حماية وأمن شبكات الواي فاي ضد الاختراق والتطفل

(بالتطبيق على كلية كسلا التقانية)

- د. أحمد محمد نور عجيل ،قسم تقانة المعلومات، جامعة السودان التقانية ،السودان

Gehad2014.system@gmail.com

- د. غفاري حسن حاج حمد، قسم علوم الحاسوب وتقانة المعلومات، كلية علوم الحاسوب، جامعة كسلا، السودان gfary55@gmail.com

المستخلص

هذه الدراسة تقدم حلولاً لمشكلة الإختراق والتطفل علي الشبكات اللاسلكية ، خصوصا شبكات الواي فاي(WI-FI) والتي أصبحت مستخدمة بصوة كبيرة في المؤسسات والشركات والمجمعات السكنية الكبيرة، إهتمت الدراسة بشكل كبير بمسألة الأختراق الغير قانوني للشبكات اللاسلكية ، وضبط عملية الإتصال بأجهزة الواي فاي. هدفت الدراسة إلي تحديد نقاط الضعف في الوصول الي أجهزة الواي فاي، والعمل علي تقويتها وتعزيزها وذالك بإستخدام نظام فلترة العناوين الفيزيائية(MAC Address) بالإضافة الي كلمات المرور القوية، واستخدمت الدراسة المنهج الوصفي التحليلي والمنهج الاستنباطي والتطبيقي لدراسة مسألة إختراق شبكات الواي فاي، واستخدمت الخوارزميات في التصميم، ونماذج لأجهزة شبكات الواي فاي ذات الإستخدام الشائع(D-link & Linksys) في التطبيق.ومن أهم النتائج التي توصلت لها الدراسة: تصميم نموذج وصول آمن لأجهزة الواي فاي وتنفيذ وتطبيق حزمة القيود التي تمنع المتطفلين للوصول الي أجهزة الواي فاي. وقد أوصت الدراسة بضرورة إستخدام أجهزة واي فاي ذات سعات أكبر لنظام فلترة العناوين الفيزيائية(MAC Address) وتشبيك أكثر من جهازي واي فاي لضمان عملية التحكم ولزيادة عدد المستخدمين للشبكة اللاسلكية. أوصت الدراسة كذلك بضرورة إعتماد جهاز واحد لكل مستخدم ، وتعقيد كلمات المرور وتغييرها بصورة دورية وتدريب المستخدمين بضرورة المحافظة علي كلمات المرور وعدم الكشف عنها. وتنشيط خاصية التحقق باستخدام العنوان المنطقي (IP Address) لزيادة الخاصية الأمنية للشبكة اللاسلكية. وإستخدام أنظمة كشف التسلل اللاسلكي (WIDS or WIPS).

الكلمات المفتاحية: شبكات الواي فاي(wi-fi)، الشبكات اللاسلكية ، الوصول الآمن، كلمات المرور، العناوين الفيزيائية(MAC address).

Secure and Protection the (WI-FI)neworks against the breakout-in application on kassala technical faculty

- **Dr. AhmedMohammedNorEjail, Department of Technology &Information, KassalaTechnological College, Technological University, Kassala, Sudan**
  Gehad2014.system@gmail.com
- **Dr. Gfary Hassan Haj Hammed' Department of Computer Science and Information Technology, Faculty of Computer Science, University of Kassala, Kassala, Sudan.** **Gfary55@gmail.com**

Abstract

This study present solutions to the problems of Hacking, and Intrusion on wireless network specially (wi-fi) networks which became using in spread way in companies , institutions and a large residential compounds. The study took more care of Illegal Hacking of Wireless Networks and complete the legal Users of applications and services of these networks, control and regulation of Wi-Fi connections. The study aimed to determine the weakness points in Access to (wi-fi) devices by using MAC address filtering in addition to strong passwords. The study used analytical description methodology, deductive and application methodology to study the Hacking of (wi=fi) devices. The study used algorithmic in designing and models for the networks of (wi-fi) devices in common use (D-link & Linksys Devices) in application. The important results which arrived by this study, design secure Access model for Wi-Fi networks. and applicant packets to deny Access the Intrusions Access to Wi-Fi networks. The study recommended to the important using of (wi-fi) devices which have a big capacity to filters physical address (MAC Address) and connecting more then one (wi=fi) to ensure the controlling process and to increasing the numbers of users on a wireless network. The study also recommended for the important to one Device per user policy and complicate the password, change it periodically, trained the users to keep the password, and activating IP Address verification to enhance the security features of the wireless network.

Keywords: (wi-fi) networks , wireless networks , safe arriving , passwords , physical address(MAC address)

المقدمة:

تعتمد اجهزة الواي فاي(wi-fi) علي اسلوب التوزيع اللاسلكي ، لتوزيع خدماتها ويتطلب ذلك ضرورة الإعداد المسبق لتقييد عملية الوصول لتلك الاجهزة وضروة تنفيذ مجموعة من الإجراءات والقيود لتشغيل تلك الشبكات للإستفادة القصوي من الخدمات والتطبيقات والوصول الآمن للإنترنت وصد كل المتطفلين علي الشبكة.

مشكلة الدراسة:

1- إختراق كلمات المرور للدخول الي أجهزة الواي فاي وتسريب كلمات المرور من قبل الموظفين لأصدقائهم للإستفادة من خدمات الإنترنت بصورة غير قانونية.

2 – البطئ الزائد والتحميل الكبير لخدمات أجهزة الشبكات اللاسلكية من قبل المتطفلين مما يسبب في مضايقة المستخدمين الحقيقيين في الإستفادة من خدمات الشبكة.

3 – عدم إتباع سياسة الخصوصية الآمنة وضعف إجراءات الوصول الي جهاز الواي فاي من قبل مشغلو تلك الشبكات اللاسلكية .

أهداف الدراسة:

- تكمن أهداف الدراسة في إتباع سياسة الخصوصية الأفضل ومنع عمليات التطفل وإختراق عملية الوصول الي أجهزة الشبكات اللاسلكية خصوصاً شبكات الواي فاي، وتصميم خطة الول للشبكة بطريقة تسمح فقط الوصول للمستخدمين الحقيقيين والمصرح لهم بالإستفادة من جميع الخدمات التي تقدم عبر الشبكة اللاسلكية، وتقديم طريقة أفضل للتشغيل الآمن للشبكات اللاسلكية باستخدام خوارزميات التشفير الأكثر شيوعًا.
- في حالة مشاركة الملفات والوصول إلى الطابعات على الشبكة اللاسلكية، من الأفضل أن يكون هنالك مصادقة والتحقق من هوية المتصلين بالشبكة وذلك باستخدام كلمات المرور وتصفية العناوين للأجهزة وتفعيل نظام الجدار الناري لصد ومنع المتسللين والمتطفلين علي الشبكات اللاسلكية، والسماح بالوصول الآمن إلى الشبكة المحلية للأطراف الخارجية.

أهمية الدراسة:

تكمن أهمية الدراسة في التحكم الفعال والوصول الآمن لخدمات الشبكات اللاسلكية خصوصاصاً شبكات الواي فاي وذلك بطريقة سهلة وفعالة في تصميم نظم التحكم الحديثة، وتقليل الجهد المبذول في عمليات

اكتشاف وتشخيص الأعطال وتسريع عملية اتخاذ القرار، ومحاولة لإثبات أهمية الوصول الآمن للشبكات اللاسلكية، وتغيير طريقة إدارة الشبكات اللاسلكية التقليدية والتي تعتمد إستخدام كلمات المرور فقط للوصول الي خدمات الشبكات اللاسلكية. أيضاً تكمن أهمية الدراسة في تعضيد الخصوصية والأمان وإستخدام طرق أفضل لإدارة الشبكات اللاسلكية، وتأمين شبكات الواي فاي ضد التطفل ومنع التسلل والإستفادة من الخدمات بصورة غير قانونية.

الدراسات السابقة:

1- دراسة(Stefaan,2004وآخرون): ركزت هذه الدراسة علي عملية تأمين وصول حزم البيانات الي الجهة المستقبلة بصورة سليمة بدون التعرض للتغير في المحتوي أو حذفها، وركزت الدراسة علي تقنية البلوتوث في الإرسال والإستقبال، وتوصلت الدراسة الي قوة الآمان فيها خصةصا عند إستخدامها في الهواتف الذكية.

2- دراسة (Wolf,2018 وآخرون): إهتمت الدراسة بمسألة الأمن بصورة عامة وركزت علي تقنية IEEE 802.11 كمعيار قياسي للشبكات اللاسلكية وإستخدامه في التقنيات الحديثة للهواتف الذكية(Smart Phones) بالإضافة لدراسة تقنية البلوتوث في الإرسال اللاسلكي.

3- دراسات (عبدالستار،2022) : إهتمت الدراسة بمسألة الثغرات الامنية ونقاط الضعف في تصميم الشبكات اللاسلكية، وركزت بصورة كبيرة علي إختراق تلك الشبكات خصوصا الشبكات الغير مشفرة، تناولت الدراسة كذالك طرق التشفير المستخدمة وكيفية تطبيقها.

4- دراسة (أحمد وآخرون،2011) : تناولت الدراسة بصورة أساسية البروتوكولات المستخدمة في الشبكات اللاسلكية وأنواعها، وتقنيات شبكات الواي فاي ، ومن ثم ركزت علي تقنية الواي ماكس من حيث الخصائص وطريقة العمل، ووضحت الفرق بين تقنية الواي فاي والواي ماكس.

5- دراسة (المنسي،2013) : ركزت الدراسة علي الأمن والمنطق في الشبكات اللاسلكية ودراسة أنواع التشفير المستخدمة بالتطبيق علي تقنية WEP وكيفية تنفيذها علي الشبكات اللاسلكية ودراسة المميزات والعيوب عند إستخدام هذه التقنية.

المقارنة والتعقيب:

معظم الدراسات السابقة ركزت بصورة عامة علي مسألة الامن في الشبكات اللاسلكية ودراستها بصورة عامة والبعض منها ركز علي مسألة الثغرات الامنية ودراسة التشفير والبروتوكولات المستخدمة فيها، والبعض منها ركزت علي تقنية الواي ماكس من حيث الخصائص وطريقة العمل، بينما الدراسة الحالية ركزت بصورة أساسية

بمسألة إختراق كلمات المرور للدخول الي أجهزة الواي فاي وتسريب كلمات المرور، وعدم إتباع سياسة الخصوصية الآمنة وضعف إجراءات الوصول الي شبكات الواي فاي من، ووضعت حلولا عملية للحد من هذه المشكلة وذلك بإضافة التحقق من هوية المتصلين باستخدام نظام فلترة العناوين الفيزيائية وكلمات المرور القوية(MAC Address & Password).

الشبكات اللاسلكية (Wireless Network):

شبكات الحاسوب اللاسلكية هي عبارة عن مجموعة من الأجهزة التي تعمل لا سلكياً بدون الحاجة للربط السلكي، حيث تعمل عن طريق الارسال اللاسلكي في إرسال وإستقبال حزم البيانات ، وتعتمد هذه الشبكات علي ميزة عدم التقيد بالمكان وحرية التنقل بالأجهزة من مكان الي آخر حول محيط بث الشبكة اللاسلكية والمسافة التي تغطيها تلك الشبكة.

أمن وخصوصية الشبكات اللاسلكية: أمن الشبكات اللاسلكية أو الأمن اللاسلكي هي عملية منع الوصول الغير المصرح به أو تلف أجهزة الحاسب الآلي أو البيانات باستخدام الشبكات اللاسلكية، والتي تشمل شبكاتWi-Fi. والذي يتضمن الخصوصية المكافئة للشبكات السلكية (Wired Equivalent Privacy)(WEP)والوصول الآمن اللاسلكي لخدمات الشبكات اللاسلكية ، هنالك عدة طرق مستخدمة لتحقيق الخصوصية وهي :

1. WEP (Wired Equivalent Privacy) الخصوصية المكافئة للشبكات اللاسلكية.
2. WPA (Wired Protected Access) الوصول الآمن للشبكات اللاسلكية- الجيل الثاني
3. WPA2 (Wired Equivalent Access) الوصول الآمن للشبكات اللاسلكية- تحسين في الجيل الثاني
4. WPA2 / WPA (Wired Equivalent Access) الوصول الآمن للشبكات اللاسلكية المختلط مع الاصدار الثاني. المعيار الحالي والأكثر أمناً وحماية هو WPA2 ؛ حيث أنه لا يمكن لبعض الأجهزة أن تدعم WPA2 دون ترقية البرامج الثابتة أو استبدالها. يستخدم WPA2 جهاز تشفير أقوى مما يساعد بتشفير الشبكة باستخدام مفتاح بطول 256 بت.
5. **WPA3** (Wired Equivalent Access) :

هو معيار أمان جديد لاتحاد WFA للشبكات الشخصية والشبكات المخصّصة للمؤسسات. ويهدف إلى تحسين أمان شبكة Wi-Fi بشكل عام باستخدام اتّباع خوارزميات أمان حديثة ومجموعات رموز تشفير أكثر أمانًا. يتكوّن WPA3 من جزأين:

- **(WPA3-Personal)** : يستخدم المصادقة المتزامنة بين جهات الاتصال (SAE) بدلاً من المفتاح المشترك مسبقًا(PSK) ، ما يقدّم للمستخدمين وسائل حماية أمان قوية ضد الهجمات، مثل هجمات القاموس بلا إنترنت واسترداد المفتاح وتزوير الرسائل.
- **(WPA3-Enterprise):** يوفّر طرق مصادقة وتشفير قوية على مستوى ربط البيانات، ووضع أمان اختياريًا بسعة 192 بت لتوفير أمان فعّال في البيئات التي تتطلب إجراءات أمان مشددة.

شبكات الواي فاي (WI - FI Network):

تعريف: تعرف شبكات الواي فاي بأنها إختصاراَ ل(wireless Fidelity) وتعني الدقة في إرسال وإستقبال الموجات اللاسلكية، وهي إحدي الطرق المتبعة في ربط الأجهزة والمعدات لا سلكياً. يتم إستخدام هذا النوع من الشبكات من قبل معظم الشركات والمؤسسات والمجمعات السكنية بغرض الاستفادة والمشاركة في خدمات الشبكة العنكيوتية(الإنترنت) وذلك بغرض تقليل التكلفة. وهي جزء لا يتجزء من الشبكات اللاسلكية والتي تجد إنتشاراً واسعاً علي نطاق إستخدامها في المؤسسات والشركات وحتي علي مستوي المجمعات السكنية، حيث تعمل هذه الشبكات علي نطاق ومسافات قصيرة نسبياَ لا تتعدي مسافة 100 متر.

مميزات شبكات الواي فاي:

1. سهولة وسرعة التركيب وضبط الإعدادات اللازمة للتشغيل.
2. التكلفة المنخفضة نسبياً بالمقارنة مع الشبكات السلكية.
3. يمكن لجهاز لا سلكي واحد أن يربط عدداً من أجهزة الحواسيب والهواتف الحديثة.
4. سهولة وسرعة إكتشاف وتشخيص الأعطال وإصلاحها.

التحديات التي تواجه شبكات Wi-Fi :

معظم شبكات (Wi-Fi) المفتوحة غير آمنة للاتصال بها وذلك لعدم تطبيق الحزمة الكافية من سياسات الخصوصية للتحقق من هوية المستخدمين، وقد ينتحل المتسللون هوية أحد المستخدمين ويعمل علي اختراق الشبكة والتزود بخدماتها أو العمل علي التعطيل التطبيقات التي تعمل علي الشبكة أو التلاعب بالبيانات والمعلومات، بصورة عامة هنالك عدة تحديات تواجهه تلك الشبكات منها:

1. مسافات تغطية أقل وقصيرة مقارنة بالشبكات اللاسلكية الأخري.
2. سرعات أقل بكثير في عملية نقل البيانات بالمقارنة مع الشبكات اللاسلكية.
3. تأثيرات جانبية علي صحة الإتسان علي المدي الطويل.

4. مشاكل تداخل البيانات عند وجود أكثر من شبكة لا سلكية في محيط واحد.

5. ظهور التطبيقات والبرمجيات الخبيثة التي تساعد في التطفل واختراق شبكات الواي- فاي

طرق التحقق من الهوية في شبكات ال WI-FI: يقصد بالتحقق من الهوية عملية ضمان صلاحية الاتصال والولوج بين نقاط المحطات اللاسلكية وذلك لبدء جلسة الاتصال ، وعلي أثرها يتم الاستفادة من الخدمات والتطبيقات التي توفرها الشبكة اللاسلكية للمستخدمين. وهنالك عدة طرق للتحقق من الهوية وضمان الوصول الآمن للشبكات اللاسلكية منها:

1. الحماية باستخدام كلمات المرور والتشفير(Password & Encryption):

تعتبر إحدي الطرق الأكثر شيوعا للتحقق من هوية المستخدمين وهي عبارة عن آلية لكتابة كلمة المرور بشكل صحيح وبدقة من أجل الولوج الي نقطة الاتصال للسماح بالاتصال بشبكة الانترنت والاستفادة من الخدمات التي تقدمها تلك الشبكة.

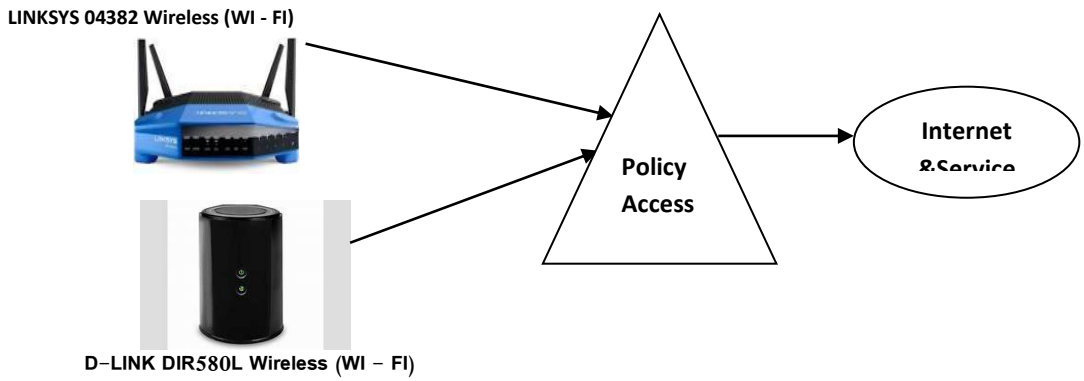
2. إستخدام نظام فلترة العناوين الفيزيائية(Filter of MAC Address):

يستخدم لتعزيز الخاصية الأمنية للشبكات اللاسلكية وتوفير آلية لتتبع الأجهزة التي لها صلاحية الإتصال بالشبة ومنع ما سواها من الأجهزة التي يستخدمها المتطفلون علي الشبكة، ويستخدم لترشيح نقاط الوصول ويحدد الاجهزة بواسطة اضافة عنوان تحكم الوصول للوسط(MAC) الخاصة بهذه الاجهزة في خانة الاجهزة المسموح لها باستخدام الشبكة اللاسلكية ويحجب غيرها.(عبدالجميد،ص217)

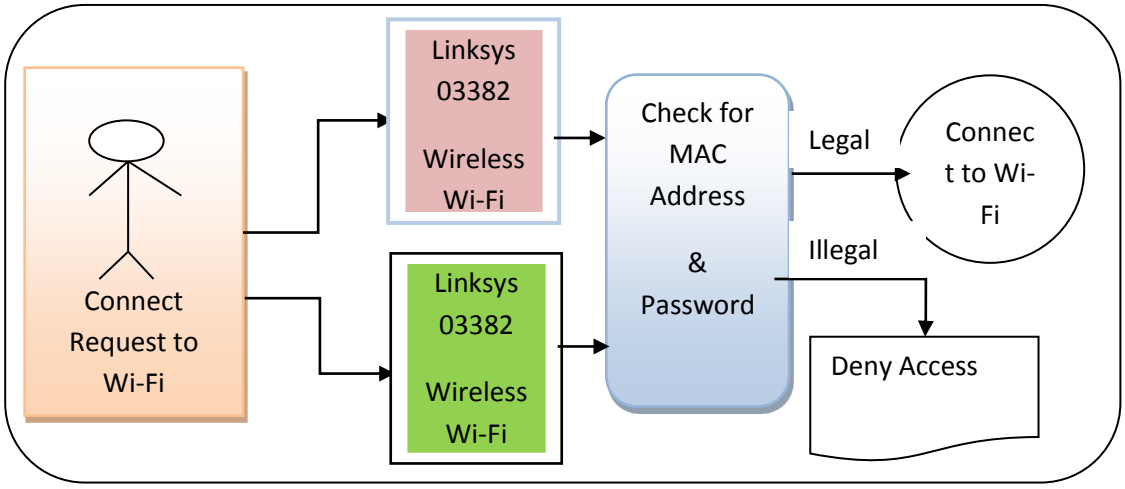
البوابات المقيدة للشبكات اللاسلكية(Firewall Filter):

عند استخدام هذه البوابات المقيدة كخاصية التحقق من هوية المستخدمين في الشبكات اللاسلكية فإن مستخدمو هذه الشبكة سيتمكنون من الاتصال والولولج بأي نقطة اتصال متوفرة وذلك بدون الحاجة الي إستخدام آليات تحقق أخري. تعمل هذه البوابات كجدران نارية (Firewall) ويمكن تطبيقها باستخدام المكونات الفيزيائية(H/W) أو إستخدم حزمة البرمجيات المتوفرة والتي تعمل علي صد ومنع أي إختراق دخول أو طلب إتصال بالشبكة غير مسموح به وهو ما يعتبر تطفل علي الشبكة، حيث تعمل علي التأكد والتدقيق في هويات المستخدمين للشبكة باستخدام عنوان الانترنت(IP Address) عبر بروتوكول الاعداد التلقائي للمضيف(DHCP) وذلك بتعديل حالة الجدار الناري والسماح لها بالحصول علي صلاحية الاتصال والوصول للانترنت عبر بروتوكول(HTTP).

النموذج المقترح للنظام(Model):



شكل(1): بنية المكونات الأساسية- المصدر: تصميم الباحثين 2025م

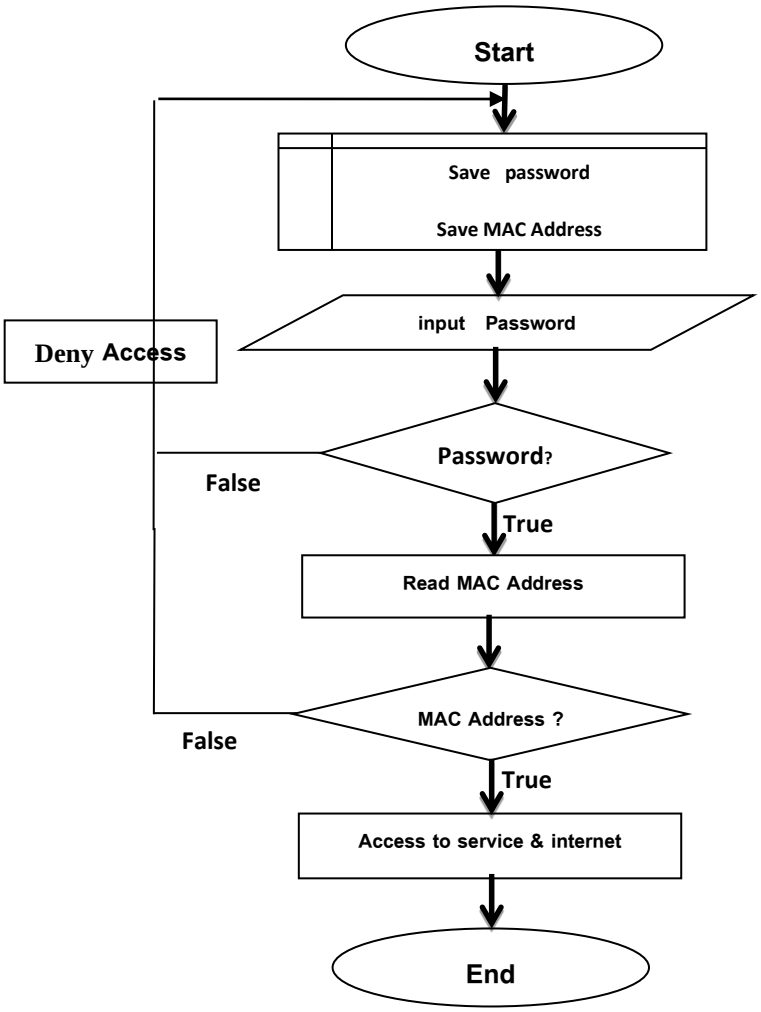


شكل رقم (2) : النموذج المقترح للنظام ، المصدر: تصميم الباحثين 2025م

طريقة عمل النموذج :

تقوم أجهزة الواي فاي بالبث اللاسلكي ضمن النطاق المسموح به وفي الغالب لا يتعدي 100 متر، بحيث تكون الاشارة قوية جدا كلما اقتربنا من محيط جهاز الواي فاي وتضعف الاشارة كلما ابتعد المستخدم اكثر من المدي الذي يغطي البث. يظهر للمستخدم إسم الشبكات للأجهزة والمعدات المتوفرة ويختار منها الشبكة التي حددت له مسبقا والتي تم تجهيز إعداداتها وحفظ العناوين الفيزيائية بداخلها(MAC Address) فإذا كانت كلمة المرور(Password) صحيحة يتم التحقق من العنوان الفيزيائي للجهاز والذي تم تسجيله مسبقا لدي جهاز الواي فاي فإذا كان موجودا يسمح له بالإتصال بالشبكة والاستفادة من الخدمات التي تقدمها حسب صلاحيات الوصول لتلك الخدمات وإلا فإن جهاز الواي فاي يعتبرها عملية إختراق وتطفل علي الشبكة ومن ثم يعمل علي حفظ عنوانه الفيزيائي وإدراجه علي قائمة الأجهزة الممنوعة من الإتصال بشبكة الواي فاي.

الخوارزمية العامة:



شكل(3): الخوارزمية العامة - المصدر: تصميم الباحثين 2025م

تسجيل العناوين الفيزيائية:

1. جهاز(Linksys 04382 wireless):

No	Device owner	department	MAC address
1	Computer	general	48:0f:cf:4d:48:5c
2	almaki	Hr	38:94:78:d0:0f:oh
3	Inaas	Computer	7c:46:85:c7:1b:ac
4	Raje	Elect	B8:6c:e8:87:ed:91
5	mohammed	Account	74:1c:27:9a:f4:92
6	Moh salih	Computer	B4:74:43:53:77:25
7	badaldain	Head dep	34:aa:8b:98:14:91
8	fadoul	security	A0:cb:fd:d0:19:18
9	montasir	labor	64:b8:53:61:44:25
10	husain	Elect	B0:89:00:92:ad:79
11	insherah	secretary	D4:7d:fc:14:8b:22
12	aboalrahim	Computer	7c:2e:d0:a2:24:9d
15	basil	mech	54:fc:f0:02:96:e0
16	zualkekil	Elect	18:3a:2d:22:d4:29
17	Ejail	Computer	Ec:df:3a:1e:69:24

جدول رقم(1): سجل العناوين الفيزيائية ، المصدر: تصميم الباحثين 2025م

2. جهاز(D-link DIR 580L wireless):

No	Device owner	job	MAC address
1	albager	Elect	08:ec:a9:95:f3:fe
2	Moh omer	Elect	0c:70:4a:27:c6:b9
3	mogtaba	mech	60:f1:89:0a:11:f3
4	Osman	mech	Bc:20:a4:c4:6a:ba
5	alfatih	Drivers	Ac:56:2c:c6:69:d6
6	Alfatih fadol	mech	E4:c8:01:83:11:b2
7	Omer tabota	mech	E4:f8:ef:02:b5:11
8	mamdouh	Account	40:d3:ae:c2:e6:da
9	karamalah	security	44:d4:e0:5a:4f:11
10	Saber moh	mech	64:89:9a:7f:31:a4
11	abdalaziz	Computer	C0:bd:d1:2d:55:f6
12	anwar	security	60:a4:d0:0c:bf:bf
15	Ahmed	security	Bc:25:e0:zb:9c:85
16	sammer	security	C0:d3:c0:1e:ce:ef
17	Amal	secretary	D0:31:69:f0:23:fd

جدول رقم(2): سجل العناوين الفيزيائية ، المصدر: تصميم الباحثين 2025م

التطبيق :

Screen (1): Allow Access to Wi-Fi Wireless

التعليق علي الشاشة :

في الشاشة أعلاه تم تفعيل خاصية فلترة نظام العناوين الفيزيائية(MAC Address) ومن خلاله تم تسجيل وحفظ عناوين الأجهزة التي يسمح لها بالاتصال بالشبكة اللاسلكية(Wi-Fi) والتزود بخدماتها.

Screen (2): Deny Access to Wi-Fi Wireless

التعليق علي الشاشة:

في الشاشة اعلاه تم رصد مجموعة الأجهزة التي حاولت التسلل الي الشبكة اللاسلكية بصورة غير قانونية، ومن ثم تسجيل عناوينها وإدخالها في قائمة المنع من الوصل الي الشبكة الاسلكية في المستقبل.

مناقشة النتائج:

من خلال تتبع عمل أجهزة الشبكات اللاسلكية وبالأخص شبكات الواي فاي توصلت الدراسة الي مجموعة من النتائج والتي تم تلخيصها في الآتي:

1. عند إستخدام نظام فلترة العناوين الفيزيائية (MAC Address) وتعقيد كلمات المرور(password) للولوج والاتصال بشبكات الواي فاي زاد من نسبة التحكم والوصول الآمن للشبكة اللاسلكية والحد من التطفل والاتصال الغير مصرح به ومزاحمة المستخدمين القانونيين للشبكة.

2. زيادة معدل سرعة الشبكة وزيادة معدل الكفاءة والاستفادة القصوي من الخدمات التي تقدمها الشبكة وذلك نسبة لمنع المتطفلين علي الشبكة وحجبهم عن الخدمات.

3. تشبيك عدد إثنين من أجهزة الواي فاي سهل من عملية حل مشكلة النطاق الضيق لإستيعاب أكبر عدد ممكن من الأجهزة وتوزيع العناوين الفيزيائية بالمناصفة علي الجهازين وذلك لضمان تطبيق سياسة الخصوصية الآمنة للإتصال بالشبكة.

التوصيات:

1. الاستفادة من نتائج الدراسة في عمليتي تضمين ودعم الوصول الآمن باستخدام كلمات المرور وتطبيق نظام فلترة العناوين الفيزيائية (MAC Address) لتلك الأجهزة والمعدات.

2. توثيق وتسجيل المعدات والأجهزة التي يسمح لها بالوصول والاستفادة من خدمات الشبكة اللاسلكية، وإستخدام خاصية التحقق من العناوين الفيزيائية لأجهزة المتطفلين وحفظها علي أجهزة الشبكة اللاسلكية وإدراجها تحت بند منع الوصول (Deny Access) لمنع وصولها مجددا.

3. إستخدام وتضمين وتنشيط خاصية التحقيق باستخدام عنوان الانترنت (IP Address) لزيادة الخاصية الأمنية للشبكة اللاسلكية. و إتباع بعض الإجراءات الشائعة والمستخدمة في تقوية نظام الحماية والامان للوصول الي جهاز Wi-Fi واستخدام سياسة خصوصية عالية ضد التطفل تجاه الشبكات اللاسلكية مثل أنظمة منع التسلل اللاسلكي (WIPS) أو إستخدام أنظمة كشف التسلل اللاسلكي (WIDS).

4. تعقيد كلمات المرور وتغييرها بصورة دورية، وتدريب المستخدمين علي كيفية التعامل مع إجراءات الأمن والحماية في الشبكة اللاسلكية، وضرورة عدم تسريب كلمات المرور للمتطفلين علي الشبكة.

5. السماح باستخدام جهاز واحد فقط لكل مستخدم للشبكة ومسح العناوين الفيزيائية للمستخدمين المنتهية عقوداتهم أو تم نقلهم الي مكان آخر مما يسمح بفرص إحتياطية لمستخدمين جدد محتملين.

6. البحث عن مجموعة الطبيقات التي تستخدم في التطفل علي الشبكات اللاسلكية وكسر وإختراق أجهزة ال WI-FI وتضمينها من خلال قائمة المواقع والتطبيقات الممنوعة من الوصول (Deny Access)

7. استخدام أجهزة واي فاي ذات سعات كبيرة وتسمح بتسجيل أكبر عدد من نطاق العناوين الفيزيائية وضرورة تشبيك أكثر من جهاز واي فاي للتحكم في الوصول الآمن للشبكة وذلك لتوفير مساحات إضافية للشبكة عند الحاجة لها في المستقبل.

قائمةالمراجع والمصادر

1. عبدالستار الشيخ احمد (2022). أمن الشبكات اللاسلكية(Wireless Network Security) ،سلسلة منشورات إتقان لتكنولوجيا المعلومات ، سوريا.
2. المنسي، نادر(2013). المختصر في أمن الشبكات اللاسلكية، سلسلة منشورات في حماية الشبكات اللاسلكية
3. احمد واخرون(2011). الشبكات اللاسلكية ((network (wi-fi,wimax)، جامعة تشرين، كلية الهندسة المعلوماتية ، سوريا.
4. عبدالحميد بسيوني(2003) – شبكات الكمبيوتر اللاسلكية – دار الكتب العلمية للنشر والتوزيع – القاهره

مصادر باللغة الإنجليزية:

1- wolf gange Osterhage (2018), " Wireless Network Security", CRC press – Tylor & Francis Group, a Science publishers Book second edition , ISBN 13:978-1-1380-9379-9 (Hardback).

2- (Stefaan Seys, Dave Singelee, Bart Preneel,2004), " Wireless Network Security" , Revue HF Tijdschift , pp 24 – 35.

Web sites:

1. https://nasainarabic.net/main/articles/view/wireless-network.
2. http://www.mhpcc.edu/accounts/password/_policy.html
3. http://www.sans.org/newlook/resources/policies/ policies.html
4. https://www.startimes.com/f.aspx/f.aspx?t=7596210
5. https://www.nasainarabic.net/main/articles/view/wireless-network
6. http://www.modwifi.bitbucket.org
7. https://www.ar.wikipedia.org
8. https://www.an.library.com.
9. https://www.wi-fi.org/discover-wi-fi/security.
10. http://www.linksys.com/support.