# أمن الشبكات اللاسلكية المخاطر والحماية
# Wireless Networks Security "Penetration and protection"

**م. أحمد نورى دخيل**
المركز المتقدم للتقنية ، قسم التوثيق والمعلومات
طرابلس ، ليبيا
yagain218@yahoo.com

**د. سعد طلحة**
كلية التقنية الالكترونية ، قسم الاتصالات
طرابلس ، ليبيا
saseya@lttnet.net

*الملخص* - **أفرز الانتشار الواسع في الشبكات اللاسلكية تزايد مخاطر وتهديدات أمن وسرية مستخدميها والمتمثلة في الاعتداء على الخصوصية واختراق وقرصنة المعلومات والبيانات، وذلك بإعتبار أنها بيئة اتصال مفتوحة والبيانات تعتبر متوفرة فى الفضاء، حيث يتم فيها استخدام موجات الراديو لتبادل المعلومات، الأمر الذى يجعلها عرضه للتصنت والهجوم النشط .**
**لذلك أمن الشبكات اللاسلكية مهم جداً للتقليل من هذه الاعتداءات والهجمات، ولتقليص المخاطر والاعتداءات الناجمة عن الثغرات الأمنية التي تهدد الشبكات اللاسلكية، بات من الضرورة ايجاد حلول أمنية لمنع الهجمات والاعتداءات التي تتعرض لها هذه الشبكات.**
**تعرض هذه الورقة سبل تحقيق الامن في الشبكات اللاسلكية ومعرفة أنواع الاعتداءات والهجمات على هذه الشبكات اللاسلكية والتعرف على الطرق المستخدمة في إدارتها وتأمينها ومن تم الوصول إلى حماية هذه الشبكات ضد الانتهاكات والتدخلات وإلى كيفية منع أو التقليل من هذه المخاطر وصولا بمجموعة من التوصيات والمقترحات.**

*الكلمات الافتتاحية*: **الشبكات اللاسلكية، أمن الشبكات اللاسلكية، المخاطر والتهديدات، برتوكولات التشفير، حماية الشبكات.**

## 1. مقدمة

تعتبر الاتصالات والشبكات اللاسلكية من المكونات الأساسية في الحياة المعاصرة والتي تتكون من ثلاثة أنواع رئيسية وهى شبكات المناطق الكبيرة MAN وشبكات المناطق المحلية LAN وشبكات المناطق الشخصية PAN وقد شهدت تقنيات الاتصالات اللاسلكية تطورا كبيرا في العقدين الماضيين، لما توفره هذه الشبكات من سهولة الاتصال والحرية الكبيرة التي توفرها للمستخدمين فى التنقل والانخفاض المتواصل فى الاسعار والعديد من المزايا الإنتاجية، وكذلك بسبب زيادة إمكانية الوصول إلى مصادر المعلومات، هذا الانتشار الواسع النطاق أسفر إلى تحفيز الشركات الرائدة في صناعة تكنولوجيا المعلومات على توفير ودعم الأجهزة الحديثة بالمواصفات التقنية اللازمة والمنتجات اللاسلكية لتتوافق مع متطلبات وخصائص تلك الشبكة، ومع ذلك فإن هذه التكنولوجيا اللاسلكية تتعرض إلى تهديدات جديدة من قبل المخترقين.

ومع توسع استخدامات شبكة الانترنت بين المستخدمين، ستنتشر المخاطر الامنية والاختراقات خصوصا فى القطاعات التجارية والصناعية والعسكرية.

استلمت الورقة بالكامل في 27 مارس 2018 وروجعت في 2 إبريل 2018 وقبلت للنشر في 4 إبريل 2018

ونشرت ومتاحة على الشبكة العنكبوتية في 6 إبريل 2018

وتشير الاحصائيات ان أغلب مستخدمي الشبكات اللاسلكية لا يعيرون اهتماما كبير في تأمين هذه الشبكات كاستخدام كلمات مرور قوية وأنظمة تشفير وما الى ذلك، لذلك برزت الحاجة لفهم أمن المعلومات في الشبكات اللاسلكية، وعن أهمية تحقيق الامن في مجال الشبكات اللاسلكية، وايجاد الحلول التقنية لتفادى الاعتداءات والاختراقات وتطبيق الاجراءات الوقائية، و للحد من هذه المخاطر عملت المنظمات على تطوير مختلف معايير التشفير التي تقلل من هذه المخاطر إلى مستوى يمكن التحكم فيه، وهناك العديد من الأبحاث حول دراسة عيوب ونقاط الضعف في هذه الشبكات [1،2].

## 2. أسباب نقاط ضعف الشبكات

عند التوجه الى تأمين الشبكات اللاسلكية يجب تحديد نقاط الضعف والتي تتكون من أربعة عناصر أساسية [3] :

1- نقل البيانات : Single-frequency radio
2- نقاط الوصول : Access point
3- الاجهزة : Computer, Mobile, ..etc
4- المستخدمين : Users

ويهدف البحث على الإجابة لبعض التساؤلات حول الوضع الأمني فى الشبكات وكيفية تحقيق أداء أمني مقبول وهذه التساؤلات:

1- ما هو مستوى التهديدات والمخاطر التي تواجه الشبكات اللاسلكية ؟
2- ماهي النتائج المترتبة من وقوع الاعتداء ؟
3- ماهي أفضل الطرق لحماية الشبكة من الاعتداءات؟

## 3. مفهوم الامن في الشبكات اللاسلكية

يقصد به حماية أنظمة المعلومات ضد أى وصول غير مرخص به أو حماية تعديل البيانات أو المعلومات المحفوظة أو أثناء حفظها، وكذلك حمايتها أثناء معالجتها أو نقلها، كما أن أمن الشبكات اللاسلكية مقصود به الحماية ضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، ويتمثل تحقيق الأمن في الشبكات اللاسلكية بتوفير حماية الاتصالات بين مكونات الشبكة، وً حماية البيانات للشبكات اللاسلكية في النقاط التالية [4] :

**موثوقية البيانات**: وتشمل ضمان استلام الرسائل من مصادر موثوقة.
**سرية البيانات**: تعني إخفاء البيانات عن الأطراف غير المصرح لهم بالاطلاع عليها.
**التصريح و تحديد الصلاحيات**: السماح فقط لمن يصرح له بالمشاركة في أعمال الشبكة.
**ضبط الوصول**: منع الوصول لغير المصرح لهم باستعمال موارد الشبكة.
**صحة البيانات**: وهي التأكد من أن البيانات سليمة ولم يتم تخريبها أو تحويرها أثناء تناقلها خلال الشبكة.
**مكافحة الإنكار (المسئولية)**: التأكد بأن مرسل البيانات والمعلومات قد حصل على إثبات بوصول البيانات إلى المرسل إليه، وأن مرسل البيانات قد حصل على إثباتٍ لتسلم المستقبل لرسالته، أو على أن المستقبل قد حصل على إثباتٍ لهوية المرسل.

ويمكن تصنيف الوسائل الأمنية[5] القابلة للتطبيق في الشبكات اللاسلكية إلى وسائل وقائية ووسائل كاشفة وأخرى تفاعلية.
وتختلف درجة الأمن المتوفرة في الشبكات اللاسلكية بناء على عدة عوامل أساسية[6] نذكر منها:

1- نوع البروتوكولات المستخدمة في إدارة الشبكة.
2- المتطلبات الأمنية المستخدمة في الشبكة.
3- عدد نقاط الدخول المكونة للشبكة، خصائصها.
4- محطات المراقبة في الشبكة.
5- طبيعة المنطقة التي تم فيها تركيب الشبكة.
6- احتمالات حدوث الاعتداءات.

## 4. تطبيق الخصائص الأمنية للشبكات

يقدم النموذج المرجعي ترابط الأنظمة المفتوحة (OSI) Open Systems Interconnect الموضح في الجدول رقم (1) والذي ابتكرته منظمة المعايير الدولية (ISO) International Organization for Standardization توصيفاً نظرياً لتصميم بروتوكولات الشبكات (الاتصالات) الحاسوبية، حيث يقوم هذا النموذج بتقسيم وظائف الاتصال المختلفة إلى سبعة طبقات مختلفة تعمل بشكل مستقل عن بعضها البعض، وينعكس اسلوب التصميم وفق مبدأ الطبقات بشكل مباشر على كيفية تطبيق الخصائص الأمنية.

الجدول 1. يبين ترابط الأنظمة المفتوحة Open Systems Interconnect

| بروتوكول TCP / IP | نموذج OSI |
|---|---|
| | L7 Application طبقة التطبيقات |
| Application طبقة التطبيقات | L6 Presentation طبقة العرض |
| | L5 Session طبقة الجلسة |
| Transport طبقة الارسال | L4 Transport طبقة الارسال |
| Internet طبقة الانترنت | L3 Networks طبقة الشبكة |
| Host – Network | L2 Data link طبقة وصلة البيانات |
| | L1 physical الطبقة الفيزيائية |

## 5. المخاطر الامنية

تتعرض الشبكات اللاسلكية إلى أشكال مختلفة من الاعتداءات الأمنية التي يمكن تصنيفها من زوايا متعددة، وتصنف الاعتداءات من حيث نشاطها إلى نوعين اعتداءات سلبية وأخرى نشطة[7،8]:

### أ. *الاعتداءات السلبية: Passive Attack*

وتتمثل الاعتداءات السلبية بالاطلاع على البيانات فقط دون إجراء تخريب أو تحوير فيها، فتتم باستخدام برمجيات تقوم بالتقاط Capture فريمات الشبكات اللاسلكية Probes ثم يقوم بتحليلها Analyzing وذلك بناء على بعض المعطيات المسبقة ورقم القناة ونوع المعيار اللاسلكي ومن أهم التقنيات المستخدمة في الهجوم السلبى مثل Sniffing ولا يمكن تفادى هذا النوع من الهجوم إلا بواسطة تشفير البيانات المرسلة.

### ب. *الاعتداءات النشيطة Active Attack*

وتتمثل الاعتداءات النشيطة بتخريب وتحوير وتعديل البيانات مثل التلاعب فى الملفات، أو إضافة أو حذف غير مرخص به للملفات، أو استغلال عملية الاتصال، ومن أهم التقنيات المستخدمة في الهجوم النشط الغش Spoofing والاختطاف Hijacking وهذا النوع من الاعتداء يتطلب العديد من وسائل الحماية مثل الجدار الناري والحماية من الفايروسات، وبعض الاعدادات داخل المنظومة الالكترونية.

## 6. بعض الأساليب المتبعة لغرض الاختراق

### أ. *الالتقاط: Hands shake*

ويقصد بها المصافحة وهى حوار ما بين المستخدم وRouter لكى يتم المصادقة على عملية الارتباط ، والمخترق يستلزم التقاط نوع من الحزم Packets أثناء هذه المصافحة، وذلك بالتصنت على الخط بعد تحديد الهدف وهو Router، وبالتشويش على الخط بغرض اعادة المصافحة ما بين المستخدم و Router، وعندما ينجح التشويش تتم اعادة محاولة المصافحة تقوم بالتقاط الحزم التي يحتاجها المخترق من هذه العملية والتي تستغرق لحظات فقط على حسب عدد المستخدمين فى الشبكة المراد اختراقها.

### ب. *هجمات نقاط الاتصال الوهمية: Rouge Access Point*

يصنف هذا النوع من ضمن مفهوم الهندسة الاجتماعية، وتتم عن طريق فصل الاتصال بين المستخدمين و Router حتى لا يستطيعوا الاتصال بالشبكة اللاسلكية، وذلك باستدراجهم بشبكة وهمية تم انشأها، حيث يعتمد القراصنة إلى خلق ونشر شبكة لاسلكية وهمية غير مؤمنة للإيقاع بضحاياهم، والغرض منها التجسس على المعلومات التي تمر عبر الشبكة من كلمات مرور ورسائل، حيث تشير الدراسات إلى أن الرغبة الجامحة لدى المستخدمين فى الحصول على اتصال بشبكة الانترنت بالمجان تتسبب في وقوعهم ضحايا لتلك الهجمات.

### ج. *التخمين: Guess*

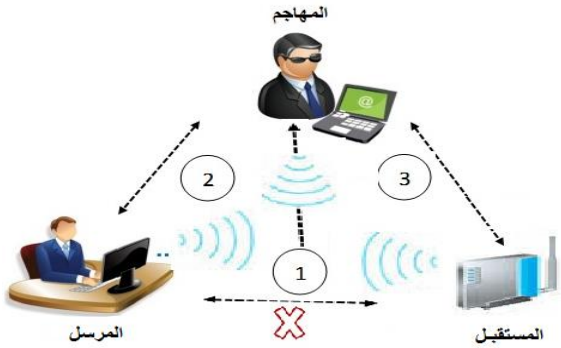
يستخدم هذا النوع من الاختراقات فقط على أجهزة Router والتي تمتلك خاصية WPS المفعلة به، وهذه الطريقة لاتحتاج الى التخمين على أي حزم لالتقاطها، وإنما تتم على تجريب الارقام المحتملة والتي تتكون من 8 أرقام وتدوم مدة التخمين عليها بضع ساعات على حسب Pin، وبعد الحصول على البين الصحيح يتم استرجاع كلمة المرور عن طريقه.
وتحدث هجمات تخمين كلمة المرور عندما يتم مهاجمة الحساب Account بشكل متكرر، وتتم هذه الهجمات عن طريق إرسال كلمات المرور المحتملة إلى الحساب (Account ) بطريقة منتظمة ، وتستخدم لغرض الحصول على كلمات المرور لاستخدامها فى الوصول أو التعديل ، وهناك نوعان من هجمات تخمين كلمة المرور وهما ( الهجوم العنيف – هجم القاموس ) .

### د. *هجمات القيادة أو التجول: War driving*

وتتم عن طريق تجول المخترقين بين الأحياء ومؤسسات الأعمال بمركباتهم للكشف عن الشبكات الغير مؤمنة من خلال أجهزة وبرامج صممت خصيصاً لهذا الغرض ومتاحة بحرية على شبكة الانترنت مثل برامج [9] Ekhau Heat Mapper، وفور الحصول على أي من هذه الشبكات اللاسلكية الغير مؤمنة يقوم المخترق باختراق تلك الشبكة والأجهزة وقواعد البيانات المرتبطة بها واختلاس ما تحتويه من بيانات ومعلومات.

ذ. *هجمات الرجل الوسيط:* Man in the Middle Attack

الرجل الذى في المنتصف ( الرجل الوسيط ) يتعامل مع المستقبل وكأنه المرسل، ومع المرسل كما وأنه المستقبل، يستطيع المخترق إعادة توجيه الضحية إلى موقع شبيه بالموقع الذى يستخدمه وذلك من أجل إدخال بيانات الضحية الشخصية والاحتيال عليها، وبشكل عام يمكن للمهاجم اعادة توجيه تبادل البيانات ، ويستخدم هذا الهجوم على سرقة البيانات والمعلومات التى تمر على الشبكة ، ويتم ذلك بقراءة كل ما يمر فى الشبكة واختلاس ونسخ جميع الحزم الإلكترونية الصادرة من وإلى جهاز المستخدم والتى تمر عبر الشبكة اللاسلكية كما في الشكل (1)، ومن تم تحليلها للوقوف على ما تحتويه من بيانات التي يمكن الاستفادة منها ككلمات المرور للحسابات كما يمكن اختلاس بيانات البطاقات الائتمان ونسخ الصور والمحادثات وما إلى ذلك من معلومات، وهى من أشهر الاعتداءات على الشبكات نظراً لسهولة تنفيذها وعدم الحاجة لتمتع مرتكبها بأي خلفية أو مهارة تقنية متقدمة [10].




شكل (1). يوضح الرجل الوسيط

المهاجم ينتحل شخصية المرسل وفي نفس الوقت شخصية المستقبل لأخذ ما يرغب فيه من بيانات.

ر. *الشبكات المخصصة:* Ad-Hoc Network

عندما يقوم المستخدم باستعمال جهاز الحاسوب في العمل ويتصل بالشبكة السلكية بعمله ونفس الوقت يمكن الاتصال اللاسلكي بجهازه بما يسمي بشبكة الند للند Ad Hoc [11] ، والتي عادة ما تكون هذه الأنواع من الشبكات قليلة الحماية ، فإنه يفتح بابا لآخرين لإمكانية التحايل والاتصال لاسلكيا بجهازه وبذلك يجعل من نفسه بوابة لاختراق الشبكة.

فمن الأفضل عند الاتصال بأي شبكة هو تعطيل منافذ الاتصال الأخرى الموجودة خصوصا اللاسلكية مثل Wi-fi و Bluetooth حتى لا يستطيع المخترقين استخدامها كثغرة الى الدخول للشبكة.

ز. *Rogue AP and Rogue Clients*

تعتبر نقاط الدخول أو ما يعرف Access point هي الاختراق الأمني الشائع في الشبكات اللاسلكية ، ويحدث ذلك الاختراق نتيجة وجود هذه الأجهزة في حيز اشارة الشبكة اللاسلكية مما يسمح لها بالتقاط اشارتها ، حيث يعتمد المخترق الى خلق ونشر شبكة لاسلكية وهمية للإيقاع بضحاياهم، فعندما يقوم المستخدمون بتشغيل الحاسوب، فإن جميع حركة المرور تمر من خلال نقطة الوصول اللاسلكية Rouge التي توفر التواصل مع مستخدمي الشبكة Network Interface Card (NIC)، وبالتالي تمكن من استنشاق حزمة لاسلكية.

م. *سوء معاملة العميل* Client Mis- Association

وتمم عملية الاختراق عندما لا يقوم مستخدمي الشبكات اللاسلكية بتغيير Service Set Identifier (SSID) الافتراضي لنقاط الدخول Access point مما يجعل إمكانية الاتصال بالشبكة بنفس الاسم في مكان أخر وبدون وجود توثيق أمر وارد، وهذا من الأساليب التي يتبعها المخترقون بما يسمي فخاخ الشبكات اللاسلكية، حيث يقوم المخترق بوضع نقطة وصول وهمية للدخول إلى شبكته ثم يقوم بعملية الاختراق ودخول الشبكة.

ن. *سرقة الهوية (خداع ماك* Identity Theft (MAC spoofing

وتحدث سرقة الهوية أو خداع عنوان تحكم وصول الوسائط Media Access Control address (MAC) عندما يقوم المخترق بعملية تزوير الفريمات Frames التي حصل عليها من عملية الـ Sniffing، ويتطلب هذا الاختراق عمل IP Spoofing تزوير عنوان IP وأيضا MAC Spoofing أي تزوير عنوان الـ MAC [12]، وكما نعلم أن الـ Frames هي أجزاء من البيانات على هيئة إطارات تحتوي على معلومات خاصة بالشبكة والبروتوكولات ومنافذها وتحتوى أيضا على Source MAC الخاص بالجهاز المرسل و MAC Destination الخاص بالجهاز المستقبل، وبعد أن يقوم المخترق بالحصول على عناوين الـ MAC والـ IP، فإنه يستطيع خداع السيرفر والأجهزة الأخرى بإرسال فريمات مزورة تحتوي على عنوان أحد الأجهزة الموجودة على الشبكة بحيث تستقبل الأجهزة الاخرى كل شي منه دون شك، وبهذه الطريقة يستطيع المخترق التواصل مع أي جهاز على الشبكة، وتوجد عدة برامج لديها القدرة على استنشاق الشبكة لتسهيل المهاجم على كيفية الحصول على عنوان MAC [13].

هـ. *الحرمان من الخدمة* Denial of service

يحدث هجوم الحرمان من الخدمة أو الخدمة الموزعة عندما يقوم المهاجم بحجب شبكة الحاسوب وتصبح غير متوفرة لمستخدميها، بمعنى حرمانهم من الخدمة التي تقدمها الشبكة كما في الشكل (2)، وتعتمد هذه الهجمات على إساءة استخدام البروتوكولات التي تتمثل المصادقة الموسعة، وتعتبر الشبكات اللاسلكية عرضةً لإيقاف الخدمة Denial of Service بسبب التشويش اللاسلكي، على سبيل المثال الحالة التي يقرر بها مستخدم شبكة أخرى إعداد تجهيزاته اللاسلكية لتعمل ضمن نفس القنوات الراديوية المستخدمة في الشبكة الاخرى، وسترسل هذه الشبكة نفس معرّف مجموعة الخدمات SSID الخاص بالشبكة الاخرى، ومن أهم أنواع الهجوم من هذا النوع هو استهلاك الموارد الحسابية وتعطيل مكونات الشبكة المادية


وتعطيل معلومات التوجيه.

شكل (2). يوضح هجوم الحرمان من الخدمة

و. *حقن الشبكة* Network injection

في هجوم حقن الشبكة، يمكن للمهاجم الاستفادة من نقاط الوصول التي تسمح بمرور البيانات عند الازدحام دون عرضها على عملية الترشيح أو الفلترة خاصة عند عملية الارسال، حيث يقوم المهاجم بعملية حقن وهمية وإعادة الاعدادات للشبكة والتي بدورها تعمل على إعادة الموجهات والمفاتيح، ومحاور الذكاء. وبالتالي يمكن اسقاط الشبكة بالكامل ، وهذا الامر يتطلب إعادة التشغيل أو حتى إعادة برمجة جميع أجهزة الشبكات الذكية.

## 7. أنواع من برتوكولات الحماية للوصول للشبكات اللاسلكية

### أ. بروتوكول الوصول *WEP: Wired Equivalent Privacy*

لقد ارتبط مفهوم سرية الشبكة اللاسلكية بمصطلح السرية المكافئة للشبكة السلكية WEP، وهو جزء من معيار IEEE 802.11 والهدف الرئيسي من هذه السرية هو تأمين الشبكات اللاسلكية بمستوى مماثل للسرية المتوفرة في الشبكات السلكية، وحماية الشبكة اللاسلكية بتحديد تصاريح المخولين للدخول للشبكة، كما يتم استعمال كلمات مرور ذات طول 64 بت أو 128 بت.

وعند استعمال برتوكول WEP فإن البيانات التي تمر فى الشبكة يتم تشفيرها باستعمال مفتاح ثابت لا يتغير يمتلكه المستخدم ويخزن في Router، ولكن يبقى هذا التشفير ضعيف لحماية الشبكات اللاسلكية لانه سهل كسر تشفيره.

كما أن برتوكول WEP لا يتضمن أي نظام لإدارة مفاتيح التشفير وكانت الوسيلة لتوزيع مفاتيح التشفير تتطلب ادخالها يدويا، مما ساهم الى العديد من الاختراقات على الشبكات التى تستعمل هذا البرتوكول.

### ب. بروتوكول الوصول *WPA/WPA2: Wi-Fi Protected Access*

وهو طريقة تشفير تستند الى معايير IEEE 802.11i في هذا البرتوكول يتم تغيير المفتاح الذى يقوم بتشفير البيانات كل 30 ثانية أو حسب اختيار المستخدم للمدة التي يتوجب عليه تغيير المفتاح والذى يكون لدى جهاز Router والمتصلين بالشبكة.

وبالنسبة لبرتوكول التشفير WAP2 فهو يقوم بتأمين حماية قوية للبيانات وله مستوى عالي من الحماية وكلا النوعين من التشفير يستعملان كلمات مرور تصل الى 256 بت، ولكن بالإمكان فك تشفيرهما بطريقة تخمين كلمة المرور وهذا يتطلب بعض الوقت على حسب طول ومكونات الكلمة السرية المستخدمة لحماية الشبكة اللاسلكية .

لقد تم تصميم بروتوكول WPA و WPA2 للعمل مع أو دون وجود خادم لإدارة مفاتيح التشفير ، في حال غياب خادم إدارة مفاتيح التشفير فإن جميع المحطات ستستخدم "مفتاح تشفير مشترك مسبقاً Pre-Shared Key (PSK)، ويعرف بروتوكول WPA2، وعند استخدام الخادم لمفاتيح التشفير ببروتوكول WPA يتطلب بروتوكول WPA2 وجود خادم يعمل بمعايير IEEE 802.1X لتوزيع مفاتيح التشفير، ومن أهم التطويرات المضمنة في بروتوكول WPA2 مقارنة بسلفه WEP هو إمكانية تبادل مفاتيح التشفير ديناميكياً بواسطة بروتوكول حماية أو سلامة مفاتيح التشفير المؤقتة (Temporal Key Integrity Protocol –TKIP).

### ج. بروتوكول الوصول *WAPS: Wi-Fi Protected Setup*

وهو النسخة المعتمدة من بروتوكول WPA والذي يشكل جزءاً من معيار IEEE 802.11i للشبكات اللاسلكية وهى عبارة عن خاصية في أجهزة Router تمثل معيار لأمن الشبكات ، ليسهل على المستخدم عملية حماية الشبكة من اعتداءات المخترقين وكذلك تسهيل اعداد الشبكة اللاسلكية بطريقة سهلة دون المرور على اعدادات Router المعقدة، وان عملية تفعيل هذه الخاصية يرفع من سرعة الاتصال مع الشبكة اللاسلكية، وينصح بعدم تفعيل خاصية WPS فى Router لإنها تستعمل البين PIN حتى يتمكن المستخدم من الارتباط مع الشبكة اللاسلكية والبين PIN عبارة عن 8 أرقام فقط وعملية التخمين عليه سهلة تتطلب فقط ساعات معدودة للحصول عليه لإنه يبقى ثابت ولايمكن تغييره في أكثر أجهزة Router [14] والجدول رقم (2) يوضح المقارنة بين أنواع مفاتيح التشفير.

جدول 2. يوضح المقارنة بين أنواع مفاتيح التشفير

| Encryption التشفير | Attributes الصفات | | | |
|---|---|---|---|---|
| Keys | Encryption Algorithm خوارزمية التشفير | IV-Size حجم التهيئة | Encryption Length طول مفتاح التشفير | Integrity Check ألية اختبار السلامة |
| WEP | RC4 | 24 Bits | 40/104 Bits | CRC-32 |
| WPA | RC4,TKP | 48 Bits | 128 Bits | CRC-32 |
| WPA2 | AES-CCMP | 48 Bits | 128 Bits | AES-CCMP |

1- WEP : يجب عدم استخدام هذا النوع من مفتاح التشفير واستبداله بمفاتيح WPA, WPA2

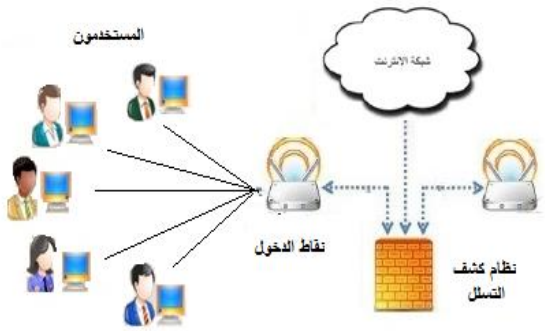
2- WPA ,WPA2 : تتضمن هذه المفاتيح دمج الحماية ضد التزوير واعادة الهجوم.

## 8. طرق حماية الشبكات اللاسلكية

هناك عدة طرق لحماية الشبكة اللاسلكية من الاختراقات والاعتداءات أهمها:

### أ. برامج مراقبة بيانات الشبكة : *Packet Sniffers*

وهى طريقة فعالة لمراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، مثل برامج الجدران النارية (Firewall) وأنظمة أنظمة كشف التسلل (Intrusion Detection Systems) حيث تستخدم هذه الأنظمة في عملية تعقب وكشف عمليات التسلل الغير مصرح بها للشبكة كما في الشكل (3) وذلك من خلال تجميع البيانات الداخلة والخارجة [15]، وهي طريقة ممكن أن تكون مفيدة في الكشف عن محاولات التسلل عبر الشبكة، وكذلك يمكن استخدامها لتحليل مشاكل الشبكة وتصفية وحجب المحتوى المشكوك فيه من الدخول إلى الشبكة.




شكل (3.) يوضح أنظمة كشف التسلل

### ب. أدوات فحص نقاط الضعف: *Vulnerability Scanners*

تستخدم برامج فحص نقاط الضعف من أجل الوصول إلى أي نقاط ضعف قد يكون وجودها مضر للشبكة والأنظمة المتواجدة عليها، وذلك باستخدام أدوات يتم تحديثها باستمرار من أجل الوصول إلى حماية أكثر، بالإضافة إلى القيام بفحص الشبكة بطريقتين، الطريقة الأولى هي القيام بتشغيل برامج الفحص بشكل داخلي للتأكد من أن الشبكة لا تظهر أي نقاط ضعف داخلية، وبعد ذلك القيام بتشغيل برامج الفحص بشكل خارجي لمعرفة إن قام أي مخترق بتشغيل برامج فحص الشبكة.

*ج. الإعدادات الافتراضية: Virtual Settings*

يتم استخدامها من خلال التأكد من الإعدادات الافتراضية للشبكة مثل كلمات المرور الافتراضية الخاصة بالخدمات أو الأنظمة التي يتم استخدامها، بالإضافة إلى الخدمات التي لا تحتاجها أو البروتوكولات التي لا تستخدم أي نوع من أنواع التشفير، فالإعدادات الافتراضية عادةً ما تكون باب خلفي للمخترقين.

*د. مراقبة تحديثات الشبكة: Patching*

وذلك بالقيام بتحديث الانظمة أو الخدمات باستمرار، والبرامج التي يتم استخدامها على الانظمة وتحديث كل شيء ليكون Up- to Date .

*ذ. اختيار كلمات المرور: Password*

يجب استخدام كلمات مرور قوية للخدمات والأنظمة، فالكلمات التي تتكون من حروف فقط من السهل اختراقها وذلك بجعل كلمات مرور قوية مكونة من حروف وأرقام ورموز، ويجب أن يملك كل مستخدم للشبكة كلمة مرور خاصة به وعدم استخدام كلمة مرور مشتركة، وعدم استخدام نفس كلمة المرور لكل الانظمة والخدمات.

*ر. الصلاحيات: Authorities*

ويقصد بها عدم اعطاء أي مستخدم صلاحيات أكثر مما يحتاجها، فمثلاً لا يجب أن يعطي مستخدم عادي حساب Router أو Admin للخدمة أو الأنظمة، ويجب أن يعطي كل مستخدم صلاحيات تناسب مهمته أو وظيفته أو استخدامه.

*ز. التوثيق: Documentation*

وهي عملية توثيق جميع المعلومات والبيانات وتوثيق بنية الشبكة والخدمات والبرامج والإعدادات التي تم استخدامها.

*م. الاستخدام الأساسي:*

يجب القيام بمراقبة الأنظمة والخدمات أثناء الاستخدام العادي لها، فمثلاً كم يتطلب التشغيل العادي لحجم الخدمات والأنظمة.

*ن. التنبيهات: Alerting*

ويتم ذلك بتفعيل أنظمة التنبيهات في كل شيء يتم استخدامه داخل الشبكة، فكل تنبيه يدل على اكتشاف أي شيء غير معتاد يحدث في الشبكة، فهذه الطريقة جيدة للتصرف السريع عند حدوث أي شيء Out of Ordinary.

*هـ. ترشيح العناوين: MAC Filtering*

يعرف العنوان (MAC) بأنه العنوان المادي، وهو معرف فريد لكل جهاز في الشبكة، ويعني مصطلح ترشيح العناوين بإدخال قائمة بالعناوين (MAC Addresses) الموجودة في الشبكة يدويا وبإعداد الموجه (Router) ليسمح فقط بتوصيل هذه العنوانين المحددة عبر الشبكة اللاسلكية، ومن أهم البرامج المتاحة لتغيير العنوان MAC من محولات الشبكة هو برنامج Ether changer [16].


الشكل (4) يوضح ألية التشفير

*و. التشفير: Encryption*

يتم باستخدام بروتوكولات تشفير خاصة بالشبكات اللاسلكية وتعمل هذه البروتوكولات باستخدام مفتاح مشترك بين المستخدمين ونقاط الدخول، ومن ثم يتم استخدام هذا المفتاح لتشفير وفك تشفير البيانات بينهم كما في الشكل رقم (4)، وهذا يوفر قدر كاف من الأمن للشبكات، والتشفير هو تغيير البيانات كي يتعذر قراءتها من أي شخص ليس لديه مفتاح لفك شفرة تلك البيانات، الأمر الذى يجعل المعلومات في الشبكة غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى الشبكة، ومعظم الموجهات اللاسلكية ونقاط الوصول لديها ألية التشفير [17].

أهداف التشفير:

- السرية Confidentiality
- النزاهة Integrity
- المصادقة Authentication
- عدم الانكار Non-Repudiation

## 9 . النتائج والتوصيات

من خلال ما تم عرضه في البحث لاحظنا زيادة التهديدات والاعتداءات المختلفة التي تتعرض لها الشبكات اللاسلكية وكذلك صعوبة اكتشاف أو تتبع التغيرات التي تحدث على الشبكات اللاسلكية، بسبب بيئة اتصالاتها المفتوحة، وكثرة عدد نقاط الدخول إليها، وعلى كيفية تفادى هذه الأخطار ومنعها أو التقليل منها من خلال بعض الاجراءات والأنظمة والبرامج التي يمكن من خلالها مكافحة ومواجهة هذه المخاطر، وبناء على ذلك تم التوصل الى بعض النتائج والتوصيات:

*أ. الاستنتاجات:*

لقد توصلت هذه الدراسة إلى مجموعة من النتائج والتي تعتبر في مجملها خلاصة البحث:

1. لا يوجد "حل أمني قياسي" يلائم جميع الشبكات اللاسلكية فمن الضروري تحديد المتطلبات الأمنية بوضوح لأن الحلول الأمنية تعتمد على خصوصية كل حالة.
2. قد تتوقف الشبكة اللاسلكية عن العمل نتيجة هجمات متعمدة لإيقاف عمل الخدمة، أو وجود برمجيات مؤذية، كما أن الشبكة قد تتعطل دون قصد بسبب وجود نقاط خفية أو مشاكل تشويش.
3. عدم التمكّن من اكتشاف الأسباب الحقيقية وراء هذه المشاكل إلا من خلال مراقبة سير البيانات عبر الشبكة.
4. قلة الوعي بأهمية امن المعلومات من قبل مستخدمي ومشغلي الأنظمة وعدم توفر الخبرة في هذا المجال قد يؤدى إلى زيادة الاعتداء.
5. صعوبة التحقق من أمان الشبكة بشكل انفرادي بسبب كثرة الخدمات التي تقدمها الشبكات.
6. إذا تم اختراق الشبكة فإن العديد من المستخدمين يمكن الوصول إليهم.
7. هناك إهمال من بعض الافراد والمؤسسات في إجراءات الحماية لتفادى هذه الاعتداءات.

*ب. التوصيات :*

1. تركيب أنظمة كشف التسلل IDS وتثبيت أحدث برامج الحماية مثل جدران الحماية النارية وبرامج مكافحة الفيروسات داخل الشبكة.
2. تدريب وتثقيف المستخدمين حول آمن السلوك اللاسلكي لتكون فعالة، ويجب تكرار التعليم بشكل دوري.
3. الحد من الوصول المادي للشبكة لمنع وصول Sniffers غير المرخص.
4. استخدام كلمة مرور قوية ومعقدة تكون خليط من الأرقام والحروف وكذلك الرموز، وتغييرها بشكل منتظم.

5. تشفير البيانات المخزنة على خوادم الشبكة، وكذلك تشفيرها قبل تراسلها لمنع قراءتها من Sniffers.
6. إيقاف تشغيل الشبكة اللاسلكية الخاصة في حالة عدم استخدامها، يقلل من مقدار الاختراق، حتى لا يتمكن المخترقين من الوصول إلى أجهزة التوجيه اللاسلكي عند إغلاقه .
7. اختبار وظائف النظام للتأكد من أن الخدمات والموارد في متناول المستخدمين المخولين فقط.
8. إخفاء معلومات عنوان الشبكة من خلال التقنيات المختلفة، مثل ترجمة العناوين، للحماية من الخداع والاختطاف.
9. تطبيق البروتوكولات الأمنية مثل بروتوكول الوصول الآمن إلى الشبكة اللاسلكية WPA2 فهو الخيار الأمثل.
10. تطبيق المصادقة القوية والمناسبة والتحكم في الوصول، مثل MAC address filtering أو مصادقة المستخدم، مقابل خدمة الدليل لمنع هجمات مثل War driving.
11. السماح لأجهزة الحاسوب المخولة بالوصول للشبكة اللاسلكية عبر تفعيل قائمة المخولين والمعروفة بـ Access List في جهاز الاتصال بالشبكة (Router) من خلال تعريف عنوان كرت الشبكة للأجهزة المخولة الـ MAC Address .
12. تغيير اسم الشبكة الافتراضي وإخفاء نشر عنوان الشبكة (SSID) وكذلك تعطيل المعرف آلية البث للشبكة حتى لا يلتقطها المخترقين الباحثين عن اتصال مجاني بالإنترنت على أن يتم تعريفها بأجهزة المستخدمين المخولين يدوياً.
13. إطفاء جهاز الاتصال بالشبكة (Router) عند عدم الاستخدام لفترة طويلة لتقليص فرص اختراق الشبكة.
14. عدم الانجراف وراء فتح الروابط المجهولة المصدر والغير موثوقة.
15. القيام بمسحٍ دوريٍ للترددات اللاسلكية لتجنب الهجمات المقصودة أو غير المقصودة.
16. عدم الافراط في زيادة طاقة الوصلات اللاسلكية لتجنب التشويش على الشبكات الأخرى.

## 10. الخلاصة

تعتبر الشبكات اللاسلكية من أهم القضايا في أمن المعلومات، وقد أدى انتشار هذه الشبكات الملحوظ إلى زيادة الاهتمام بتوفير الحماية الأمنية لهذه الشبكات، وذلك بسبب تزايد المخاطر والتهديدات لأمن مستخدميها سواء أفراد أو جهات حكومية أو شركات أو جهات أمنية وعسكرية، وعلى الرغم أنه من المستحيل القضاء تماما على جميع المخاطر المرتبطة بالشبكات اللاسلكية وخصوصاً في ظل الطبيعة العشوائية 8للشبكات، ومع عدم وجود حل أمني قياسي يلائم جميع الشبكات اللاسلكية. أصبح من الضروري تحديد المتطلبات الأمنية بوضوح لأن الحلول تعتمد على خصوصية كل حالة فمن الممكن تحقيق مستوى معقول من الأمن العام من خلال تقييم وإدارة تلك المخاطر، وأن هناك حاجة ملحة لتطوير بروتوكولات وتقنيات أمنية تعمل ضمن موارد الشبكة المحدودة دون أن تستنزفها.

وقد عرضنا في هذه الورقة أشكال الاعتداءات التي تهدد أمن الشبكات اللاسلكية، ونقاط الضعف المرتبطة بكل مكونات التكنولوجيا الأساسية من الشبكات اللاسلكية (المستخدمين، نقاط الوصول)، ووصف مختلف التدابير المتاحة التي يمكن استخدامها للتخفيف من تلك المخاطر وتحديد الوسائل الدفاعية التى تختص بتوفير الحماية من بعض هذه الاعتداءات.

## المراجع


[1] E. Tews, R. P. Weinmann and A. Pyshkin, "*Breaking 104 bit WEP in lessthan 60 seconds*," IACR Eprint Server, http://eprint.iacr.org/ 2007/120.pdf , number 2007/120, Accessed April 1, 2007.

[2] Anil Kumar Singh, Bharat Mishra and Sandeep Singh "*WLAN Security Flaw: Cracking 64 bit WEP Key*," IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6, pp. 296-299, Nov. 2010.

[3] Hassan Tahir, Syed Asim Ali Shah**,** Wireless Sensor Networks - A Security Perspective**.** Multi topic Conference, INMIC 2008. IEEE International

[4] Tanveer A. Zia, An overview of wireless sensor networks and their security issues. Advanced Networks Research Group, School of Information Technologies, 2010, University of Sydney

[5] Michael Healy, Thomas Newe, Elfed Lewis, Security for Wireless Sensor Networks: A Review, IEEE Sensors Applications Symposium New Orleans, LA, USA – 2009

[6] Ali Nur Mohammad Noman, A Generic Framework For Defining Security Environments Of Wireless Sensor Networks, 5th International Conference on Electrical and Computer Engineering ICECE 2008, Dhaka, Bangladesh

[7] Panu Hämäläinen, Mauri Kuorilehto, Timo Alho, Marko Hännikäinen, Timo D. Hämäläinen: Security in Wireless Sensor Networks: Considerations and Experiments. SAMOS 2006

[8] T.Kavitha, D.Sridharan, Security Vulnerabilities In Wireless Sensor Networks: A Survey, Journal of Information Assurance and Security, Vol. 5, 2010

[9] "NetSpot: WiFi Site Survey Software for MAC OS X & Windows"

[10] Kaufman, Charlie; Perlman, Radia; Speciner, Mike. Network Security: Private Communication in a Public World, Second Edition. Prentice Hall PTR. p. 169. ISBN 978-0-13-046019-6

[11] Margaret Rouse. "Encryption". TechTarget. Retrieved 26 May 2015.

[12] Penetration Tester's Open Source Toolkit by Johnny Long and others, Syngress Publishing, Inc., 2006, page 301.

[13] "SMAC 2.0 MAC Address Changer". klcconsulting.com. Retrieved 2008-03-17.

[14] مقال بعنوان تقنيات التشفير في الشبكات اللاسلكية، جميل طويله، 27 نوفمبر 2015.

[15] مقال بعنوان مصائد محترفي الشبكات، Isecur1ty، 11 سبتمبر 2016

[16] Wireless Security Handbook by Aaron E. Earle, Auerbach Publications, 2006, pages 319- 320.

[17] International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 3, July, 2008 , 83