مجلة جامعة تشرين للدراسات والبحوث العلمية _ سلسلة العلوم الهندسية المجلد (28) العدد (1) 2006
Tishreen University Journal for Studies and Scientific Research- Engineering Science Series Vol. (28) No (1) 2006

تقانات أمن شبكات الاتصال اللاسلكية wlan

الدكتور علي عمران سليمان*

(قبل للنشر في 2006/5/18)

□ الملخّص □

إن شبكات الاتصال السلكية تعتمد على تمديد الأسلاك ضمن مجاري مطمورة وعليه يكون الوصول إليها من خلال الكشف على هذه المجاري بعمليات حفر أو كسر وهذا يجعل أمر ملاحظة ذلك سهل من قبل القائمين عليها.

بينما الشبكات اللاسلكية WLAN فتعتمد في ابسط حالاتها على محطتين واحدة للبث والثانية للاستقبال والمعروفة BSS وبعد إضافة نقاط الولوج AP وربطها مع بعضها لتشكل نظام DS المعروف.

حيث لن يكون هناك أسلاك " ما بين المستخدمين على الأقل " وتنتشر الموجات الكهرومغناطيسية في مجال تغطية المحطة ويمكن لمن يقع ضمن مجال التغطية الموصول أليها نظراً لعدم وجود مثل هذه الحماية الفيزيائية هذا تطلب الكثير من العمل لجعل المعلومات آمنة من التجسس في الوصول إليها .

هذه المشكلة تتطلب الكثير من العمل والاهتمام لتحقيق أكبر قدر من السرية.

تطرق البحث على بنية الشبكة والتدابير الأمنية المتوفرة وكذلك المتوقفة أهم نقاط الضعف وكيفية معالجتها.

تستخدم هذه الشبكات نظراً لأهميتها الاقتصادية وسهولة الاستخدام والتطوير وإعطاء حرية الحركة والتنقل ضمن المجال المعطي بالموجات

الكلمات المفتاحية:

نقاط النفاذ – الشبكات اللاسلكية – السرية – أمن الشبكات – بروتوكولات الشبكات اللاسلكية.

* مدرس، قسم الحاسبات والتحكم الآلي، كلية الهندسة الميكانيكية والكهربائية ،جامعة تشرين. اللاذقية – سوريا.

مجلة جامعة تشرين للدراسات والبحوث العلمية _ سلسلة العلوم الهندسية المجلد (28) العدد (1) 2006
Tishreen University Journal for Studies and Scientific Research- Engineering Science Series Vol. (28) No (1) 2006

Security of Wireless Local Area Network

Dr. Ali suleiman *

(Accepted 18/5/2006)

□ ABSTRACT □

Wired communication networks depend on wires that are, in general, buried underground. Reaching such wires would need digging, breaking, or other types of work, which are usually visible to those administrating the networks.

A WLAN constitutes in its basic form (known as BSS) of one broadcasting and one receiving stations. The addition of multiple access points (APs) forms a distributed system (DS). Wires in major parts of such networks are replaced with electromagnetic waves, which are prone to be accessed by non intended people. Tackling the security in this case is more complicated and requires more attention and efforts.

The research deals with network structure and different available and under-research security strategies. The main weak points of these strategies and how to handle them are covered too. WLANs are widely used because of their economical benefits and flexibility of development and access.

Key Words: IEEE 802.11, Ad – Hoc, Integrity Cheek Value, Challenge, Access Point, ISO/OSI, Extended Service Set, TKIP,ERP, Shared Key, Distribution System, Authentication, Wired Equivalent Privacy Protocol, Data Integrity, Service Set Identifier, Frame Check Sequence, BSS, Wi-Fi, WLAN ,

* **Assistant Professor, Department of Computer and Automation, Faculty Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.**

مقدمة عن أهمية البحث:

نظراً لأن الشبكات السلكية توضع ضمن مجارٍ مطمورة بشكل عام ضمن وخارج المباني تجعل أمر الوصول إليها (التجسس عليها أو اختراق أمنها) أمر غير بسيط حيث يحتاج ذلك إلى التنقيب والكشف عنها وملاحظة ذلك من قبل القائمين على أمنها. وعند الاعتماد على الشبكات اللاسلكية نجد سهولة في هذا الأمر نظراً لعدم وجود مثل هذه الحماية الفيزيائية حيث يمكن التقاط الإشارة من داخل مجال تغطية موجات محطة الإرسال وهذا ما يجعل أمر الأمن والأمان لاستخدامها هذا النوع مدعاة للشك نسبياً.

الأهمية الاقتصادية والتطويرية حيث لا يرتبط المستخدم لها بمكان ولا توجد مشكلة في إعادة ترتيب توضع المستخدمين ضمن المبنى الواحد أو ضمن المباني ولا تحتاج إلى المال المصروف في تحديد الأسلاك وطمرها وتثبيتها ولا سيّما من الأماكن التي يجب عدم التغير فيها مثل: المتاحف، الأماكن الأثرية، الجامعات، المطارات، محطات القطارات، المستشفيات، المباني الضخمة التي لم تؤخذ بعين الاعتبار قبل ذلك، الأماكن المتباعدة والتابعة للشركة المفصولة نفسها بمسافات واسعة، أو الجزر المعزولة بالمياه ....الخ ".

هذه الحرية في التنقل ضمن المجال المعطي بالموجات دون التأثير في قطع الاتصال وإعادة وصلة، وكذلك عدم الحاجة إلى إعادة ترتيب تمديد الأسلاك ونقاط الدخول إلى الشبكة السلكية، وهذا ضروري أكثر للجامعات التي لم تستقر أماكن توضع مستخدمي الشبكة "وإداراتها"وسيكون أفضل بالنسبة لكافة الجامعات القديمة التي لم تدرس شبكاتها عند التصميم والبناء " نظراً لعدم وجود مثل هذه الشبكات في حينها " حيث يتاح الولوج إلى المعلومات من أية مكان مرغوب ضمن مجال تغطية المحطات .. وقد يكون المخترق أحد أنواع عده نذكر منها:

1. Sniff : يوجد في حال تبادل المعطيات ك Email or Text document
2. Spoof: الدخول من خلال مفتاح خاطئ (مخادع) للوصول إلى المعطيات والمصادر.
3. Hijack: الوصول إلى المعطيات واستخدامها والعودة بها دون أن يشعر المستقبل باختطاف المعطيات.
4. Brute Force Attacker: استخدام برمجيات تشكل كلمات مرور بكل الاحتمالات وتجريبها للوصول إلى الكلمة الصحيحة.
5. Denial of service Attacker: تحميل المصادر حتى الشلل وبعدها يتم كشف هؤلاء ولكن الأمر يصبح متأخر.

وهنا يجب التنويه إلى قضية أهمية المعطيات هل هي كافية ليصرف hacker وقت للوصول إليها أم يكمن الخطر عندما يتم قيادة قاعدة بيانات وبالتالي نقل الأرقام المميزة للزبائن Personal Identification Number وأرقام المصادقة Transactions Number والتي تعطي Hacker إمكانية الوصول إلى حسابات الزبائن، ومثال آخر عند الوصول إلى ملفات المرضى لدي إحدى المراكز العلاجية يكون ذلك مربك.كما ويعالج هذا البحث بنية وتخصيص بروتوكولات هذه المواصفة IEEE 802.11 الموضوعة لشبكاتWLAN حيث نتطرق في الفقرات القادمة على المفاهيم والبنية المكونة لـ WLAN وطرائق قياس الأمن، وأهم نقاط الضعف والتحسينات الأمنية عليها.

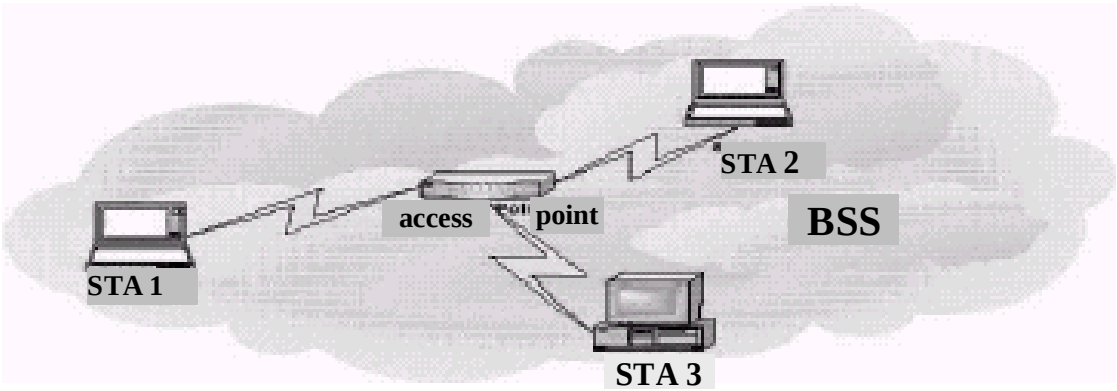
وعن طريقة البحث تم دراسة ما هو متوفر حالياً من خلال النشرات والأبحاث المنشورة والتركيز على النقاط التي أمكن التطوير بها بحث أصبح من الممكن الاستفادة منها وتبنيها ضمن مؤسساتنا والوصول إلى أفضل الممكن حالياً.

النتائج والمناقشات:

- **بنية الشبكة WLAN.**

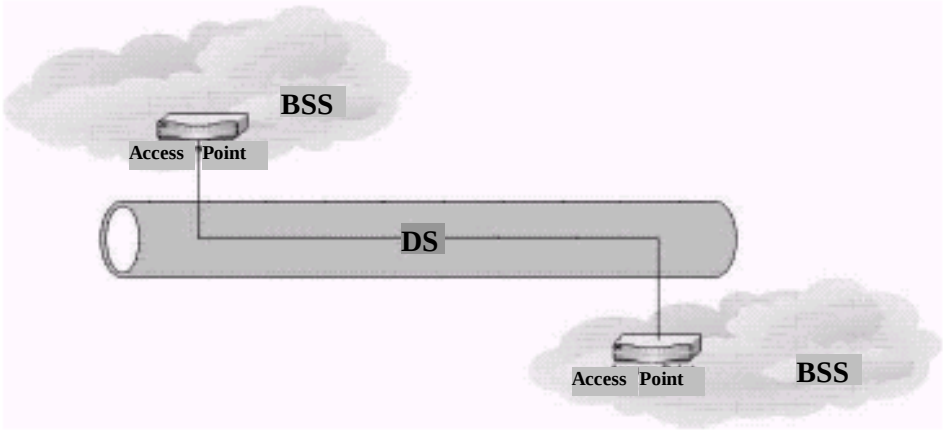
سنعرض هيكلية WLAN وبعض البروتوكولات المستخدمة معها.حيث تتألف الشبكة على الأقل من زوج من الاتصالات والمعرفين بالمحطات (STA) station وذلك من خلال استخدام بطاقة اتصال خاصة بهذا النوع من الشبكات ويتم تبادل المعطيات عبر الموجات الكهرومغناطيسية المتبادلة ما بين المحطتين وعلى مجال تغطية هذه الموجات والذي يدعى (BSS) Basic Service Set وهو المجال الذي يتم فيه الاتصال بشكل مباشر ما بين محطتين والتي تعرف بشبكات Ad – Hoc. [1]

بشكل عملي تملك البنية التحتية للشبكة ما يدعى بنقاط النفاذ AP (Access Point) في كل BSS توجد نقطة واحدة والتي نراها في الشكل (1) البنية التحتية للشبكة.



الشكل (1) البنية التحتية للشبكة

تخدم AP في زيادة مجال تغطية BSS وربط عدد من BSS_s مع بعضها بعضاً. وعند ربط عدد من BSS_s مع بعضها بعضاً تدعى بالأنظمة الموزعة (DS) Distribution System حيث تربط كل BSS عبر AP ومن خلال البطاقة الخاصة Ethernet إلى DS، ومن ثم من DS إلى نقاط دخول أخرى كما في الشكل (2) النظام الموزع DS.



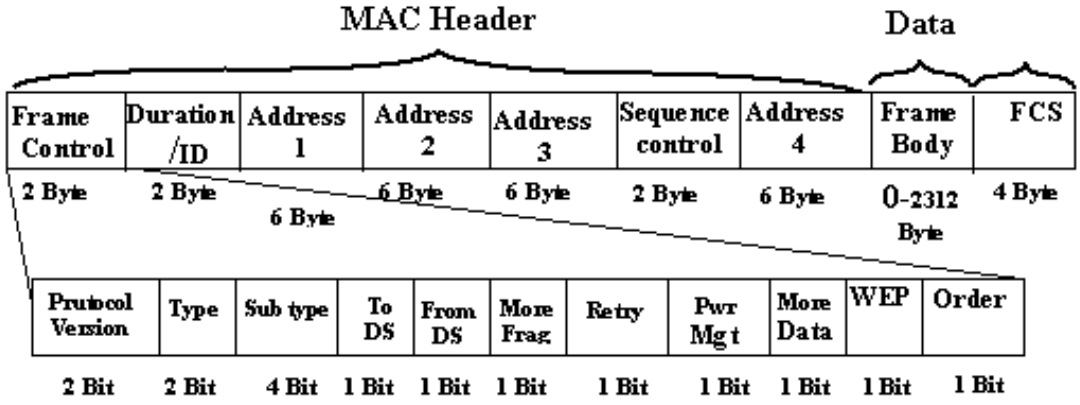
الشكل (2) النظام الموزع DS

ومجموع DS مع المجالات BSS_s تدعى مجموعة الخدمات الموسعة ESS (Extended Service Set)، وبعد أن يتم إجراء الاتصال يأتي دور البروتوكول الموصف في IEEE 802.11 والموجود ضمن موديل ISO/OSI

(International Standard Organization / Open System Interconnection) وهذا البروتوكول موجود في طبقة ربط المعطيات Data Link Layer وعلى الجزء الثاني منها MAC (Media Access Control) والخاصة في السؤال عن الوسط الناقل وكذلك التشفير وضبط الإرسال ...

مكونات الإطار في Wlan.

- رأس MAC وبطول 30 Bytes
- جسم الإطار المعطيات ويتراوح طوله ما بين 0 ¬ 2312Bytes
- اختبار تتابع الإطار Frame Check Sequence (FCS) وبطول 4 Byte



الشكل (3) شكل الطرد لـ MAC

يقسم حقل التحكم بالإطار Frame Control إلى حقول جزئية بأطوال مختلفة، وأنواع وأجزاء أنواع مختلفة وضمن إطار واحد يمكن أن تملك ثلاث أنواع مختلفة.

1- نوع Data: هي المعطيات المستخدمة في إرسال جسم الإطار.

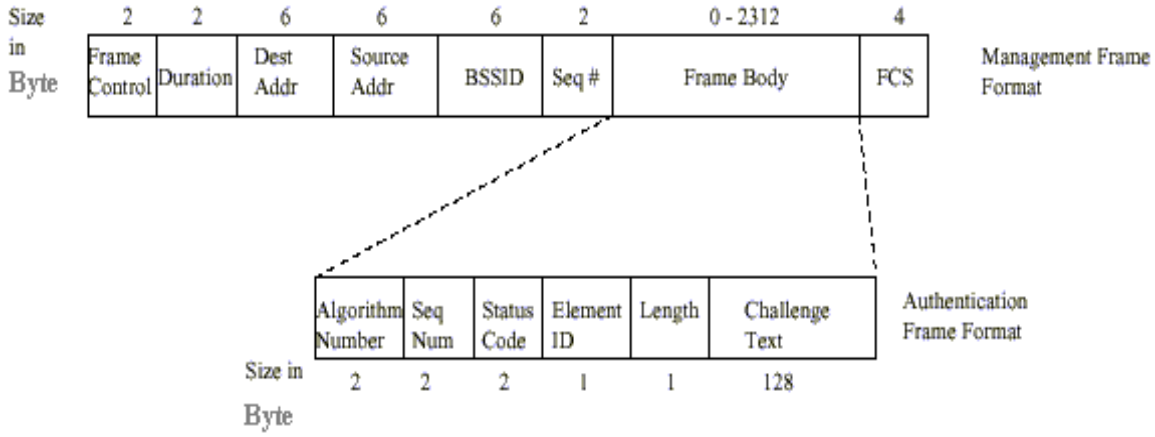
2- نوع Control: تستخدم مثلاً من أجل إدارة القدرة " البطارية مثل إرسال خانة بشأن الاستمرار في انتظار الاستقبال أو بشأن التوقف عن الانتظار بغية تخفيض استهلاك الطاقة.

3- النوع Management: تستخدم مثلاً من أجل إدارة التسجيل والارتباط.

في نهاية إطار التحكم توجد خانة تدعى WEP (Wired Equivalent Privacy Protocol) للدلالة فيما إذا كانت المعطيات الموجودة في جسم الإطار قد تم تشفيرها أم لم يتم تشفيرها. وفي حقل الاستمرارية duration في رأس MAC يتم إعطاء الحجم الأعظمي للنقل، وفي جزء التحكم بالترتيب توجد معلومات حول تجزئة الرسالة وأرقام ترتيب الحزم. وتملك حقول العنونة 4،3،2،1 وفق ترتيبها في إطار التحكم دلالات مختلفة.

- العنوان الأول: يحدد عنوان المستقبل النهائي.
- العنوان الثاني: عنوان أول مرسل.
- العنوان الثالث: عنوان المستقبل التالي.
- العنوان الرابع: عنوان آخر مرسل.

أما جسم المعطيات فيتم تجزئته وفق الشكل 4 الآتي:



الشكل (4) إطار المعطيات

- التدابير الأمنية IEEE 802.11 Security Mechanisms Standard

من أجل زيادة الأمن على الشبكات WLAN يجب الأخذ بعين الاعتبار ما يلي:

- § التقليل قدر المستطاع من تبادل الإرسال البعيد، وذلك لجعل اختراق الشبكة أصعب واستخدام هوائيات موجهه أو التقليل من قوة الإشارة لحد الوصول إلى تغطية مجال الشبكة فقط.
- § استخدام Firewall مابين الشبكة السلكية وللاسلكية من أجل التقليل من دخول مخترقي الشبكة السلكية عبر الإنترنت إلى الشبكة وللاسلكية والشبكة السلكية يجب أن تحمى من الداخل ب Firewall خاص بها وهنا يجب التذكير المثابرة على الإشراف مراقبة مستمرة واختبار مباشر للشبكة وضبط قواعد الدخول والتحكم بها بشكل مباشر.
- § التغيير الدوري في مفتاح WEP يصبح الزمن الذي يستفيد منه في اختراق الشبكة أقل.
- § أبطال تفعيل إرسال SSID التي تتضمن محددات الشبكة ضمن Beacon Frames وإن ذلك خيار تعطيه معظم نقاط النفاذ AP كخيار broad Cast Option .
- § عدم تفعيل المشاركة بـ IP بشكل تلقائي من خلال DHCP ضمن WLANs وإعطاء المحطات عنواناً ثابتاً وفي هذه الحالة يجب على المخرق معرفة مجال العناوين أولا ومن ثم إعداد إحداها، وفي حال تفعيل DHCP يحصل المخترق على عنوان بشكل تلقائي بدون تعب.
- § مجال عناوين IP يجب أن تختار ضيقة قدر الإمكان واستخدام عدد من العناوين اقل وتصبح حرجة أكثر للمخترقين.
- § يجب تبويب متاعب الشبكة من أجل جعل تحليلها
- § استخدام Intrusion Detection System (IDS) التي تسرع كشف المخترقين واتخاذ إجراءات مضادة لذلك.
- § ربط VPN والتي تعتمد في الحماية على طرق Crypt graphics كما هو مع IPSec.
- § وحماية إضافية تعطيها AP المربوطة مع LAN وهى أن يتم الإعداد من جهة WLAN فقط لأن تقانات WEP غير كافية وبالتالي أي تغيير في Configuration سيتم من جهة WLAN.

§ إدارة الوقت بالنسبة للـ AP التي تسمح لها بالعمل ضمن ساعات الدوام فقط وعدم العمل في نهاية الأسبوع ويصبح البحث عن المحطة أصعب ولاسيما أن War Driving Attack يعملون في نهاية الأسبوع أو الوقت الفارغ خارج أوقات الدوام.

§ عدم إجراء الإدارة للشبكة خارج أوقات الدوام،أو لوقت طويل خارج أوقات الدوام وبالتالي لا توجد معطيات منقولة وعدم وجود معلومات عن مفتاح WEP السري.

4-2-1 مجموعة خدمات التعرف SSID (Service Set Identifier):

إن SSID هي عبارة عن اسم الشبكة المؤلف من 0 -32 Byte من أجل تعريف BSS أو ESS وهي لا تعبر عن تقنية أمن حقيقية بل تعبر عن التحكم بالدخول إلى الشبكة ويمكن لنقطة النفاذ AP أن تحتاج SSID وفق نوعين:

إما أن يكون طولها 0 Byte أي يعبر عنها بسلسلة فارغة ومنقولة كـ SSID، ويمكن لكل STA أن ترتبط.

أو أن تكون أية سلسلة محرفيه فتعتبر كسلسلة تحكم وهي خاصة بنقطة النفاذ إلى AP ويمكن لـSTA أن ترتبط فقط من خلال نقطة النفاذ هذه وهذا ما نراه في الشكل (5)

الشكل (5) مطابقة الصحة

- التصفية وفق عنوان MAC MAC- Address Filter

إن كل بطاقة شبكة تملك عنواناً معرفاً عليها وثابتاً وهو ما يعرف بعنوان MAC ويمكن تخزين لائحة من عناوين البطاقات MACs التي تتعامل مع نقطة الدخول AP وعليه يمكن لهذه البطاقات التي عناوينها في AP أن تتصل معها وسيتم بعدها تجاهل باقي الإطارات التي عناوين إرسالها MAC غير مدون ضمن اللائحة ACL، ويجب أن يتم تحديث اللائحة من قبل مدير المحطة. [3]

إلا أن ذلك يقوم بتحديد المستخدمين في نقطة نفاذ محددة >وبالتالي تفقد الشبكة بعضاً من إحدى أفضل مميزاتها.

- وصول المعطيات من دون تغيير أو تكامل المعطيات Data Integrity

من أجل حماية تكامل المعطيات يستخدم bit 32 والمعروف CRC32، حيث يلخص المرسل معلومات عن المعطيات ويلحق ذلك في نهاية الحزمة ويعرف هذا التلخيص (frame Check sequence) FCS .

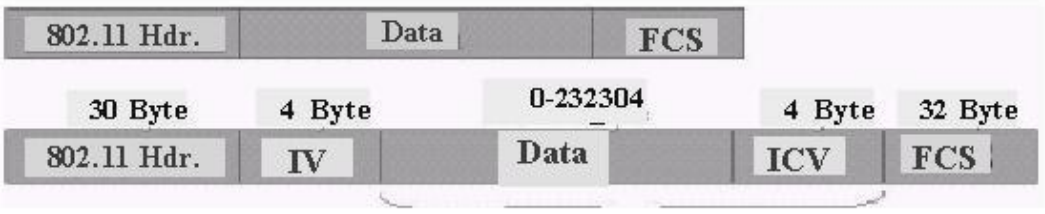
تستعمل خوارزمية CRC32 لحساب معلومات الرأس والمعطيات المستقبلة وتقارن نتيجة الحساب مع ما تم إرساله FCS في نهاية الرزمة وإذا تطابقت النتيجة سيتم استقبال الحزمة وإلاّ سيتم رفضها.

- التشفير مع البرتوكول WEP (Wired Equivalent Privacy protocol)

لحماية تكامل وأمن المعلومات يستخدم بروتوكول WEP ، بالتالي تحتاج كل من STA وAP في WLAN إلى مفتاح متماثل بطول 40 Bit أو 104 Bit، ويعرف هذا المفتاح بالمفتاح المشترك.

بعدها يتم وضع WEP Bit في إطار التحكم "Frame Control"ضمن MAC -Head.

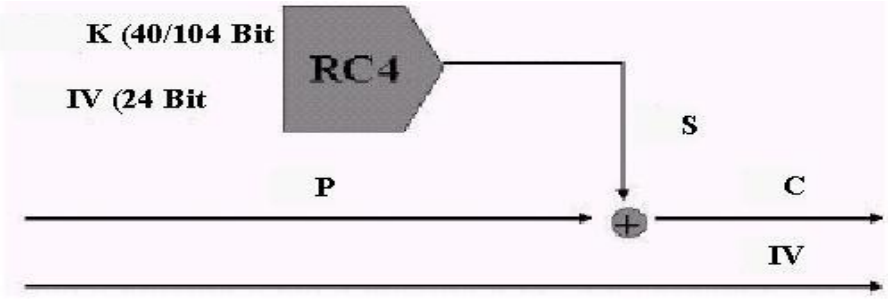
قبل إرسال الحزمة سيختار المرسل 24bit تدعى IV (initialization vector) ويرسله ما بين الرأس والمعطيات في الحزمة. وبعدها من خلال CRC32 ويتم إيجاد ICV (Integrity Check Value) عن المعطيات ويوضع ما بين المعطيات وFCS ويتم وضع المعطيات وICV بشكل مشفر ويدعى ذلك بـ p وإذا كانت WEP=0 هذا يعني بدون تشفير وإذا كان WEP=1 تكون مع تشفير كما هو موضح في الشكل (6).



الشكل (6) إطار MAC مع وبدون WEP

التشفير من P يتم من خلال الاعتماد على خوارزمية RC4، مع RC4 توجد خوارزمية تشفير تيار النبضات ومن خلال المفتاح المشترك K ومع IV سنحصل على S .باستخدام IV مختلف ودمجها مع k الثابتة عبر لـ RC4 فنحصل على S مميزة "فريدة" ويتم جميعها مع P عبر XOR لتشكل الخرج المشفر C كما نجد في الشكل(7) إن الناتج C يرسل مع IV المخصص لكل حزمة.

يقوم المستقبل بعمل مماثل للمرسل حيث يفك IV من الحزمة من خلاله والمفتاح المشترك K وبحسب S. ويقوم باستخدام XOR لإجراء الجمع لـ C وS للحصول على P ويتم الحساب للمعطيات كما في 4-3-3 ويتم المقارنة مع ICV.

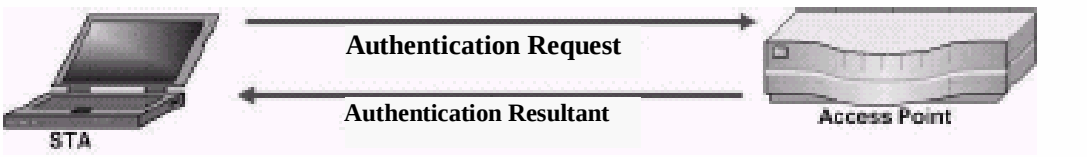


الشكل(7) تشفير باستخدام WEP مع RC4

4-2-5- المصادقة والمطابقة (Authentication):

للإعلام والتأكد من المصادقة والمطابقة نوعان – النظام المفتوح ومطابقة المفتاح المشترك.

–عند التأكد في النظام المفتوح يتم سؤال AP من قبل STA عبر إرسال استفسار Request التأكد المميز. قبول Result هذا السؤال بدون إبعاد STA يعطي ذلك نتيجة واضحة أن التأكد باستخدام النظام المفتوح لا تعطي ضمان ضد المخترقين.



الشكل (8) التأكد من الصحة في النظام المفتوح

– إن التأكد باستخدام المفتاح المشترك تعرض بالمقارنة طريقة Challenge – Response ، ويحتاج ذلك إلى المفتاح المشترك K والمستخدم عند تشفير WEP، تقوم المحطة STA بإرسال سؤال المطابقة وتجيب AP من خلال Challenge .

Challenge يتكون من 128byte من دون تشفير ونص مولد بشكل عشوائي.

تختار STA الـ IV وتشفر معه ومع K بالاستفادة من RC4 ومع Challenge P .

هنا ترسل STA كل من C و IV و Pإلى AP فإذا كانت نتيجة مقارنة فك التشفير C وكذلك p مع Challenge المرسل إيجابية (مطابقة) عندها تعطي القبول. الشكل (9)

الشكل(9) التأكد من الصحة باستخدام المفتاح المشترك

4– نقاط ضعف الـ IEEE 802.11

إضافة إلى القلق الذي تم ذكره حول صحة المعطيات التي تم عرضه كتقنية ضمان ضمن ، تباع "مكونات" WLAN وقد تم تفعيل القليل من تقنيات الأمن عليها ويقع تجهيز ذلك على مدير نظام الشبكة WLAN وسيتم التطرق على نقاط الضعف الموجودة في تقنيات أمن المعلومات لاحقاً. [4]

1– *مشاكل أمن* MAC-Address filter و SSID (Service Set Identifier)

تكمن مشكلة SSID في ضبط دخول المشترك في أن SSID ترسل كنص واضح غير مشفر. ويستطيع المخترق لنظام أن يشارك بكتابة برتوكولات والحصول على SSID . نظراً لأن أعمال MAC- Address من الممكن استخدام MAC- Address filter

2- *مشاكل أمن تكامل معطيات* CRC

يتم الآن العناية بمشكلة الأمن عند التحقق من صحة وصول المعطيات واستخدام CRC32 لملخص الكشف، وسنتناول هنا التغيير غير الملحوظ في الرسالة المشفرة وكذلك الأمر ICV وهذا الأمر ينطبق على FCS غير المشفر بصورة مماثلة.

عند اختبار CRC32 كضمان للتغيير تظهر سلبيات كثيرة منها :

إن CRC32 يستخدم تابع خطي، وهذا يعني:

$$c(P1 \text{ XOR } P2) = c(P1) \text{ XOR } c(P2)$$

c() تابع الاختبار، P النص الواضح، C النص المشفر، S تستنتج من A' , RC4(K,IV) التغيير، C' التغيير في النص المشفر، M' التغيير في الرسالة.

وبالتالي يمكن كتابة ما يلي:

C=RC4(IV,k) XOR <P,c(P)>
C XOR < A', c(A') > = [RC4(IV,k) XOR < P, c(P) >] XOR < A', c(A') >
C` = RC4(IV,k) XOR < PXOR A', c(P)XORc(A') >
C` = RC4(IV,k) XOR < P`, c(PXOR A') >
C` = RC4(IV,k) XOR < P`, c(P`) >

هذا يعني يمكن للمرء أن يقوم بتغيير دون معرفة مفتاح الأخبار، والمستخدم لنقطة الضعف هذه والتي تدعى إعادة توجيه IP. ويكون الهدف بعد الحصول على الحزم، مثل IP المنبع المرسل في رأس IP للمكان الذي حصل عليه المخترق وقام بالتغيير، ومن ثم يتم متابعة إرسال الحزمة ولن يعود الجواب إلى المرسل الأصلي ولكن إلى من قام بالتغيير.

3- *مشكلة أمن برتوكول* WEP.

يتم التشفير من خلال خوارزمية تشفير تيار النبضات stream cipher ولضمان الأمن بشكل جيد يجب مراعاة التبديل عند وضع الخوارزمية السابقة ، إذا كان لدينا نصان مشفران بـ S نفسه سيتم كشف S بسهولة وعليه يجب تجنب استخدام IV نفسه مع K نفسه لغير مرة.

لتكن P1 و P2 نصين واضحين ومع S نفسه وعبر خوارزمية RC4 مع المفتاح المشترك K نفسه والمشفرة مع نفس IV,v .

$$C1 = P1 \text{ XOR } RC4(v, K) \text{ and } C2 = P2 \text{ XOR } RC4(v, K)$$

ويكون:

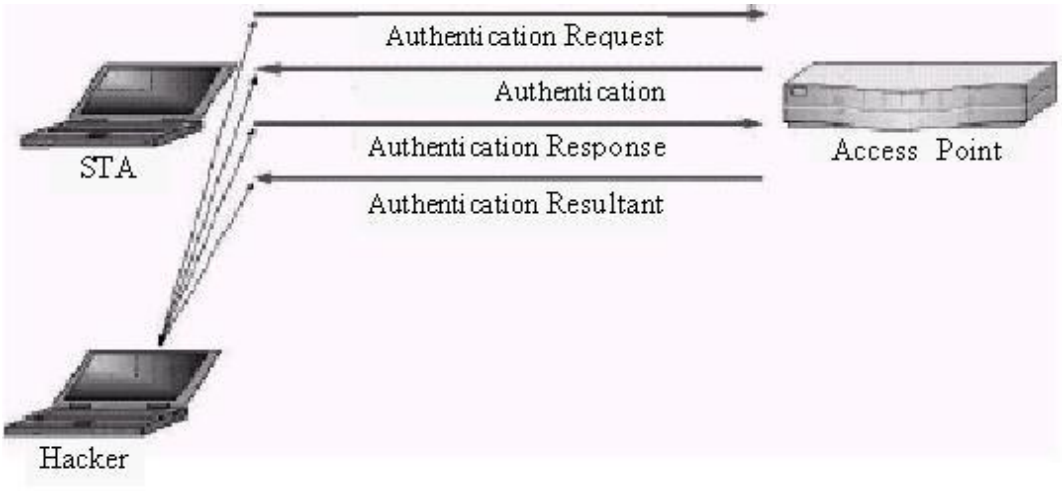
C1 XOR C2 = [P1 XOR RC4(IV1, k)] XOR [P2 XOR RC4(IV1, k)]
C1 XOR C2 = P1 XOR P2 XOR RC4(IV1, k) XOR RC4(IV1, k)
C1 XOR C2 = P1 XOR P2

هذا يعني عندما يملك الإنسان نصين مشفرين ومع S نفسه والمعروضين، يحصل على الاثنين عبر الربط باستخدام XOR ، إن استخدام زوج من IV v ونص المشفر C والنص الواضح P يمكن أن يتم فك التشفير مع نص مشفر C2 يمكن أن يعرض مع IV v و K.

4- *مشاكل مطابقة المفتاح المشترك* Shared Key Authentication

كما ذكرنا سابقاً تبني آلية التحقق من صحة المعلومات المعتمدة على تقنية المفتاح المشترك على مبدأ Response – Challenge وفي الخطوة الثانية من التحقق ترسل AP سلسلة رموز بدون تشفير بطول 128byte وبشكل عشوائي إلى STA.

تقوم المحطة STA بتشفير ذلك مع مفتاح مشترك K ومع v IV خاص مختار " كما في4-2-4" ولكن إذا حصل أحد المخترقين على Byte 128 عند الدخول على التعرفة كما في الشكل 10 " يحصل هو على نص واضح p، وchallenge في شكل غير مشفر وكذلك C الخاصة بشكل مشفر والصدى Response ، وInclusive لـ v IV المستخدم. [1]



الشكل(10) المخترق على التأكد من الصحة باستخدام المفتاح المشترك

ومع هذه المعرفة لا يمكن للمخترق أن يغلق على مثل المفتاح K المستخدم. ويمكنه من خلال الربط لـ P وC عبر XOR لحساب S ويمكن للمخترق من خلال استخدام IV v المختار مع S أن:

1- يغلق من خلال مطابقته الخاصة لـ Challenge P ويطابق لنفسه كما يرغب.

2- إغلاق سلاسل P لإخبار النصوص الواضحة.

بالرغم من أنه لا يعلم المفتاح المستخدم K .

ومن أجل الإيضاح ثانية نجد ذلك في الشكل 7 السابق.

5- *مشكلة استخدام* WEP:

رغم كل التحذيرات لأخذ كل التدابير الأمنية المتاحة من أجل تأمين الأمن للمعطيات المنقولة وللشبكة، إلا أن بعضاً يتعاطى بعهما أو بجهل مع هذه التدابير ويجب أن نؤكد على بعضها:

- تفعيل التشفير مع WEP(Wired Equivalent privacy protocol) رغم أن ذلك لم يعد حالياً أمن إلا أنه يطيل من الزمن اللازم للدخول للشبكة من قبل Hacker .

- تفعيل صحة المفتاح المشترك (shared key Authentication) الذي يعطي احتمال للاختراق أثناء طلب المصادقة.

- ACL(Access control list) هنا تضاف محدد آخر للدخول إي الدخول فقط من AP المخصصة التي تملك عنوان MAC المسجلة لدى اللائحة.

- SSID(Service set Identifier) لا يسمح بإعادة المفتاح المشترك للشركة ويستخدم أسم الشركة كـSSID ويمكن Hacker من الوصول إلى مكان الشركة سواء التقط معطيات مفيدة أم لم يلتقط.

- Change default password for administrator : إن 6 byte لعنوان MAC تتوضع مع العنوان وOUI والمستخدمة من قبل المنتج، OUI مسجلة لدى IEEE ويمكن الوصول إليها من خلال بعض المواقع مثل http://standards.ieee.org/regauth/oui/index.shtml

- وعند التسجيل لدى الشركة وإعطاء كلمة المرور الصحيحة يمكن عندها تنزيل Handbook من الصفحة الرئيسة والتي تملك كل كلمات المرور لـ administrator وعلية يمكن الوصول إلى إعدادات نقاط العبور AP وكذلك الدخول إلى ACL وتوسيعها.

- War Driving: وهنا نجد ظهور الهواة الذين يعملون عند أوقات الفراغ للدخول في الشبكة، ويستطيع هؤلاء الدخول ببساطة في الشبكات المحمية بشكل ضعيف أو الشبكات المفتوحة، التي يمكن أن تستخدم للدخول إلى الإنترنت، وتكون في معظم الحالات في المطارات الكبيرة التي يزداد الازدحام بها نظراً لتغطيتها مجالاً كبيراً ويعقد هؤلاء ندوات في المدن الكبيرة ومباراة لمن يجد أكبر عدد من الشبكات التي تم اختراقها ويحتاج المخترق إلى جهاز محمول وهوائي إرسال وبرمجيات خاصة والتي تظهر الشبكة التي تم إيجادها، والهوائيات في العادة مصنعة بشكل شخصي والبرمجيات الشهيرة موجودة على مواقع من هذا القبيل. www.netstumbler.com

- وتقوم بالبحث ضمن جميع الخطوط وتظهر شبكات WLANs التي تجدها حيث تظهر APوبجوارها SSID ورقم الخط وقيمة الضجيج ومسافة الضجيج وفيما إذا كان WEP مفعّل أم لا.

وهذه الشبكات التي تم اختراقها ترسل إلموقع مثل (والتي يتم تغييرها بشكل مستمر) www.netstumbler.com وما على المخترق إلا البحث عن الشبكة التي تهمه ومن ثم عليه الوصول إلى مجال تغطية أحد محطاتها إما السفر أو المشي War Walking .

- يتم الحديث هنا عن war Chalking التي تعطي أربع معلومات مهمة SSID المجهزة للاستخدام ، عرض الحزمة، رقم الخط المستخدم والتحكم بالوصول وفي المرحلة الأخيرة نجد ثلاثة رموز مستخدمة من أجل معرفة الشبكات المخترقة.

واحدة للشبكات المفتوحة والثانية لمعرفةWLAN المحمية مع WEP والخيرة للشبكات الأمنية كما في الشكل.

- وبشكل واضح يجب على النوعين الأول والثاني زيادة الاهتمام بالحماية أما النوع الثالث فإن استخدامه حرج لأن ذلك لا يزال غير محكم نظراً لوجود Hacker لم يجرب بعد وربما هو أكثر مهارة من المحاولين الاختراق.

وكما لاحظنا يعطي WEP بعض الحسنات وكذلك يقدم عدد كبير من مشاكل الأمن ونذكر منها:

الحسنات:

1- تشفير كل حزمة بشكل منفرد وبالتالي لا توجد مشاكل عند ضياع أية حزمة.

2- إغلاق Efficient: مع حساب كل المركبات من IV المختلفة ومع K نفسها يمكن الحصول على كل S وعند إرسال الحزمة يمكن أن ترى في جدول لكل من IV, S

3- أن توضع كخيار للتفعيل.

السيئات أو المشاكل:

1- الأمن غير كافٍ لا يمكن استخدام IV مرتين مع K نفسها و S نفسها مما يخلق مشاكل في الأمن.

6-*مشاكل* WEP :

من أجل تشفير معطيات الشبكة نجد 802.11 والذي يجب أن يكون أمن لحماية المعطيات المنقولة من الاستماع وسلامة المعطيات وكذلك التحكم بالدخول إلى الشبكة.

يستخدم WEP128 في معظم شبكات WLAN حتى يتخيل أنة هو القياسي،وتعاني الشبكات التي تعتمد على WEP من ضعف في الأمن للأسباب التالية:

- – طول Initialization Vector قصير 24bit.
- طول المفتاح 40-104 bit قصير.
- تقنيات WEP مفتاح متناظر وعدم إتاحة إدارة مفاتيح وكذلك عدم تقسيم مفتاح WEP.
- إمكانية كسر تقنيات Authenticates.
- عدم استخدام التأكد من تقنيات المطابقة وإنما Adepter .
- خوارزمية ضبط Initialization ضعيفة نشبياً ويمكن تعديلها.
- يمكن تغيير محتوى الإطارات للسبب السابق.
- إن ضعف Initialization Vector يعطي الـ War Attacker, Brute Force Attacker, dictionary Attacker إمكانية الاختراق.
- تطوير خوارزمية التشفير من خلال استخدام Pseudo Random Number Generator(PRNG) واستخدام مفتاح بطول 128 bit منها 104 bit للمفتاح السري و 24 bit من اجل Initialization Vector وسيتم بناء ترتيب معروف بـ Seed يتم أستخدمها من قبل PRNG لتوليد Random stream from chaffer bites والمستخدمة في تشفير المعطيات عبر RC4 المصنعة من قبل شركات منها www.rsaasecurity.com وبعد التشفير سيتم الحصول على ملخص اختبار Integrity check value (ICV) والمرسل مع الرسالة.
- وسيتم عبر XOR دمج النص مع ICV و stream chaffer bites لينتج Initialization Vector والمعطيات المشفرة في جزء المعطيات في الإطار المنقول.
- ويحصل المستقبل على الإطارات المنقولة التي يستخلص منها Initialization Vector ومن خلاله مع ومفتاح WEP السري المستلم يقوم المستقبل ببناء stream chaffer اللازم لفك تشفير الإطار وبعدها يتم اختبار تكامل المعطيات وفق IVC.

وباعتماد WEP يتم النقاش حول تقنيات التشفير المتناظرة والتي يجب على المرسل والمستقبل استخدام مفتاح WEP نفسه السري وعليه يفقد مدير النظام إمكانية إدارة المفاتيح وبالتالي لابد من إعطائها يدوياً لكل مجموعة WLAN.

7- *مستقبل مفتاح* WEP.

- إن Weak attack يحصل عندما تكون خوارزمية WEP ضعيفة أي يمكن معرفة مفتاح تشفير WEP السري، وتوجد بعض الخوارزميات Weaknesses in key scheduling Algorithm of RC4 التي يمكن أن نجد منها في: http://odysseus.ieee.org

وهنا نجد احتمال توليد تكرار لـ Initialization Vector ويصبح أمر الحصول على المفتاح العكسي سهلاً ففي شبكة مزدحمة بشك وسط ولكسر مفتاح WEP السري تحتاج إلى التقاط من 5 إلى 10 مليون إطار مشفر والتي تحتاج إلى عدة ساعات مما دعي إلى إيجاد WEPplus حيث يتم تامين لكل Initialization Vector - stream chaffer bites وبالتالي تكفل المطابقة القياسية لـ WEP .

- عند استخدام Initialization Vector يجب النظر إليه بشكل حرج لأن الحجم 24 bits هو 2^{24} تعطي 16,777,216 احتمال وهى قيمة ليست كبيرة بالنسبة لشبكة كبيرة بعدة نقاط دخول ولا تحتاج أكثر من ساعات لتوليد الـ Initialization Vector مكرر من جديد ولا سيما أن إعادة إقلاع أية مركبة من مركبات الشبكة هو إعادة استخدام Initialization Vector .

- إن العديد من مركبات الشبكات تقوم بوضع Initialization Vector للقيمة صفر عند إعادة الإقلاع ويزداد بمقدار واحد لكل إطار مشفر ويصبح احتمال الإطار المكرر بعيد وإذا تم الحصول على رسالتين مع نفس Initialization Vector فإن ذلك يعطي المخترق مجال لفك التشفير ويمكن من خلال استخدام XOR والرسالتين المشفرتين V1 و V2 والنصين K1 و K2 ومتاح التشفير S نحصل على :

$$V1=K1 \text{ XOR } S \quad \text{and} \quad V2=K2 \text{ XOR } S$$

ومن خلال عملية حسابية بسيطة يمكن إجرائها نجد

$$V1 \text{ XOR } V2 = K1 \text{ XOR } S \text{ XOR } K2 \text{ XOR } S$$
$$V1 \text{ XOR } V2 = K1 \text{ XOR } K2 \text{ XOR } S \text{ XOR } S$$

وبما أن S XOR S تنفي بعضها نجد

$$V1 \text{ XOR } V2 = K1 \text{ XOR } K2$$

وبمعرفة واحدة من الزوج V1,K1 وإعادتها إلى الأصل يمكن حساب K2 بدون معرفة المفتاح

$$K2 = K1 \text{ (V1 XOR V2)}$$

وبالتالي يكون الاستخدام مع نفس Initialization Vector نقطة ضعف .

- Brute Force Attacker: نجد ذلك عند تجريب كافة الاحتمالات الممكن للمفاتيح والزمن اللازم يتعلق طبعاً بطول المفتاح وقدرة جهاز المخترق للحساب.

- وعند استخدام WEP40 or WEP128 ومع مفتاح بطول 64 or 128 bots نجد الاحتمال 2^{40} or 2^{128} ويحتاج مع الحواسب الحالية و WEP128 إلى زمن طويل جداً عدة ترليونات من النوات من أجل اختبار كل الاحتمالات.

- = عند استخدام Dictionary attack : معظم مديري الأنظمة يستخدمون كلمات تكون شهيرة بالنسبة لهم وعلى الأقل يمكنهم تذكرها من أجل توليد مفتاح WEP وعند جمع هذه الكلمات ضمن قاموس يمكن عندها تخمين هذه الكلمات، وهنا سيتم تجريب الكلمات الشهيرة من لائحة الكلمات للحصول على الكلمة المستخدمة، ومن أجل مشاكل WEP والتقليل منها على الأقل وضعت IEEE حلول أمن جزئية لمواصفات 802.11i. وهي ما تدعى .. (Protected access وتتركز على تحسين:_

– تطوير 802.11i:

لقد تمت معرفة مشاكل WEP وشكلت فرق عمل من أجل ذلك وعملت على تطوير البرتوكول 802.11i وعلى طبقة MAC بغية تعزيز أمن المعطيات المنقولة وكذلك تحديد الدخول إلى الشبكة.

والمشاكل الجوهرية عند تطوير تقانات الأمن المادية هي المحافظة على التوافق compatible مع الإنتاجان القيمة المستخدمة في الشبكة ويكون من خلال تجديد مادي اقل ما يمكن وتجديد برمجي إن أمكن وفي النهاية تم إيجاد بنى مادية تراعي النقاط الثلاث التالية:[5]

Temporary Key Integrity Protocol (TKIP) تعتني بالدخول من خلال البني المادية والتحديث من الشركة المصنعة للشبكة ومع TKIP تمت تغطية معظم نقاط الضعف لتقنيات WEP.

Advanced Encryption Standard (AES) تعني بتقديم حلول لتشفير المعطيات ذات حماية كافية لما هو متوفر حالياً والتطوير هو مادي لتحسين تابع التشفير AES.

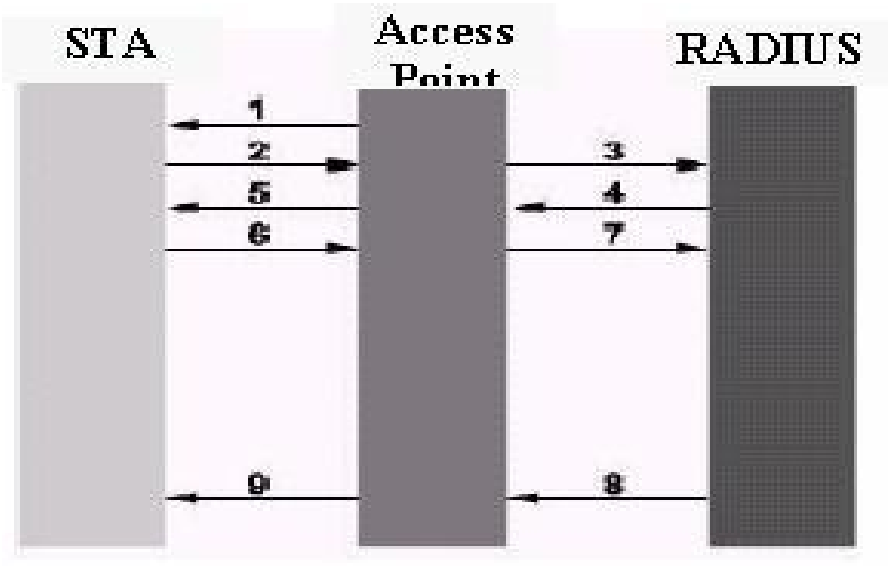
Radius Authentication : المطابقة للفرد الواحد بدل من مطابقة المفتاح المشترك.

1- تحسين المطابقة من خلال بروتوكول EAP(Enhanced Authentication Protocol)

2-تحسين تشفير المعطيات من خلال بروتوكول TKIP (Temporal Key Integrity Protocol) وسنعطي نظرة عن كل مجموعة.

-بروتوكول EAP (Enhanced Authentication Protocol)

EAP تعتمد للمطابقة على عدد من تقنيات المطابقة من أجل الحصول على ضمان مضمون بدرجة عالية. وهى غير مفيدة للشبكات الصغيرة وإنما جيدة ومن أجل الشبكات الكبيرة ويحتاج إلى مخدّم مطابقة مثل RADIUS or KERBEROS وتصبح المطاقة كما في الشكل(11).



الشكل (11) ERP

إنّ AP تطالب من نقطة النفاذ 1 STA(1) موافقة فريدة " مفتاحيه" وبعدها تعاد إلى AP (2) ثم توصل إلى RADIUS (3) وبعدها يتم إرسال Challenge من RADIUS عبر AP(4) إلى STA(5) وتقوم STA بالإجابة عبر AP(6) إلى RADIUS (7) وبعدها تحصل المطابقة في الخطوتين (8,9)

– وضمن 802.2x نجد Extensible Authentication protocol (EAP) الذي يكتب ببساطة تقنيات Request & Response للمعطيات المتبادلة والجواب سيكون من مخدم المصادقة.

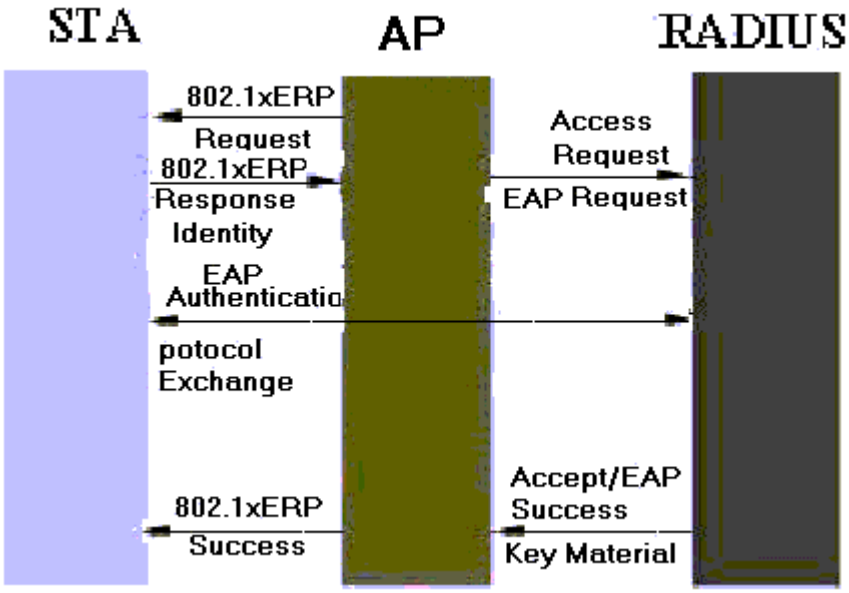
– EAP-MD5: والتي تعني بأبسط نوع من المصادقة والمشروحة في RFC 1321 والمعروفة بخوارزمية تنظيم الرسائل (Message Digest Algorithms) إن EAP-ND5 ترمز المعطيات المتبادلة عبر MD5-Hashing ومن دون طلب مسبق للمصادقة ما بين المرسل والمستقبل. EAP-ND5 لا تحمي مفتاح WEP الديناميكي وإنما تحمي الستاتيكي، وهي بالتالي تحمي الميزات للمستخدم والذين يرغبون بالوصول إلى المصادر على الشبكة.

= EAP-Transport layer Security Protocol (EAP-TLS) وهى حالة مركبة من EAP والموصوفة في RFC 2716 وهذه الحالة تطالب المصادقة ما بين المخدم والمستقبل وتحمي مفتاح WEP الديناميكي وتجديد المفتاح الآلي في مجال ضيق.

= EAP-Tunneled Transport layer Security Protocol (EAP-TTLS) عبارة عن جيل متطور عن السابق (EAP-TLS) حيث يتم بناء حماية للقناة مابين مخدم المصادقة WLAN Adapter للمستخدم قبل طلب المستخدم المصادقة، ومن خلال القناة الآمنة TLS سيقوم المستخدم بتعريف نفسه عبر كلمة مرور واسم المستخدم.

وهذا يتطلب بشكل أساسي ترخيص وهو ما يعرف Secure Socket Layer (SSL) لمصادقة TLS فقط ترخيص من جهة المخدم من اجل حماية معلومات المصادقة.

= Light Weight EAP (LEAP) وهى تتحدث عن الحلول الأولية التي تم تطويرها من قبل Cisco والمتعلقة بـ 802.1x عندها يجب أن يحصل كل من المخدم والمستخدم على المصادقة بشكل متبادل. ويتم إنتاج المفتاح الديناميكي من Cisco عبر تقنيات WEP-Key Hashing حيث يتم بناء Hash-Word من خلال Initialization Vector ومفتاح WEP الديناميكي، وهذه سوف تستخدم ثانية لمفتاح WEP والتي ترتبط مع Initialization Vector كمل في الشكل11–1 التالي. (6)



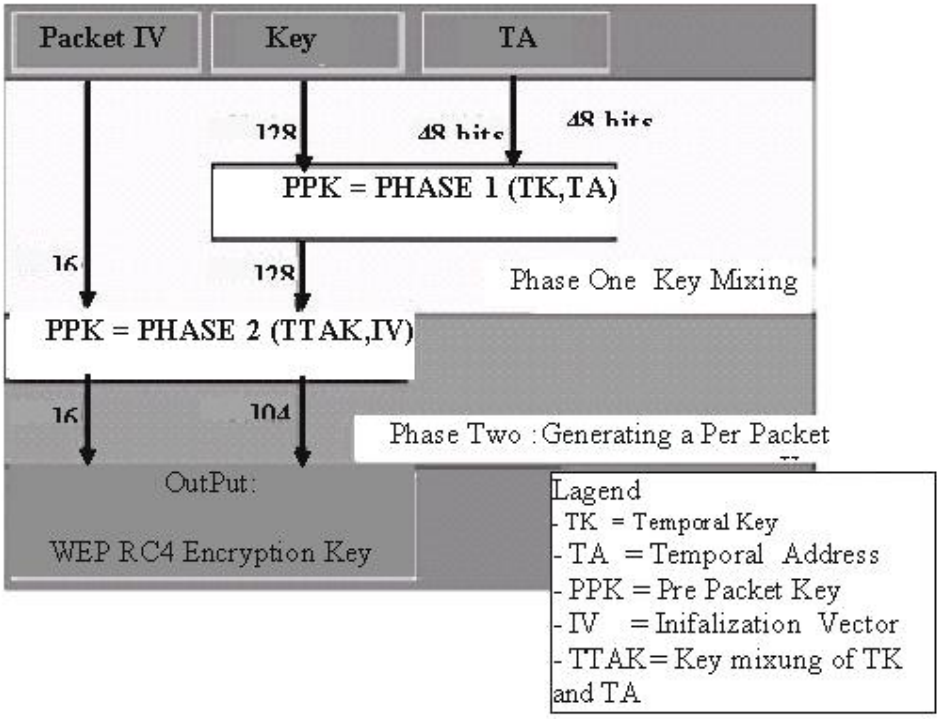
- بروتوكول TKIP (Temporal Key Integrity Protocol):

من المهم عند تعريف تقانات TKIP الاعتناء بقدرات AP المتواضعة، ويتم ذلك من خلال مولد للمفاتيح التي سوف تستخدم في تشفير المعطيات ويصبح التشفير غير مرتبط مع مفتاح ثابت وإنما مع مفتاح مؤقت والذي يتم تغييره بعد 1000 إطار على الأكثر وهذا ما يعرف Re Keying وسيتم بالاعتماد على زيادة طول Initialization Vector من 24إلى 48 bits ومن أجل تشفير المعطيات سيتم بناء مفتاح منفرد لكل إطار من خلال تابع Hash function ويحمي تابع Hash نفسه من خلال أمرين: الأول من خلال مزج المفتاح المؤقت مع عنوان MAC ومع 32 bits الأولى من Initialization Vector(IV32)، الثاني سيتم استخدام مزج خرج المرحلة الأولى والمفتاح المؤقت و 16bits الأخيرة من Initialization Vector والنتيجة سيتم استخدامها لتوليد RC4-PGNG والنتيجة سوف تستخدم لبناء stream chaffer bites .

إن 16bits الأخيرة من Initialization Vector(IV16) تبني الرقم التسلسلي والذي يزداد مع كل إطار وبالتالي استحالة إعادة استخدام stream chaffer bites نفسه ونظراً لتغيير Initialization Vector المستمر سيتم استخدام مفتاح لكل إطار Per Packet Keying .

وكذلك من خلال TKIP يمكن الحديث عن اختبار متكامل للرسائل Message Integrity Check (MIC) من خلال التحكم المتكامل، والتغيير غير المعلوم وكذلك تغيير وضع إحدى الخانات ضمن الإطار المشفر، والتحكم المتكامل لا يعتني بالمعطيات فقط بل بعنوان MAC للمحطة المرسلة أيضاً.

الرقم المتسلسل سيتم إعادة وضعه طالما أنه يتم استخدام تيار جديد، وإذا تم تسجيل رقم تسلسلي صغير أو مكرر من قبل المستقبل يتم تسجيل آخر ترتيب متقبل ويتجاهل الإطار المستقبل.



الشكل 12 لكل حزمة مفتاح

تستخدم لتحسين تشفير المعطيات بالاعتماد على أربعة نقاط.

1- لكل مفتاح حزمة، أي عنوان MAC للمرسل يستخدم للتشفير إضافة إلى IV وK كما في الشكل 12

ويمكن الوصول إلى كل STA تملك مجال حجمه 2^{*24} وتستخدم IV من 24 Bit. وعليه لا تحصل على S مشابهة.

المرسلة من STA مختلفة حيث تختلف مفاتيح الاتصال IV1 من STA إلى AP عنه من AP إلى STA مع IV1 وذلك يتحقق وفق خوارزمية RC4.

2- تحسين حماية تكامل المعطيات MAC .

3- تحسين IV بالاعتماد على حماية Replay-Attacker من خلال IV كأرقام متسلسلة. Replay-Attacker هي الاختراق للحزم التي تم الحصول عليها والتي ترسل بعد زمن قصير.

إذا تم استخدام IV كرقم متسلسل ستكون الحزم مع أرقام متسلسلة أقل من الحزم الجاهزة للوصول.

4- إدارة المفتاح والتبديل السريع للمفاتيح قبل جريان مجال القيم لـ IV وK.

- Virtual Private Network in WLAN (VPN)

لها سمعة طيبة جداً وهى معلومة لتأمين وصلة آمنة لـ End to End وسيتم بناء Tunnel آمن من أجل نقل المعطيات المستخدمة.

في حلول VPN نجد برتوكول للطبقة الثانية Layer 2 Tunneling Protocol (L2TP) أو برتوكول قناة طرف لطرف Point to Point Tunneling Protocol(TPTP) أو IP Security Protocol (IPSec) حيث إن كل من البرتوكولين L2TP وTPTP يدعيان بتقنية VPN غير الآمنة ويبدو ذلك مختلف مع IPSec ويتبع إلى التقنيات المستخدمة مع IPSec هل تم استخدام DES أو Triple DES أو AES .

DES تتحقق على مفتاح بطول 54 bits وثلاث DES تتم من خلال ثلاثة مفاتيح طول كل منها 54 bits والتي تعطي مفتاح بطول 168 bits أما AES تستخدم مفتاح بطول 128 or 192 or 256 bits وبمقارنة هذه التقنيات الثلاث نجد تفوق AES في مجال الآمن وكذلك فعالية تحقيق الخوارزمية المستخدمة، والتي تعطي AES آمن اكبر وفعالية أفضل، ولكن يبقى السؤال القائم إلى متى تقنيات التشفير الموجودة آمنة؟ يمكن القول حتى الآن لا توجد طريقة معلومة تستطيع كسر خوارزمية AES .

وفقط من خلال التجريب يمكن كسر مفتاح AES ويحتاج ذلك من أجل مفتاح بطول 128 bits إلى عدد من المحاولات 10^{38}* 3.402823669209384634633746074317 وهى طريقة استنزاف البحث عن المفتاح أو البحث ضمن كامل المجال Exhaustive Key Search.

وهذه هي طريقة البحث الخطي ضمن كامل الاحتمالات الممكنة للمفتاح حتى الوصول المؤكد عليه، ويستخدم البعض كمية قليلة من المعطيات والمحاولة من خلال تخمين تشفيرها للوصول للمفتاح الصحيح، وهذه الطريقة غير فعالة ويحتاج ذلك في وقتنا الراهن ومع التقنيات المتاحة للكمبيوترات إلى زمن غير معلوم، إن احتمال الوصول إلى المفتاح من خلال المحاولات الأولى هي مستبعدة جداً.

أن احتمال إيجاد مفتاح AES المؤلف من 128bits هو

10^{38}* 1/3.402823669209384634633746074317 ومن أجل المقارنة مع مفتاح DES والمؤلف من 56 bits مع مفتاح AES 128 bits نجد أنها أكثر بـ 10^{16}*7.2 مرة وبالتالي يكون الزمن المحتاج للوصول إلى AES أكبر من الزمن للوصول إلى DES هو 10^{21} مره أكثر،.

وباستخدام ألف كمبيوتر والتي تعطي 2000000 مفتاح في الثانية تحتاج إلى أكثر من 5 تريليون عام من أجل الوصول إلى مفتاح بطول 128 bit، وبالمقارنة مع تطور التقنيات ستكون الحواسب في المستقبل ذات قدرة أكبر وعلية يجب التفكير دائماً مع جيل جديد من AES .

وعليه يكون استخدام 192 bits التي تعطي آمن أكثر حيث نجد 10^{57}*6.2 بدل 10^{38}*3.4 ومع 256 bits نجد 10^{77}*1.1 وهى مطمئنة وعندما نصل إلى الحرج لابد من التفكير بما هو أفضل.

إن حل VPN ضمن شبكات WLAN سيتم استخدام مخدم VPN وزبون VPN ومخدمات VPN توجد في العادة بالحلول المادية والتي تعطي إمكانيات تقنية كافية وتؤمن فنوات VPN من أجل عدة محطات WLAN بالوقت نفسه والمشكلة أن AP سوف تقل قدرتها نظراً للتحميل، ولهذا السبب نجد استخدام حزمة ضيقة جاهزة للاستخدام.

ينعكس ذلك على المستخدمين الجوالين لكي يتم قبولهم في AP وتحقيق ذلك من قبل VPN خاصة عند تبديل AP الذي يتطلب بناء اتصال VPN جديد، وعلى محطات WLAN يتم بشكل نظام تجهيز مستخدم VPA والذي يملك خوارزمية التشفير، وهذا المستخدم يسمح له بتبادل المعطيات المشفرة وعلية إذا وصل إليها المخترق لا يمكنه إعادة الترميز من دون المفتاح السري وتصبح معطيات غير مفيدة.

تبنى فنوات VPN وفق شهادات تراخيص لمخدم VPN وكذلك مستخدم VPN وتملك هذه التراخيص مفاتيح سرية التي تستخدم من أجل تشفير وفك تشفير المعطيات وتخدم بالوقت نفسه المصادقة، فقط مستخدمي VPN التي تملك تراخيص فعالة تستطيع أن تبني قناة الاتصال مع مخدم VPN.

وفي حال وجود شبكتين سلكيتين وكانت الحاجة بربطهما لاسلكياً يتطلب الأمر مخدمين VPN من كل طرف ويجب حماية قوة الإرسال من خلال بناء اتصال VPN آمن وهنا من المهم أن يكون عرض مجال مخدمي VPN متساوٍ من أجل أن لا تكون هناك فجوة متوفرة للدخول.وعرض مجال الشبكة السلكية يجب أن يكون أكبر أو يساوي عرض مجال مخدمات VPN لكي لا نقع في مشكلة عنق الزجاجة.

- Advanced Encryption Standard (AES)

لقد طور 802.11i من أجل زيادة الحماية على المعطيات المنقولة والمعرفة Data Encryption Standard (DES) للوصول إلى AES هي مواصفة من المعهد العالمي للقياسات والتقانات NIST حيث تم تطوير DES من قبل Joan Daemen و Vincent Rijmen والخوارزمية المطورة عرفت Rijndael وهي خوارزمية سهلة التحقيق ضمن البنى المادية والبرمجية المطورة .

وحتى يومنا هذا لا توجد تقنيات لكسر هذه الخوارزمية وإنما لا يزال الباب مفتوحاً وخاصة عند Brute Force Attacker .

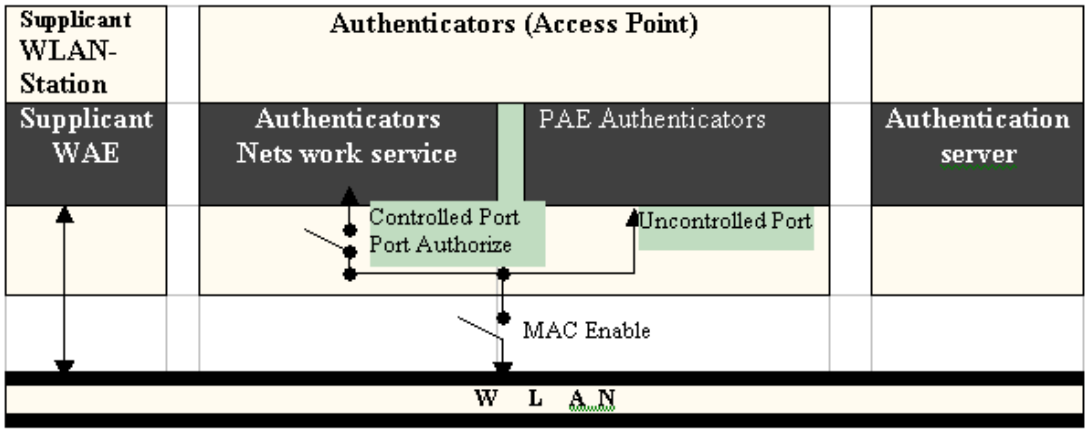
إن تقنية 802.11i EAS تبنى على 128 bits طول المفتاح ومع الحواسيب الحالية يحتاج المخترق إلى زمن عير محدد بدقة للاختراق، ويكمن عامل الأمن العالي في اقتراح مجموعة عمل تطوير 801.11i من التحقق عبر AES والمتواضعة على شريحة متكاملة ويتم تحديثها كلما دعت الحاجة.

ورغم عدم اعتراف IEEE بتطوير 802.11i على الأقل حتى خريف 2004 فإن بعض المنتجين لمركبات WLAN قاموا بتحقيق حلول TKIP ضمن منتجاتهم، وهذه المنتجات قد تعاني من بعض المشاكل في التوافقيات من منتج إلى أخر.

Authentication (RADIUS)

Remote Authentication Dial in user server(RADIUS) العناية دخول الشبكة من خلال التحقق من الاتصال من خلال Port Based Network Access control حيث تم وصف آلية جريان المعطيات من خلال البنية التحتية للشبكة والمعروف على مداخل البوابات وتوجد طرق مصادقة (تحقق) عديدة في 801.1x ولكن الأهم هو RADIUS ومع هذه يمكن تحديد المستخدم بمداخل محددة، والتي تحدد بدوره المصدر الذي يستخدمه المستخدم والمدة الزمنية للدخول وكذلك التحدث عن AAA (- Authentication من هو المستخدم - authorize وماذا يمكن أن يعمل المستخدم - Accounting وما المصادر التي استخدمها المستخدم)؟

في مجال WLANنقاط الدخول والمحطات تقوم بمناداة مخدم RADIUS من أجل المصادقة على العمل وهذا المخدم يمكن أن يكون proxy لمخدم RADIUS آخر وكذلك يمكن أن يتم توصيل السؤال إلى مخدم RADIUS آخر. وهذا الاتصال يجب أن يكون آمن وكما نرى ذلك في الشكل (14):



الشكل (14) بنية 802.2x

- Wi-Fi Protected Access :

في نهاية عام 2002 تم تسجيل تقانات أمن من قبل مجموعة Wi-Fi ما تدعى Wi-Fi protected Access (WPA) ومع WPA سيتم تحقيق تشفير معطيات بشكل أفضل ووضع عدد كبير من المنتجين لمركبات الشبكات يعطون WPA كخيار ضمن منتجاتهم.

WAP تستخدم تقانات الأمن المستقبلية من 802.11i والتي تم وضعها ضمن TKIP والمؤلفة من تطوير Initialize Vector و Re-Keying و Message Integrity Check .

WAP مفيدة فقط إذا كانت كل مركبات WLAN تعمل مع WAP ويتطلب الأمر تحديث كل مركبات الشبكة القديمة عبر برمجيات تحديث أو طرفيات جديدة(Adapter) .

ومن أجل استخدام الشبكة سيتم استخدام IEEE 802.1x and Extensible Authentications Protocol(EAP) والمستعملة من أجل الوصول إلى مخدم RADIUS في الشبكات الكبيرة. [9]

النتائج والتوصيات:

بعد مناقشة القياسية IEEE 802.11 المخصصة WLAN ومعظم تطويراتها وكذلك المواصفات لتبديل الاتصالات من أجل الوصل إلى الأفضل في مجال الأمن، وكذلك مواصفات الأمن من تكامل المعطيات والاستقرار والراحة لتبادل المعطيات وصحتها وما تعطيه هذه الشبكات من مرونة في الاستخدام وتوفير للجهد نجد ما يلي:

1- ضرورة تفعيل الإجراءات الأمنية والاقتراحات الأمنية بشك دائمً .

2- مراعاة التحسينات والاقتراح على WPA المقدمة من خلال ترقية للبرمجيات.

3- اعتماد الحماية على IPS_{ec} و VPN عالية الجودة.

4- مراعاة التطويرات التي تطبق على EAP والترقية من TKIP مع تشفير RC4 إلى تشفير AES والتي تعتبر ضمان لأمن وألفة تبادل المعطيات.

5- عدم وضع المعطيات الخطيرة والمهمة جداً والأبحاث السرية على شبكات WLAN ونرغب بالقول إنه لا يوجد نظام آمن 100% سوى النظام المعزول.

6- ولهذا نري أن استخدام هذه الشبكات ضمن ما ذكر سابقاً مع تحميل المعلومات المتعلقة بالخدمات والتعليم المفتوح والطباعة على طابعات الشبكة عن بعد من أي مكان يعتبر أمر ضروري ولا مفر منه نظراً للحسنات المشروحة سابقاً.

جدول المختصرات

AES..... Advanced Encryption Standard
AS ..... authenticate server
ASCII ..... American Standard Code for Information Interchange
c..... calculation CRC-32
C..... Chiffre text
CRC..... Cyclic Redundancy Checksum
id ..... Key Nummer
IP ..... Internet Protocol
ICV..... Integrity Check Value
IPsec..... IP Security Protocol
ISO..... International Standards Organization
IV ..... Initialisierungs Vektor
k..... hidden WEP Key
M..... Net data
MIC..... Message Integrity Code
MAC-Adresse ..... Medium Access Control Adresse
OSI ..... Open Systems Interconnection
P ..... M|c(M)_
pad..... Padding
PRNG..... Pseudo Random Number Generator
RC4 ..... Ron's Code 4
S ..... v|pad|id|C
SSID..... Service Set Identifier
SSL..... Secure Sockets Layer
TKIP..... Temporal Key Integrity Protocol
v..... Initialisierungs Vektor
VPN..... Virtual Private Network
WEP .....Wired Equivalent Privacy
Wi-Fi .....Wireless Fidelity
WPA.....Wi-Fi Protected Access
WLAN.....Wireless Local Area Network

المراجع:

1- RECH, J. – Wireless LANs. Heisen Zeitschriften Verlag GmbH & Co. KG, Hannover 2004, pp. 204-237.

2-NETT, E.; MOCK, Michael; GERGELEIT, Martin; Das drathlos Ethernet – Der IEEE 802.11 Standard, Datacom Akademie, Addison Wesley Muenchen 2001

3- IEEE Std 802.11b, part 11 : Wireless LAN Medium Access Control (MAC) and physical Layer (AHY) Specification, Higher-Speed Physical Layer Extension in the 2.4 GHz Band, Institute of Electrical and Electronics Engineers, Inc, New York, USA, 1999.

4- IEEE DRAFT 6.1 802.11g : Wireless LAN Medium Access Control (MAC) and physical Layer (AHY) Specification, Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band, Institute of Electrical and Electronics Engineers, Inc, New York, USA, 2003.

5- IEEE DRAFT 6.1 802.11i : Wireless LAN Medium Access Control (MAC) and physical Layer (AHY) Specification, Medium Access Control (MAC) Security Enhancements Institute of Electrical and Electronics Engineers, Inc, New York, USA, 2003.

6- IEEE DRAFT 2.2 802.11h : Wireless LAN Medium Access Control (MAC) and physical Layer (AHY) Specification, Spectrum Access and Transmit Power Management Extensions in the 5GHz Band in Europe, Institute of Electrical and Electronics Engineers, Inc, New York, USA, 2003.

7- NEWSHAM T, Cracking WEP Keys Mar 2003,
http://www.lava.net/~newsham/wlan/WEP/

8- FERGUSON N, DOS attack on WPA 802.11?Nov 2002,
http://www.mail-archive.com/cryptography@wasabisystems.com/msg03078.html

9- Wi-Fi IC Shipments Set To Top Expectations, According To ABI Study, Dec 2002
http://www.alliedworld.com/pdfs/wlic03pr.pdf

10-SULEIMAN A. - introduction to computer and algorithm Tishreen University 2006