توجيه الرزم إلى وحدة التحكم فقط في حالة ملاحظة قدر غير عادي من حركة حزم ARP. وفي هذا الجزء اقترحت تعديلات لتحسين عمل الخوارزمية.

5-3-1 آلية عمل التحسين المقترح :

يستخدم التطبيق المعلومات التي تم جمعها في المرحلة الأولى:

1. لتحديد عدم التطابق ويصدر تنبيهًا.
2. إلى جانب التنبيه ، يتم إضافة إدخال إلى جداول تدفق المبدلات لإسقاط جميع الحزم من المهاجم.
3. يقوم التطبيق بعد ذلك بإنشاء رزمة طلب ARP نيابة عن الضحية وإغراق بقية الشبكة بها.
4. لا ينتظر التطبيق حدوث التحديث التلقائي لذاكرة التخزين المؤقت ARP وبدلاً من ذلك يتم تنفيذ تحديث استباقي.
5. لذلك تستمر الشبكة في العمل بالطريقة العادية دون أي انقطاع.

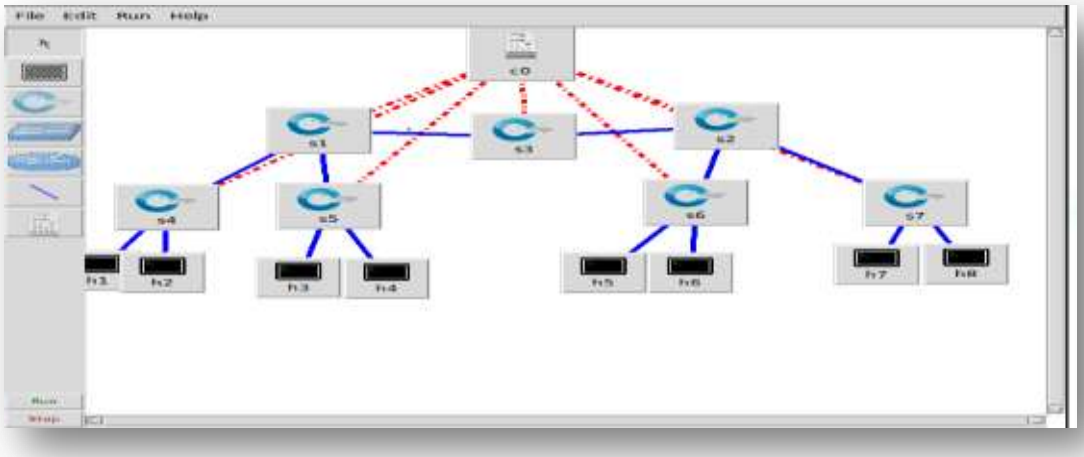
النتائج والمناقشة:

المحاكاة:

السيناريو الاول:

الهدف من السيناريو هو مقارنة أثر عدة أنواع من الهجمات على الشبكة تم تحقيق هجوم Man-in-the-Middle من نوع ARP ومن نوع TCP- attack ومن نوع ssh- attack , ودراسة أثر الهجمة على الشبكة .

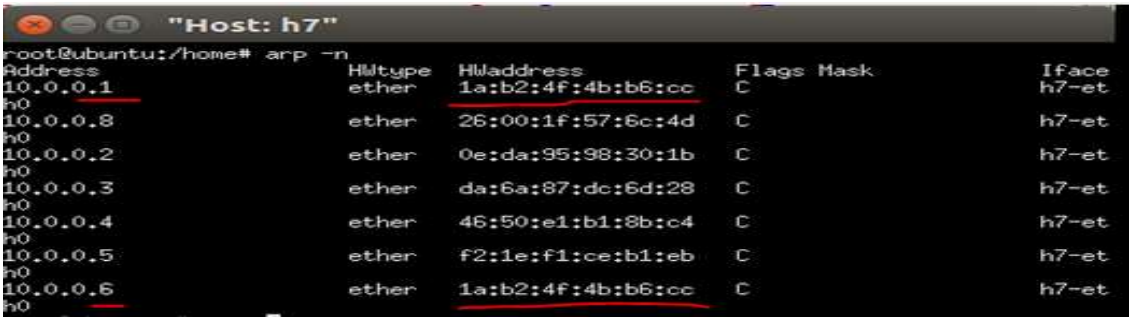
تم تجهيز بيئة العمل لتشغيل طبولوجيا الشبكة و تشغيل المتحكمات وتم استخدام أداة لتوليد الهجوم وهي ettercap والطبولوجيا هي من نمط tree كما هو موضح في الشكل التالي (6-1):



الشكل (6-1) الطبولوجيا المستخدمة

نعتبر المضيف Host1 هو المهاجم وطرفي الاتصال هما Host7 , Host6 بضبط إعدادات الهجوم في ettercap ومن ثم نتحقق من نجاح الهجوم حيث أن عنوان الهدف هو نفسه عنوان المهاجم.

يتم التحقق كما في الشكل (6-2):

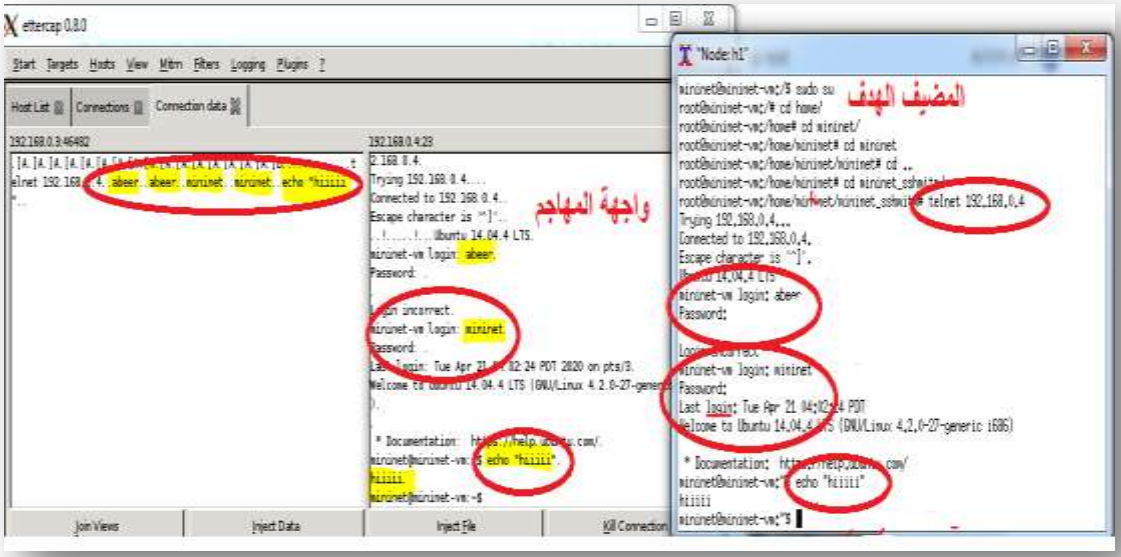


الشكل (6-2) جدول الARP

تمت مراقبة كل حركة مرور الشبكة بين الطبقات باستخدام تقنيات التزييف ARP.

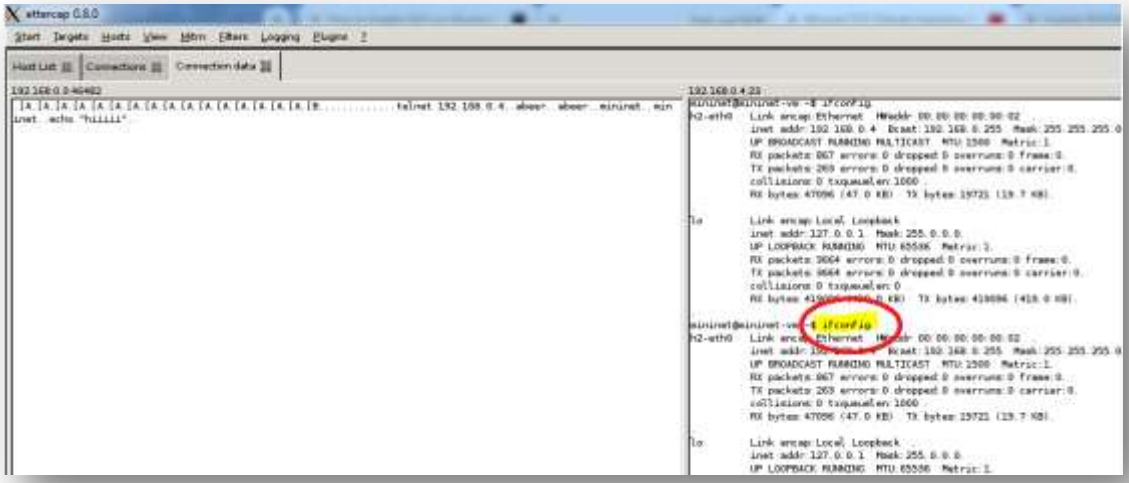
تحقيق هجوم TCP- attack , ودراسة أثر الهجمة على الشبكة وما يمكن للمهاجم القيام به:

الطبولوجيا المستخدمة من نمط single (3 hosts with single switch) نقوم ببناء الطبولوجيا ثم نضبط إعدادات الهجوم بحيث يكون h3 هو المهاجم و h1 هو الهدف لاحظنا أنه بالإضافة إلى سرقة الحساب يستطيع المهاجم الوصول إلى جميع العمليات التي تتم خلال جلسة الاتصال بين الطرفين الهدف.



الشكل (6-3) استعراض واجهة المهاجم بعد تنفيذ الهجوم

بالإضافة إلى أنه من واجهة المهاجم يمكن أن يقوم بتنفيذ أي أمر لدى الضحية أي التحكم بجهاز الضحية كما في الشكل (6-4) :



الشكل (6-4) استعراض واجهة المهاجم بعد حقن أمر لدى الضحية

تحقيق هجوم SSH-attack ودراسة أثر الهجوم على الشبكة وما يمكن للمهاجم القيام به :

الطبولوجيا المستخدمة من نمط single(3 hosts with single switch) نقوم ببناء الطبولوجيا

ثم نضبط إعدادات الهجوم بحيث يكون h3 هو المهاجم و h1 هو الهدف لاحظنا أنه بالإضافة إلى سرقة الحساب المشفر حيث سيقوم بفك التشفير للحصول على بيانات الحساب كما يستطيع المهاجم الوصول إلى جميع العمليات التي تتم خلال جلسة الاتصال بين الطرفين الهدف.

وبمقارنة الهجمات التي تمت دراستها نلاحظ في الجدول (6-1) مايلي:

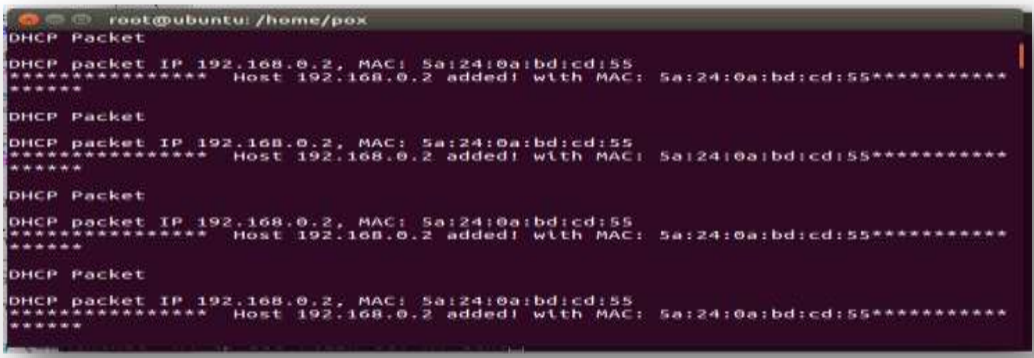
ARP spoofing	TCP attack -SSH attack
يتظاهر المهاجم بأنه مضيف موثوق	يتظاهر المهاجم بأنه مضيف موثوق
يلتقط المهاجم الرسالة ويعيد إرسالها	يمكن للمهاجم مراقبة الاتصال ومراقبة المعلومات المرسلة
يقوم المهاجم بتغيير أو حذف أو تسجيل أجزاء من الرسالة الأصلية	يمكن للمهاجم الحصول على حركة المرور أو أي معلومات مفيدة مثل كلمة المرور والبيانات المرسلة بين الطرفين.
يمكن للمهاجم أن يجعل الهدف غير متاح للمستخدم أي قطع الاتصال	يمكن للمهاجم رؤية جلسة الاتصال بوضوح بالإضافة إلى تسجيل الدخول الى الحساب المسروق وتنفيذ أي أمر على الجهاز الهدف.

الجدول (6-1) مقارنة هجمات الرجل في المنتصف

السيناريو الثاني :

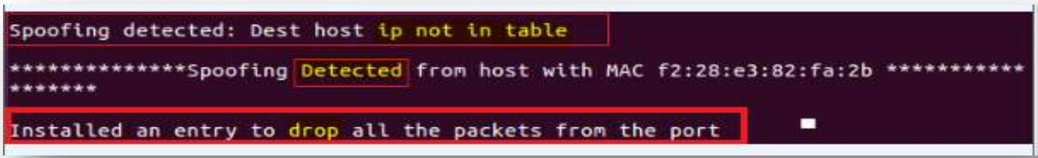
الهدف من هذه السيناريو هو تحقيق الهجوم ومن ثم الكشف عن الهجوم وصد هذه الهجوم عبر استخدام خوارزمية [9] Mitigating ARP Spoofing Attacks وتقييم أداء هذه الخوارزمية على الشبكة.

هنا في الشكل (6-5) يوضح كيف المتحكم سيقوم بمراقبة جميع الحزم الواردة إلى منفذه



الشكل (6-5) مراقبة المتحكم لجميع الحزم الواردة إلى منفذه

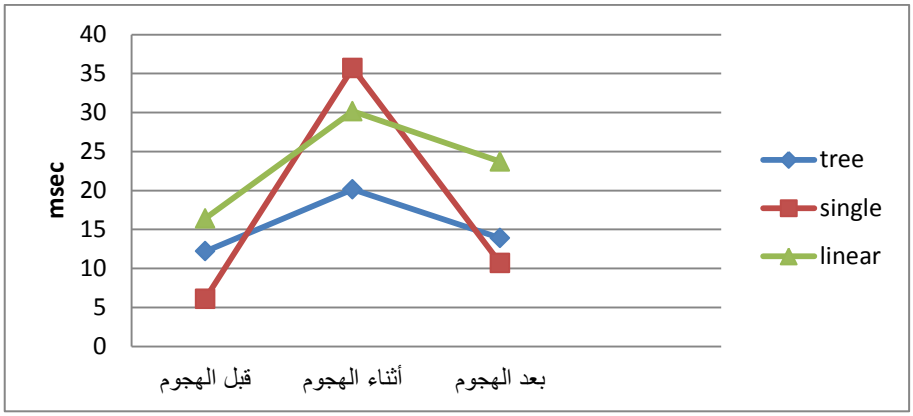
في حال تم اكتشاف التدفق الكبير للحزم الضارة سيتم إيقافها كم في الشكل (6-6):



الشكل (6-6) اكتشاف التدفق للحزم الضارة و إيقافها

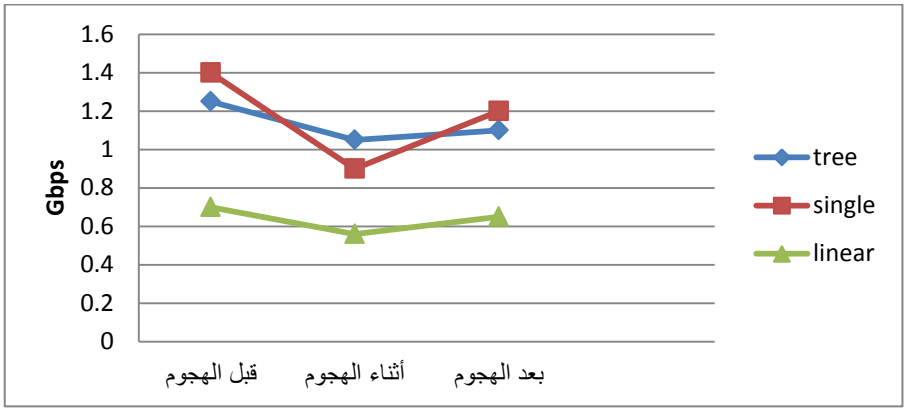
قيّمنا أداء الخوارزمية السابقة عبر دراسة أهم البارامترات وهي زمن تأسيس الاتصال بين المبدل والمتحكم و زمن الرحلة الانكفائية RTT (Round Trip Time) وهو الزمن الذي تحتاجه أول رزمة تُرسل في الشبكة للوصول للهدف و متوسط الإنتاجية وهي متوسط البيانات المستقبلة بوحدة الزمن الثانية باستخدام الإحصائيات المتوفرة ضمن برنامج wireshark وباختلاف الطبولوجيات فكانت النتائج كما يلي:

<u>أولاً:</u> زمن تأسيس الاتصال حيث تم حساب الزمن من لحظة تأسيس اتصال TCP بين المتحكم والمبدل وحتى انتهاء عملية التهيئة وتمت دراسة هذه البارامتر قبل الهجوم و أثناء الهجوم وبعد الكشف عنه وصده وهو مبين في الشكل (6-7):



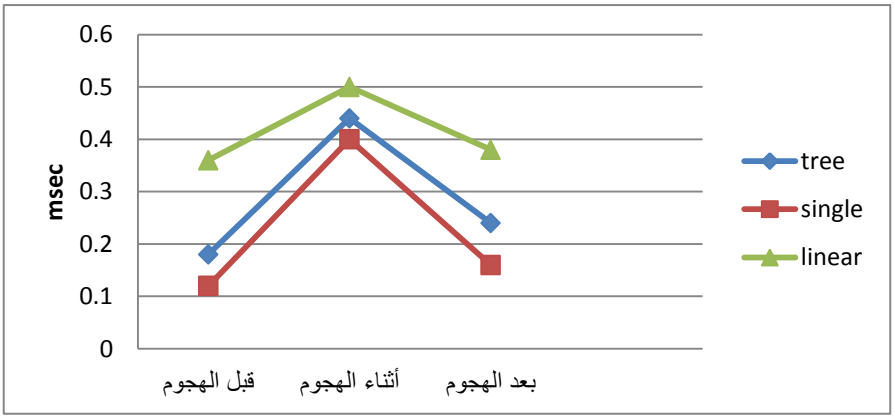
الشكل (6-7) زمن تأسيس الاتصال

ثانياً: متوسط الإنتاجية وهي مبينه في الشكل (6-8):



الشكل (6-8) الإنتاجية

ثالثاً: زمن الرحلة الانكفائية وهو مبين في الشكل (6-9) :



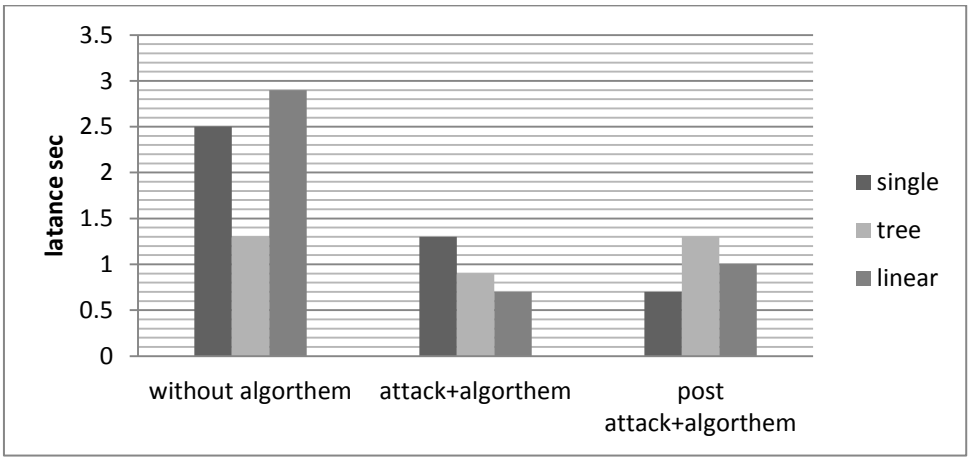
الشكل (6-9) زمن الرحلة الإنكفائية

نلاحظ أن زمن تأسيس الاتصال لجميع الطبولوجيات يزداد بشكل كبير أثناء هجوم ARP Spoof نلاحظ بعد التعافي من الهجوم أن الطبولوجيا single كانت الأقل بزمن تأسيس الاتصال والأقل بزمن الرحلة الإنكفائية والأكثر بالإنتاجية لأنه تم توصيل جميع العقد مع مبدل واحد بينما يكون التأخير في الطوبولوجيا الخطية أكبر والإنتاجية أقل نظرًا لأن أعداد القفزات بين العقد الطرفية أكبر ، ويلزم المزيد من وقت الانتشار للعقد الوسيطة لتوصيل الرزمة إلى وجهتها المحددة.

السيناريو الثالث:

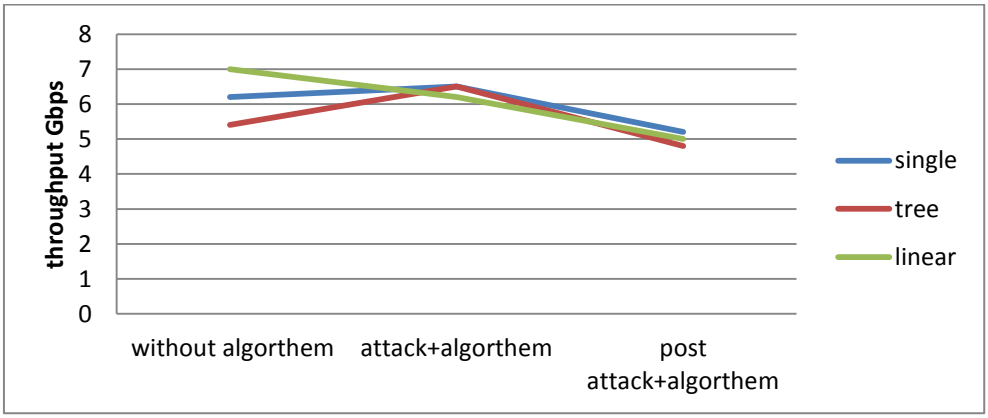
قمنا بتقييم أداء الخوارزمية NetWatch عبر دراسة أهم البارامترات وهي التأخير وهو يمثل زمن تأسيس الاتصال و زمن الرحلة الإنكفائية و متوسط الإنتاجية باستخدام الإحصائيات المتوفرة ضمن wireshark وباختلاف الطبولوجيات فكانت النتائج كما يلي:

التأخير بالنسبة للطبولوجيات المختلفة للخوارزمية NetWatch وهو مبين في الشكل (6-10):



الشكل (6-10) التأخير بالنسبة للطبولوجيات المختلفة للخوارزمية NetWatch

متوسط الإنتاجية وهي مبينه في الشكل (6-11):

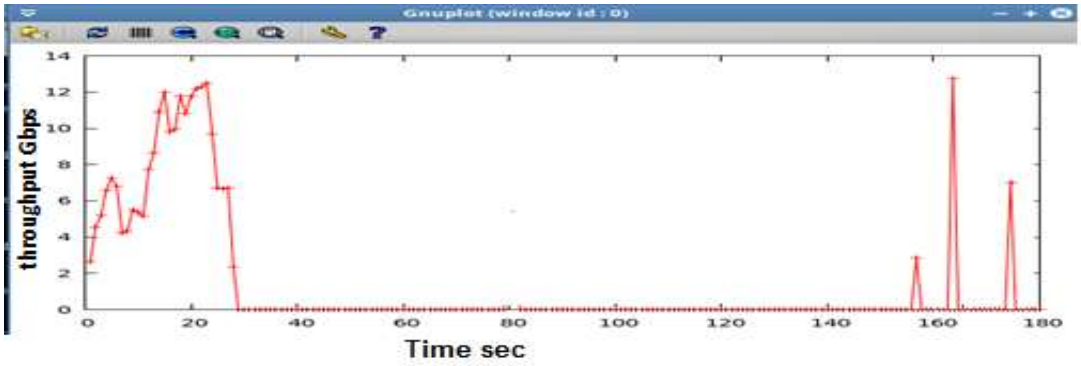


الشكل (6-11) الانتاجية بالنسبة للطبولوجيات المختلفة للخوارزمية الاولى:

نلاحظ أن الطبولوجيا الشجرية أكثر ثباتاً من حيث زمن التأخير و من حيث الإنتاجية

نلاحظ أن التأخير في هذه الخوارزمية قبل حدوث الهجوم أكبر وذلك بسبب الوقت المستغرق لتأسيس الاتصال وبناء جدول التدفق.

وعند دراسة تغيرات الانتاجية عبر الأداة Gunplot أثناء إجراء اتصال TCP لمدة دقيقتين ضمن طبولوجيا شجرية بين مضيفين بحيث يكون الاتصال دون هجوم لمدة 20 ثانية ثم حدوث الهجوم كانت النتيجة كما هو موضح في الشكل (6-12):



الشكل (6-12) تغيرات الانتاجية عبر اجراء اتصال TCP ضمن طبولوجيا شجرية

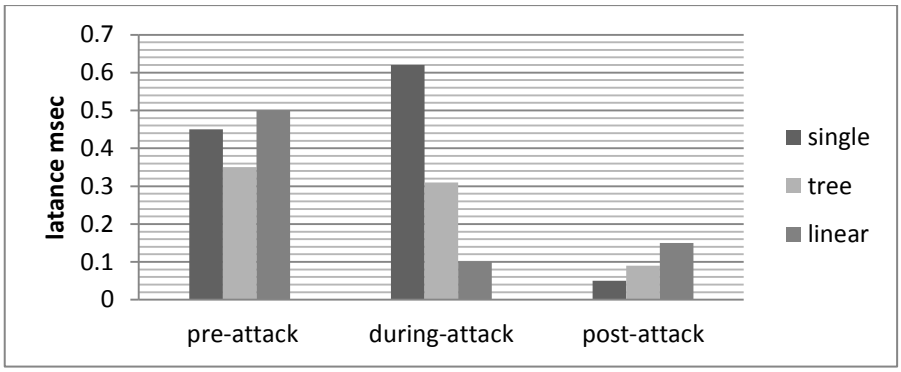
نلاحظ تعطل الشبكة لبعض الوقت إلى أن اكتُشف الهجوم. تعود الشبكة إلى عملها بعد فترة مع إعادة جميع القواعد إلى الجدول.

السناريو الرابع:

تقييم أداء الخوارزمية المقترحة كتحسين للخوارزمية NetWatch :

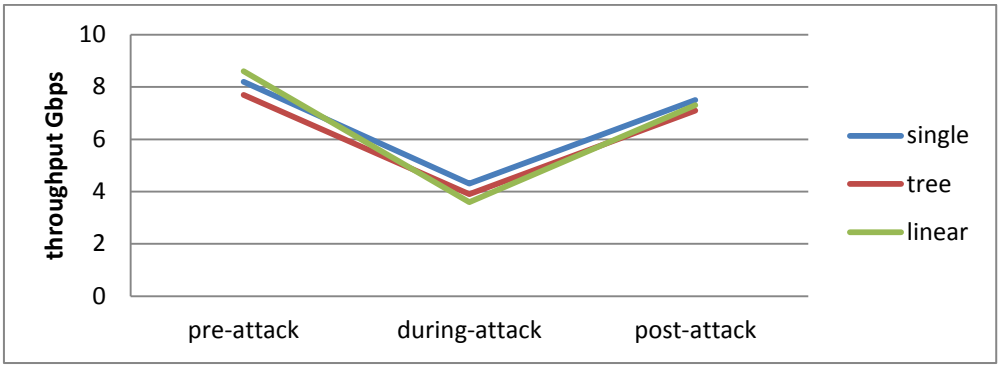
سجلت نتائج المحاكاة خلال ثلاث مراحل قبل وأثناء وبعد اكتشاف الهجوم والتخفيف منه. أجريت التجارب باستخدام طوبولوجيات المختلفة الشجرة وكذلك الطوبولوجيا الخطية وال single.

تم قياس التأخير والانتاجية بين الأجهزة قبل وأثناء وبعد الهجوم كما هو موضح في الشكل (6-13):



الشكل (6-13) تم قياس التأخير بين الأجهزة قبل وأثناء وبعد الهجوم.

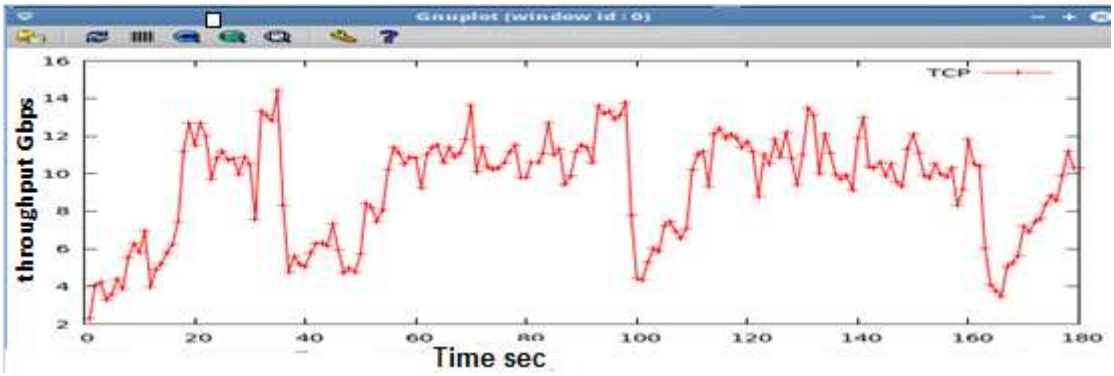
يوضح الرسم البياني أن التأخير أقل من الخوارزمية السابقة بالنسبة لجميع الطبولوجيات، و لا يوجد اختلاف كبير في زمن الانتقال بين الأجهزة المضيفة في مرحلتي ما قبل الهجوم وبعده بالنسبة للطبولوجيا الشجرية أما بالنسبة للطبولوجتين الخطية و single نلاحظ أثناء الهجوم أن الطبولوجيا الخطية أفضل بالنسبة للزمن ذلك بسبب تعدد المبدلات التي تنقل الرزم أما الخطية مبدل واحد يعمل لذا أثناء الهجوم يحتاج أكبر زمن.



الشكل (6-14) تم قياس الانتاجية بين الأجهزة قبل وأثناء وبعد الهجوم.

نلاحظ من الشكل (6-14) أيضاً لم تكن هناك اختلافات كبيرة بين قيم ما قبل الهجوم وما بعده لجميع الطبولوجيات. نلاحظ أن الإنتاجية تنخفض في هذه المرحلة لأن وحدة التحكم تقوم بتحليل الحزم المشبوهة. تواصل الشبكة حالة عملها بعد كشف الهجوم وصده.

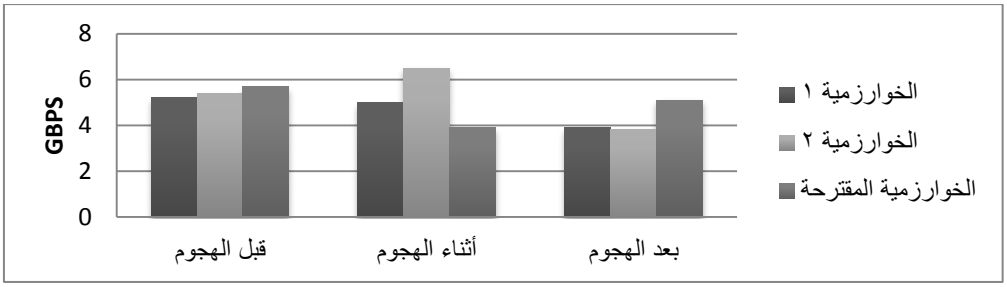
وعند دراسة تغيرات الإنتاجية عبر إجراء اتصال TCP لمدة دقيقتين ضمن طبولوجيا شجرية بين مضيفين بحيث يكون الاتصال دون هجوم لمدة 20 ثانية ثم حدوث الهجوم كانت النتيجة كما هو موضح في الشكل (6-15) :



الشكل (6-15) تغيرات الانتاجية عبر اجراء اتصال TCP ضمن طبولوجيا شجرية

لم تتوقف الشبكة في الوقت الذي تم فيه اكتشاف هجوم ARP نلاحظ انخفاضها ولكن لم تصل للقيمه صفر .

بمقارنة الخوارزميات الثلاث بسيناريو بطبولوجيا شجرية من ناحية الانتاجية نلاحظ كما في الشكل (6-16) :



الشكل (6-16) مقارنة الخوارزميات الثلاث من حيث الإنتاجية

نلاحظ أن الخوارزمية المقترحة تعيد إنتاجية الشبكة كما كانت تقريب بعد التعافي من الهجوم

الاستنتاجات والتوصيات:

- تمت دراسة ثلاث أنواع من الهجمات التي تهدد الشبكات المعرفة بالبرمجيات من نوع ARP و TCP– attack وattack –SSL. في النوع attack –SSL. بالإضافة إلى سرقة الحساب المشفر حيث سيقوم بفك التشفير للحصول على بيانات الحساب. قمنا بمقارنة أثر الهجمات الثلاث على الشبكة.
- تمت دراسة خوارزميتين وتقييم أدائهما بالنسبة للإنتاجية والتأخير. بالإضافة إلى تقييم الخوارزمية المحسنه والمقارنة بين الخوارزميات الثلاث .
- لاحظنا أن الخوارزمية NetWatch تحتاج وقت أكبر لتأسيس الاتصال وأن الشبكة تعطلت عن العمل حتى يتم اكتشاف الهجوم من قبل المتحكم. تعمل الخوارزمية على افتراض أنه سيتم حظر المضيف الضار خلال مدة معينة بمجرد إصدار التنبيه.
- الخوارزمية المحسنة بمجرد اكتشاف الهجوم ، تضيف إدخالاً جديداً في جدول التدفق لإسقاط جميع الحزم من المهاجم وإصدار تنبيه. بعد ذلك ، تقوم باسترداد ذاكرة التخزين المؤقت ARP التي تعمل في وحدة التحكم عبر إنشاء رزمة طلب ARP نيابة عن الضحية وإغراق بقية الشبكة بها. ثم يتم غمر رزم المسار به يؤدي هذا إلى تصحيح ذاكرة التخزين المؤقت ARP لجهاز الضحية دون الحاجة إلى انتظار انتهاء مهلة ذاكرة التخزين المؤقت وبالتالي يحافظ على اتصال الجهاز بالشبكة.
- من الأعمال المستقبلية دراسة حلول أمنية ذكية والتي تتحقق في الزمن الحقيقي ، وكشف الهجوم وصده بالاعتماد على التعلم الآلي. ودراسة خوارزميات لتحقيق الأمن بشكل أفضل عبر كشف الهجوم وصده بالاعتماد على التعلم الآلي في اتخاذ القرارت في الشبكات المعرفة بالبرمجيات.

References:

[1] Alper Kaan Sarica and Pelin Angin. *Explainable Security in SDN-Based IoT Networks* . Department of Computer Engineering, Middle East Technical University,2020.

[2] E. Suresh Babu, P S V Srinivasa Rao, M Srinivasa Rao, C Nagaraju. *A Novel Method to Detect and Defend the MITM attack in Software Defined Networks*. International Journal of Advanced Engineering and Global Technology I Vol-03, Issue-04, College of YV University, Proddatur, A.P, India, April 2015.

[3] Michael Brooks, Baijian Yang. *A Man-in-the-Middle Attack Against OpenDayLight SDN Controller*. Department of Computer and Information Technology Purdue University, 2015.

[4] Ramachandra Kamath Arbettu. *Security Analysis of OpenDaylight, ONOS, Rosemary and Ryu SDN Controllers*. Department of Computer Science TU Darmstadt, Germany,2016.

[5] Oluwadamilola, Shahram.Heydari. *Security Analysis Of ONOS SoftWare –Defined Netwark Platform*, Faculty of Business and Information Technology Faculty of Business and Information Technology, Canada ,2016

[6] Cheng Li, Zhengrui Qin, Ed Novak, Qun Li, Member . *Securing SDN Infrastructure of IoT-Fog Networks from MitM Attacks*, IEEE 2018.

[7] Kai Zhang Beijing . *CMD: A Convincing Mechanism for MITM Detection in SDN*, Key Laboratory of Network System Architecture and Convergence Beijing University of Posts and Telecommunications Beijing, China.2018.

[8] E. Suresh Babu, P S V Srinivasa Rao, M Srinivasa Rao, C Nagaraju. *A Novel Method to Detect and Defend the MITM attack in Software Defined Networks*. International Journal

of Advanced Engineering and Global Technology I Vol-03, Issue-04, College of YV University, Proddatur, A.P, India, April 2015.
[9] Ahmed M.AbdelSalam, Ashraf B. El-Sisi. *Mitigating ARP Spoofing Attacks in Software-Defined Networks*. Faculty of Computers and Information, Menoufia University.Menoufia, Egypt 2015
[10] Deepa Balagopal Dept . *NetWatch:Empowering Software-Defined Network Switches for Packet Filtering*. of Computer Applications Karpagam University Coimbatore,India,2015.
[11] Alhasan Abo Obaid Mohammed Sobih. *Performance evaluation of controllersin software-defined networks*. Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (04) No. (5) 2018
[12] Afraa Mohammad Ahmad Saker Ahmad .*A Study of OpenFlow Protocol and POX Controllerin Software Defined Networks(SDN) Using Mininet.* Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (41) No. (1) 2019.
[13] Ranim Sino Radwan Dandah,Talal AlAateky**.** *A Study and Performance Evaluation of OpenDaylightController in Software Defined Networks (SDN).* Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (42) No. (3) 2020**.**
[14] NOX. Retrieved from <https://github.com/noxrepo/>
[15] Ryu. Retrieved from <http://osrg.github.com/ryu >.
[16] Floodlight project, available at: <http://floodlight.atlassian.net>