فصل سوم

مقایسه پروتکل های امنیتی در شبکه های محلی بیسیم

۳-۱-مقدمه

امنیت اصلی ترین ضعف در تکنولوژی بیسیم می باشد، زیرا هیچ کنترلی روی کانال ارتباطی(رسانه بیسیم)وجود ندارد . در شبکه های سیمی هر رد و بدل اطلاعاتی باید به رسانه ارتباطی(سیم)دسترسی فیزیکی داشته باشد .رسانه ارتباطی

بیسیم یک رسانه باز است که هر کاربر با یک دستگاه مجهز به واسط بیسیم می تواند به استفاده و اشتراک گذاری انتقال اطلاعات از طریق رسانه ارتباطی امواج با دیگر کاربران بپردازد .برخی از اشکالات و ضعف های*WLAN* عبارتند از:

- نبود هیچگونه کنترل فیزیکی بر روی اتصالات شبکه بیسیم .
- ضعف توکار اقدامات امنیتی .
- اتصال غیر قابل اطمینان به هسته شبکه سیمی(بدون نظارت).

در سال های گذشته چندین پروتکل امنیتی(یعنی*WPA،WEP* و *IEEE 802.11i)* به منظور افزایش تصدیق هویت بیشتر، محرمانگی بیشتر و جامعیت (صحت) پیام بیشتر در*WLAN* ،توسعه یافته است.

هر مکانیزم امنیتی مورد استفاده در*WLAN* باید ویژگی های زیر را ارائه دهد:

محرمانگی : حفظ اطلاعات از دسترسی کاربران غیرمجاز .

تصدیق هویت : فرایندی که مشخص می کند ، آیا کاربر واقعا همان کسی است که خود را معرفی کرده است یا خیر. البته قبل از آنکه بتواند به منابع شبکه دسترسی پیدا کند.

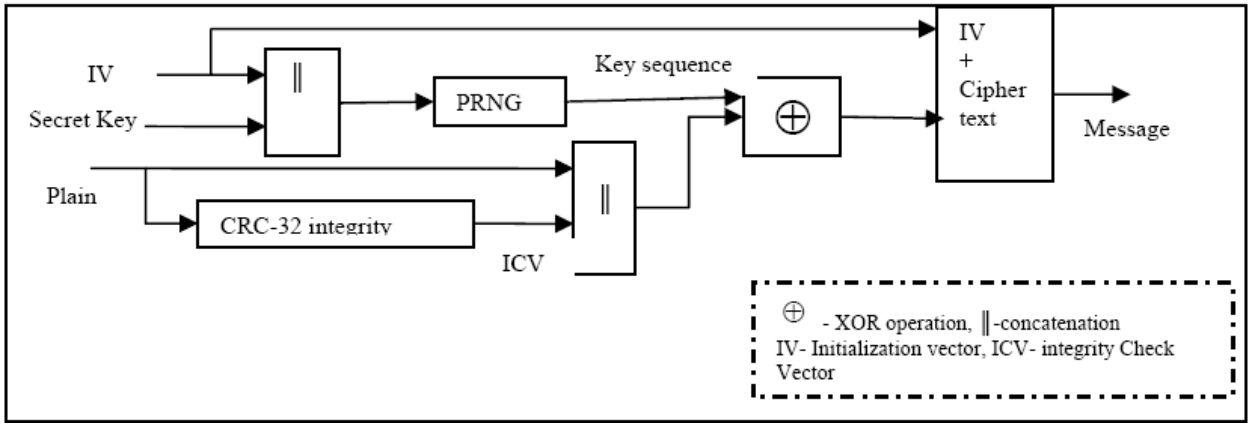
جامعیت (صحت) : چگونگی این که یک نفر مطمئن باشد که یک پیام دریافت شده ، در حین انتقال تغییر پیدا نکرده است.

این فصل تجزیه و تحلیلی از مهمترین و پرکاربردترین مکانیزم های اجرا شده ، به منظور حل مشکلات امنیتی*WLAN* ها، ارائه می دهد .ما قدرت ها و ضعف های این تکنولوژی ها را از نقطه نظر امنیتی معرفی می نماییم .این مقایسه همراه با نتایج به دست آمده در خصوص تاثیر این مکانیزم ها بر کارایی شبکه ، می تواند راهنمای ارزشمندی در تصمیم گیری برای انتخاب پروتکل امنیتی برای یک شبکه محلی بیسیم باشد.

(Wired Equivalent Privacy) WEP–۲–۳

WEP به منظور تدارک امنیت در شبکه های محلی بیسیم ، معادل با آنچه در شبکه های محلی سیمی وجود دارد ، به وجود آمد . الگوریتم*WEP* از یک عمل*xor* استفاده می کند، که بر روی متن(بیت به بیت) و با یک کلید نیمه تصادفی ترتیبی با طول برابر،انجام می شود.

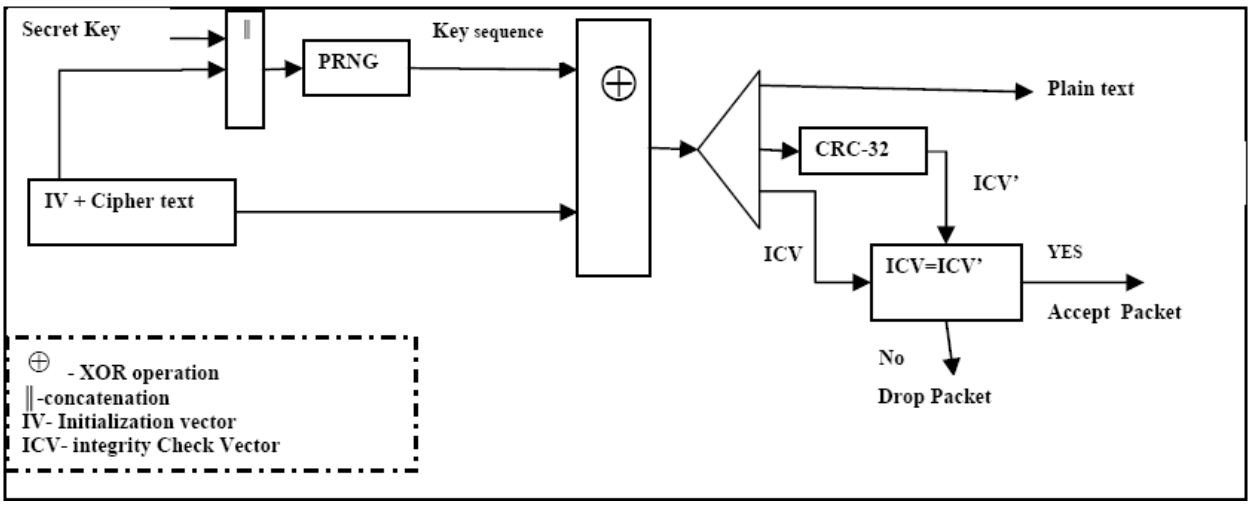
WEP یک الگوریتم متقارن است که از کلید یکسانی برای رمزنگاری و رمزگشایی استفاده می کند .رمزنگاری با کلید مخفیی شروع می شود که بین تمام ایستگاه های بیسیم توزیع شده است .کلید مخفی به یک بردار اولیه*(IV)* الحاق شده و نتیجه در ورودی تولید کننده نیمه تصادفی*(PRNG)* قرار می گیرد.*PRNG* یک دنباله کلید*(K)* از بایت های نیمه تصادفی تولید می کند که در اندازه برابراند با تعداد بایت های داده ایی که قرار است منتقل شوند، به اضافه۴(از آنجایی که دنباله کلید برای محافظت مقدار بررسی جامعیت*(ICV)* استفاده می شود (همانند داده ها)). فرایند رمزنگاری*WEP* در شکل ۳-۱ نشان داده شده است.



شکل۳ – *1* فرایند رمزنگاری*WEP*

بردار اولیه ممکن است برای هر بسته تغییر کند و از آنجایی که این بردار با پیام منتقل می شود، گیرنده همیشه قادر به رمزگشایی پیام خواهد بود .بردار اولیه به صورت یک متن واضح فرستاده می شود .زیرا باید برای گیرنده شناخته شده باشد تا بتواند عمل رمزگشایی را انجام دهد.

فرایند رمزگشایی با رسیدن یک پیام آغاز می شود .بردار اولیه موجود در پیام تازه رسیده ، برای تولید دنباله کلید لازم برای رمزگشایی پیام ، استفاده خواهد شد .ترکیب شدن متن کد شده و دنباله کلید ، متن اصلی و*ICV* را نتیجه می دهد . صحت رمزگشایی با انجام الگوریتم بررسی جامعیت بر روی متن اصلی بازیابی شده و مقایسه *ICV* ورودی با*ICV* منتقل شده به همراه پیام ، تایید می شود .اگر هر دو مقدار برابر نباشند، پیام دریافت شده، خراب تصور می شود . همانگونه که در شکل ۳-۲ نشان داده شده است. *WEP* فقط از کلیدهای رمزنگاری استفاده می کند و عمل تصدیق داده ها را انجام نمی دهد .بنابراین کلیدهای جامعیت داده ندارد.



شکل ۳-۲ فرایند رمزگشایی *WEP*

۳-۲-۱-مشکلات *WEP*

فضای محدود شده بردار اولیه : یکی از مشکلات *WEP* آن است که طول *IV* فقط *24* بیت است. یک *24 IV* بیتی بدین معناست که 2^{24} ترکیب مختلف وجود دارد و این به معنای آن است که 2^{24}فریم می تواند قبل از آنکه فضای *IV* تمام گردد، انتقال داده شوند .هنگامی که این اتفاق می افتد، *IV* در یک سیکل جدید و همانند ارزش های قبلی شروع به ارزش گیری می نماید .محدوده *IV* عملا نشان دهنده احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است.

برای *WLAN، IEEE 802.11g* با سرعت *54 Mb/s = 6750000* بایت در ثانیه عمل می نماید .با بسته های به طول *1500* بایت، در کل *4500* بسته در ثانیه ارسال خواهد شد .در نتیجه در *3728 = 4500 / 2^{24}* ثانیه، یعنی تقریبا *1*ساعت ، کلیدهای تکراری خواهیم داشت .که این زمان با بسته های با طول کمتر از *1500* بایت ، کمتر هم خواهد شد.

حملات غیر فعال : که به رمزگشایی ترافیک اشاره می کند .نفوذگر به استراق سمع تمام ترافیک بیسیم می پردازد . هنگامی که یک تلاقی *IV* رخ می دهد (دو بسته از *IV* یکسانی استفاده می کنند)،با *xor* کردن آن دو بسته کد شده، دومتن اصلی را به صورت زیر بدست می آورد:

فرض کنید *CT1* و *CT2* دو متن کد شده باشند که از *IV* یکسانی استفاده می کنند و *PT 1* و *PT2* دو متن اصلی باشند.

CT1= PT1⊕RC4 (IV, K) and CT2=PT2⊕RC4 (IV, K) then:

$$CT1 \oplus CT2 = (PT1 \oplus RC4(IV, K)) \oplus (PT2 \oplus RC4(IV, K)) = PT1 \oplus PT2.$$

می توان برای یکی از پیام ها تمام متن را بازیابی کرد و از آن پس برای تمام پیام ها که از بردار اولیه یکسانی استفاده می کنند ،متن مستقیما بدست می آید.

حملات فعال : به تغییر و تزریق ترافیک اشاره می کند .هنگامی که یک نفوذگر، متن دقیق یک پیام رمز شده را می داند، می تواند از این دانش به منظور ساخت بسته های رمزشده صحیح استفاده کند .روال مربوطه شامل ساخت یک پیام جدید، محاسبه *CRC-32* و انجام جابجایی و تغییر بیت ها بر روی پیام اصلی رمز شده است .ویژگی اصلی آن است که $RC4(X) \oplus X \oplus Y = RC4(Y)$. حال این پیام می تواند به یک نقطه دسترسی یا دستگاه بیسیم ارسال شود و به عنوان یک بسته معتبر ، پذیرفته خواهد شد .شکل دیگری از این حمله، تغییر بیت های انتخابی در یک پیام و تنظیم موفق *CRC*رمز شده است .چنانکه بتوان نسخه رمز شده صحیحی از بسته اصلاح شده بدست آورد .اگر مهاجم ، دانش جزئی درباره محتویات بسته داشته باشد، می تواند با رهگیری و استراق سمع به تغییر آن دست بزند.

اعتماد گذرا : اگر شبکه محلی بیسیم جزئی از یک شبکه بزرگ سازمانی باشد، مزاحمین می توانند با استفاده از یک دستگاه بیسیم اعتماد موقت و گذرایی را بدست آورده و خود را به عنوان یک گره یا نقطه دسترسی معرفی کنند و تمام ایستگاه های بیسیم به جای ارتباط با یک نقطه دسترسی واقعی، سعی در برقراری ارتباط با آن می نمایند.

حمله های عدم پذیرش سرویس*(DoS)* : این نوع از حملات می توانند با استفاده از یک فرستنده قوی ، برای ایجاد سیگنال های رادیویی قدرتمند ، انجام شوند .این سیگنال ها که در انتقال های*WLAN* دخالت می کنند، باعث می شوند که دستگاه های بیسیم قادر به استفاده از مسیر رادیویی نباشند.

۳-۳-*WPA (Wi-Fi Protected Access)*

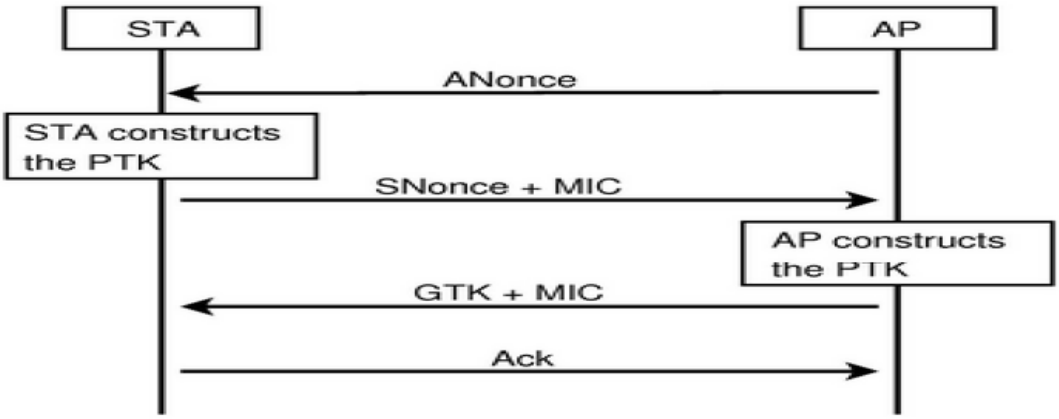
استاندارد دسترسی محافظت شده به*Wi-Fi (WPA)* به عنوان یک جایگزین موقت برای*WEP* معرفی شد .به عنوان یک نسخه موقت از مشخصات امنیتی*IEEE 802.11i*،*WPA* از*TKIP* به منظور رفع نواقص پروتکل*WEP* و تامین جامعیت بسته استفاده نمود.

WPA دو نوع فرایند تصدیق هویت دارد:*PSK (PreShared Key)* و*IEEE 802.1x* .

- در روش تصدیق هویت*PSK* ، یک کلید به صورت دستی بر روی هر دستگاه شبکه بیسیم تنظیم می شود . از *PSK*مستقیما به عنوان*PMK (Pairwise Master Key)* که برای ایجاد دیگر کلیدها در رمزنگاری تولید شده است ، استفاده می شود .از آنجا که روش*PSK* ساده تر است، در صورت استفاده از روش تصدیق هویت *IEEE 802.1x*، برخی از معایب آن نمایان نخواهد شد .کلید*PSK* که به صورت دستی تنظیم شده است، در صورت نیاز می تواند بر روی هر یک از وسایل شبکه بیسیم تغییر کند.
- در صورت استفاده از روش تصدیق هویت*IEEE 802.1x*، نرم افزار سرویس دهنده تصدیق هویت خاصی مورد نیازاست که با عنوان سرویس دهنده *AAA (Authentication, Authorization and Accounting)*شناخته شدهاست .نقطه دسترسی نیاز به تصدیق هویت خود به مشتری بیسیم و استخراج کلیدهای رمزنگاریی دارد که در رمز کردن ترافیک استفاده می شوند .با استفاده از پروتکل تبادل پیام*EAP* (پروتکل تصدیق هویت توسعه پذیر که قالب پیام های انتها به انتها را تعریف می کند که این پیام ها در یک محاوره بین مشتری و سرویس دهنده تصدیق هوت مورد استفاده قرار می گیرند)، کلید مخفی اشتراکی*PMK* ارائه می شود .بنابراین یک *4 Handshake* طرفه برای ایجاد کلیدی دیگر استفاده می شود ، که به این کلید*PTK (Pairwise Transient Key)* گفته می شود.*PTK* از به هم پیوستن خصوصیات زیر تولید می شود:*PMK*، *(Access Point Nonce) Anonce*،*(Station Nonce) Snonce*، آدرسِ *MAC* نقطه دسترسی و آدرس*MAC* ایستگاه .رشته حاصل در نهایت به تابع*Hash* رمزنگاری*MD 5* داده می شود.

همچنین*Handshake* ، منجر به کلید موقتی گروهی *(GTK)* می شود، که از آن برای رمزگشایی ترافیک پخشی استفاده می شود. پیام های واقعی که در طول*Handshake* مبادله می شوند ، در شکل شماره ۳-۳ نشان داده شده اند.

- نقطه دسترسی*Anonce* را به ایستگاه ارسال می کند .هم اکنون مشتری*PTK* را می سازد.
- مشتری*Snonce* را به همراه یک*MIC (Message Integrity Code)* که بعدا توضیح داده خواهد شد) به نقطه دسترسی می فرستد.
- نقطه دسترسی*GTK* و یک شماره توالی را به همراه یک*MIC* دیگر ارسال می کند .شماره توالی شماره سریالی است که در عمل پخشِ قاب بعدی مورد استفاده قرار می گیرد.
- ایستگاه یک پیام تایید به نقطه دسترسی ارسال می کند.



فرایند ۳-۳ شکل *4 Handshake* طرفه

به محض اینکه*PTK* بدست آمد، به سه کلید جداگانه تقسیم می شود.

- کلید تائید *EAPOL-Key* - کلید مورد استفاده برای محاسبه *MIC* برای بسته های *EAPOL-Key*
- کلید رمزنگاری *EAPOL-Key* – کلید نورد استفاده برای تامین محرمانگی برای بسته های *EAPOL-Key*
- کلید موقتی *(TK)* – کلید مورد استفاده برای رمزنگاری ترافیک بیسیم واقعی

پروتکل تصدیق هویت توسعه یافته *(EAP)* یک چارچوب تصدیق هویت است که تعدادی از عملکردهای عادی و یک مذاکره از مکانیزم تصدیق هویت مطلوب ارائه می دهد .هنگامی که *EAP* توسط یک دستگاه تصدیق هویت *802. 1 x* مانند یک نقطه دسترسی بیسیم، فراخوانی می شود، متدهای *EAP* می توانند یک مکانیزم تصدیق هویت امن ارائه داده و یک *PMK* امن بین سرویس دهنده تصدیق هویت و مشتری رد و بدل کنند .پس از آن می توان از *PMK* برای رمزنگاری بیسیم استفاده کرد که از *TKIP* (پروتکل جامعیت کلید موقتی) یا *CCMP* *(authentication code Protocol Counter mode with Cipher block chaining Message)* استفاده می کند.

یکی از متدهای *EAP* که در *802.1 x* استفاده می شود *EAP-TLS*، است که برای ایمن سازی ارتباطات در سرویس دهنده تصدیق یا هر نوع دیگری از سرویس دهنده تصدیق ، از زیرساخت کلید عمومی *(PKI)* استفاده می کند. نیاز *EAP-TLS RADIUS* آن است که هم مشتری و هم سرویس دهنده یک گواهی معتبر از یک مقام قابل اطمینان داشته

باشند .بنابراین هرچند که*EAP-TLS* امنیتی عالی فراهم می کند ، اما سربار ناشی از گواهی های سمت مشتری یک اشکال محسوب می شود.

الگوریتم رمزنگاری استفاده شده در*WPA* پروتکل جامعیت کلید موقتی*(TKIP)* است که از*IV* و*4 CR* استفاده می کند .اما*IV* به *48* بیت گسترش یافته و به عنوان شمارنده توالی*TKIP (TSC)* مورد استفاده است *16* .بیت اول*TSC* در فیلد*WEP IV* ذخیره می شود درحالیکه *32* بیت باقیمانده در فیلدی با نام*IV* گسترش یافته ذخیره می شود .در نتیجه واحد داده پروتکل برای جا دادن این فیلد اضافی ، گسترش یافته است.*TSC 48* بیتی یک شمارنده افزایشی است که زمانیکه کلید موقتی*TKIP* مقداردهی اولیه می شود یا تغییر می یابد، مقدار یک می گیرد .هر فریم دریافت شده بایستی*TSC* ی بیشتر از*TSC* فریم قبلی دریافت شده از همان فرستنده داشته باشد .این کار باعث محافظت در برابر حمله پاسخ جعلی می شود . فضای *48TSC* بیتی است . یعنی می توان 2^{48}=*281474976710656* فریم را قبل از اینکه تمام مقادیر*TSC* برای یک کلید موقتی استفاده شوند، ارسال کرد .یک نقطه دسترسی که با سرعت *54* مگابیت بر ثانیه، به صورت متوالی ، بسته های *1500* بایتی را ارسال می کند، بیش از *1983* سال نیاز دارد تا یک فضای*TSC* را مصرف کند .برای شبکه های بیسیم*IEEE 802.11g* این عدد و موضوع صادق است.

TKIP یک کد صحت پیام *(MIC)*۶۴ بیتی به نام *Michael* دارد که از آن برای محافظت پیام ها از تغییر در حین عبور استفاده می نماید.*MIC* از روی آدرس مبدا و مقصد، یک فیاد اولویت، *3* بایت ذخیره شده و کل قسمت اصلی متن ساخته می شود. *MIC* حملات فعال را تشخیص داده و اقدامات متقابل را برای جلوگیری کردن از حملات آینده بکار می گیرد.*WEP ICV* هنوز هم در رابطه با تشخیص های غلط ناشی از اشتباه های*MIC* و در نتیجه اقدامات متقابل اشتباه، مورد استفاده است.

***(Wi-Fi Protected Setup) WPS*–۴–۳**

این پروتکل نوظهور که توسط اتحادیه*Wi-Fi* ایجاد شد و رسما در سال *2007* راه اندازی شد و راه اندازی حفاظت شده *Wi-Fi* نامیده می شود، برای استقرار آسان و امن یک شبکه بیسیم طراحی شده است .این استاندارد *4* روش برای اضافه کردن یک دستگاه جدید به شبکه تعریف می نماید.*2* اجباری و *2* اختیاری .ما گزینه های اجباری را شرح می دهیم که درزیر شرح داده شده اند:

- روش *PIN* : یک *PIN* (شماره شناسایی شخصی) بایستی از برچسب هر ایستگاه خوانده شود .این روش اجباری است وهر محصول مجاز *WPS* باید آن را پشتیبانی کند.
- روش پیکربندی دکمه فشاری *(PBC)* : کاربر به سادگی باید یک کلید را بفشارد .خواه یک کلید واقعی و یا یک نمونه مجازی از آن . هم در نقطه دسترسی و هم در دستگاه جدید مشتری بیسیم .پشتیبانی از این مدل برای نقاط دسترسی اجباری و برای ایستگاه ها اختیاری است.

پروتکل *WPS* سه نوع دستگاه را در یک شبکه تعریف می کند.

۱) ثبت کننده *(Registrar)* : دستگاهی با توانایی صدور و لغو اعتبار نامه در یک شبکه .یک ثبت کننده ممکن است در یک نقطه دسترسی قرار گیرد و یا از آن جدا باشد.

۲) متقاضی *(Enrollee)* : دستگاهی که به دنبال پیوستن به یک شبکه *LAN* بیسیم است.

۳) تصدیق کننده : یک نقطه دسترسی که به عنوان یک پروکسی بین ثبت کننده و متقاضی عمل می کند.

برای کلید توزیع و پیکربندی شبکه امن ،*WPS* از دو نوع عمل استفاده می نماید .*In-band* و *out-of-band*. در حالت پیکربندی *In-band* ،*PIN* یا کلمه عبور مورد استفاده است .در حالت پیکربندی *out-of-band* یک درایو فلش *NFC* یا *USB* (ارتباطات نزدیک میدان) مورد استفاده است.

همچنین *WPS* یه مفهوم را از پروتکل ثبت نام ، به عنوان پروتکل های *in-band* سه بخشی، برای اختصاص اعتبارنامه به متقاضی، ارائه می دهد .پروتکل بین متقاضی و ثبت کننده عمل نموده و ممکن است پشتیبانی هایی از یک پروکسی دریافت کند . در حالت پروتکل ثبت نام ، به کاربر پیامی داده می شود که کلمه عبور دستگاه را وارد کند .سپس ثبت کننده یک پیام شامل توضیحات را با متقاضی می فرستد .این پیام متقاضی را قادر می سازد تا دستورات لازم را به کاربر داده و آنها را در استفاده از ثبت کننده صحیح راهنمایی می کند .دیگر پیام های پروتکل ثبت نام در رابطه با دانش مربوط به کلمه عبور دستگاه بوده و سپس داده های پیکربندی رمز شده ، رد و بدل می شوند .حفاظت مخفی برای پیام ها بر پایه روش *KDK (Key Derivation Key)* می باشد، که از مقادیری همچون آدرس *MAC* متقاضی و غیره ، محاسبه می شود.

۳-۴-۱-امنیت *WPS*

پروتکل ثبت نام *WPS* برای محافظت قوی در برابر حمله های غیر فعال و همچنین تشخیص و محافظت سیستم از حمله

، برای پیکربندی های *in-band* و *out-of-band* طراحی شده است.

برای پیکربندی *in-band* ، اگر یک ثبت کننده یک مهاجم را تشخیص دهد که وانمود می کند یک متقاضی قانونی است، ابتدا تشخیص می دهد که مهاجم کلمه عبور را نمی داند .این تشخیص قبل از آنکه پروتکل ثبت نام اطلاعات کافی برای افشای کلمه رمزرا به مهجم بدهد، رخ می دهد .در برخورد با مهاجم ، اگر یک خطای ارتباطی یا تصدیق *PIN* بعد از ارسال پیام خاصی رخ دهد ، ثبت کننده به کاربر هشدار داده و به صورت خودکار از آن *PIN* استفاده نخواهد کرد .ثبت کننده یک *PIN* مشابه را بدون صدور هشدار به کاربر نخواهد پذیرفت .اگر به جای *PIN* ، یک کلمه عبور قوی با حداقل *32* بایت تصادفی استفاده شود، ثبت کننده اجازه دارد که از این کلمه عبور ، چندین بار استفاده کند .بدون اینکه هشداری به کاربر در مورد خطاهای رخ داده بدهد. برای پیکربندی *out-of-band*، کلمات عبور طولانی (مانند *256* بیت با مقادیر تصادفی) می توانند برای ثبت کننده ارسال شوند، که شامل کلید عمومی متقاضی نیز می شوند.

کلید رمز شده می تواند از یک کلید مشتق شده از کلید عمومی *Diffe-Hellman* ، متعلق به ثبت نام کننده استفاده کند که ازکانال *in-band* بدست آمده است .این کار در زمانی انجام می شود که ثبت کننده تنظیمات مربوط به متقاضی را رمز می کند.در پیکربندی *out-of-band* ، یک درایو فلش *USB* یا یک *NFC*(ارتباطات نزدیک میدان .یک تکنولوژی اتصال کوتاه برد است که برای اعمال کمتر از *10* سانتیمتر کاربرد دارد) استفاده می شود .اگر برای وارد کردن رمز دستگاه از *USB* یا *NFC* استفاده شود، ثبت کننده *hash* مربوط به کلید عمومی *Diffe-Hellman* مربوط به متقاضی را نیز ارائه می دهد . این فرایند، تصدیق هویت متقاضی توسط ثبت کننده زا تقویت می نماید.

۳-۵-آسیب پذیری از حالت *PSK* از *WPA*

نسخه *PSK* از *WPA* از حمله فرهنگ لغت که به صورت *offline* انجام می شود، رنج می برد .زیرا پخش اطلاعات نیاز به ایجاد ورسیدگی یک کلید *Session* دارد .در حالت *WPA* ،*PMK* (کلید اصلی) به منظور ایجاد *PTK* و نصب آن بر روی هر دو طرف، تولید می شود.

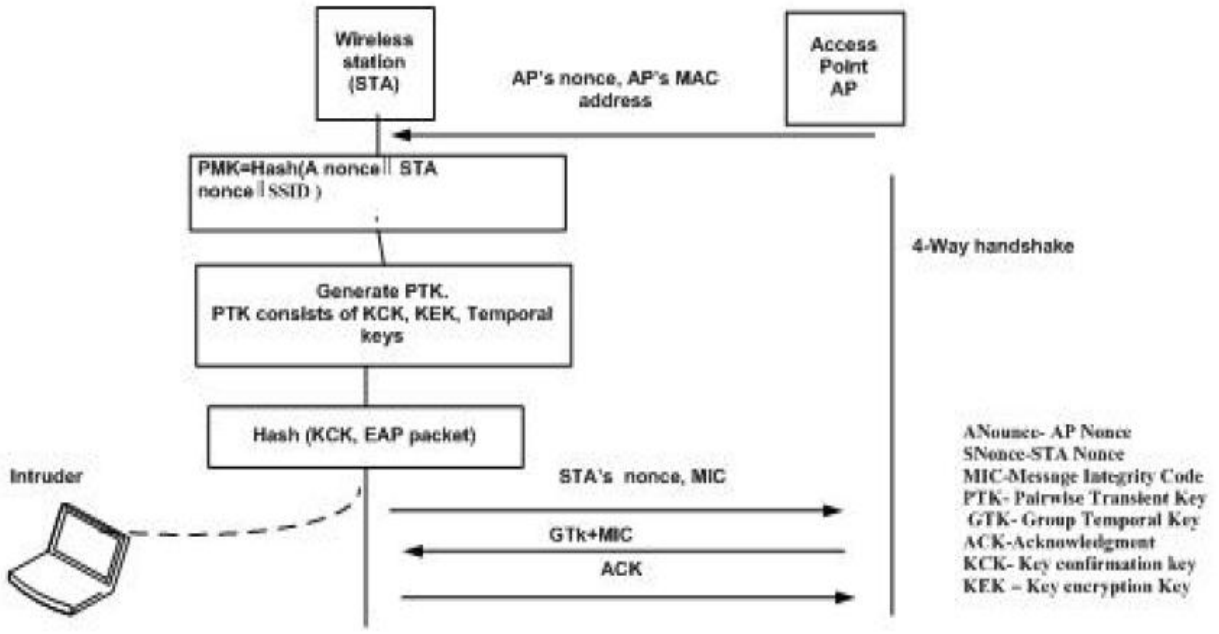
PTK از ورودی های زیر ایجاد می شود :

- رشته ای از کلمه عبور
- *SSID (Service Set IDentifier)* (نام واحد و حساس به متن یک شبکه بیسیم)

- طول $SSID$

که این ورودی ها در یک الگوریتم $hash$ استفاده شده و پس از انجام 4096 مرتبه عمل $hash$ ، یک مقدار 256 بیتی تولید می شود .از آنجا که $SSID$ به راحتی قابل بازیابی است، باید یادآور شد که به منظور تشخیص یک PMK معتبر ، فقط باید یک عبارت عبور را حدس زد.

به علاوه در تولید PTK برای مقاصد کرک کردن، از آنجایی که همه دیگر فیلدها می توانند به صورت بدیهی کشف شوند، فقط نیاز است که PMK مشخص شود .اولین مرحله از $4Handshake$ طرفه، $Anonce$ و آدرس MAC نقطه دسترسی را مشخص می کند .حال آنکه دومین مرحله، $Snonce$ و آدرس MAC ایستگاه را مشخص می نماید و فقط امضای PTK تولید می شود .پس از دریافت اولین بسته در $4Handshake$ طرفه ، مشتری PTK را تولید کرده و تابع $MD5\ hash$ را روی KCK و بسته EAP که باید ارسال شود، اجرا می کند .بعد از آن این $hash$ به بسته EAP اضافه شده و به عنوان مرحله دوم ، روی شبکه ارسال می شود .حال یک مزاحم می تواند از قسمت $hash$ این بسته استفاده کرده و آن را با $hash$ حاصل از PTK ایی که حدس زده و بسته EAP جمع شده ، مطابقت دهد .عبارت عبور درست حدس زده شده، امضای یکسانی تولید می کند .بنابراین مزاحم می تواند با استراق سمعِ غیر فعال به دو بسته $EAPOL$ ، یک حمله فرهنگ لغت $offline$ را شروع کند .این حمله در شکل ۳-۴ نشان داده شده است.



شکل ۳-۴ حمله فرهنگ لغت غیرفعال*WPA*

***IEEE 802.11i*-۶-۳**

خصوصیات*IEEE 802.11i* راه حلی برای استاندارد*IEEE 802.11* در تامین امنیت بهتر و حل مشکلات امنیتی *WEP*است. *IEEE 802.11i* شامل چندین خصوصیت کلیدی می باشد :

- الگوریتم های رمزنگاری

-*TKIP* به منظور پشتیبانی از دستگاه های سنتی، *IEEE 802.11*، *TKIP* را به عنوان یکی از الگوریتم های رمزنگاری استفاده می کند .(همانند*WPA*)

*IEEE 802.11i -CCMP*همچنین شامل پروتکل رمزنگاری دیگری به نام*AES-CCMP* است. *AES* به معنای استاندارد رمزنگاری پیشرفته است که یکی از الگوریتم های قوی در رمزنگاری است. *AES-CCMP* به سخت افزارهای اضافی برای استفاده نیاز دارد.

-جامعیت (صحت) پیام

مانند یک الگوریتم جامعیت داده قدرتمند (بررسی جامعیت پیام*Michael)* اعمال می شود(*WPA)*

-تصدیق هویت متقابل

802.11i از *802.1x/EAP* برای تصدیق هویت کاربران استفاده می کند (مانند*WPA*)

-دیگر خصوصیات امنیتی

مجموعه خدمات پایه ای مستقل*(IBSS)* امن، جابهجایی سریع و امن(دستگاه بیسیم می تواند از یک نقطه دسترسی به یک نقطه دسترسی دیگر جا به جا شود ، بدون اینکه اختلالی در انتقال داده ها به وجود آید) و خدمات قطع ارتباط امن.

-پشتیبانی از*Roaming*

IEEE 802.11i دو کلاس از الگوریتم های امنیتی برای شبکه های*IEEE 802.11* تعریف می کند:

۱) الگوریتم هایی برای ایجاد و استفاده از انجمن شبکه امنیتی قدرتمند که الگوریتم های*RSNA* نامیده می شود .*CCMP*، *TKIP)*، توابه تشکیل و قطع*RSNA*، شامل استفاده از تصدیق هویت*IEEE 802.1x* و روال های مدیریت کلید)

۲) الگوریتم های*Pre-RSNA* *(*تصدیق هویت*WEP)*

یک ایستگاه بیسیم می تواند به طور همزمان الگوریتم های*RSNA* و*Pre-RSNA* را انجام دهد.

۳-۷-انجمن های امنیتی

IEEE 802.11 برای شرح یک عملیات امن از نماد یک انجمن امنیتی استفاده می کند .یک انجمن امنیتی مجموعه ای از سیاست ها و کلیدهای مورد استفاده برای محافظت اطلاعات است .اطلاعات در داخل انجمن امنیتی ، توسط تمام بخش ها ذخیره شده و باید در بین تمام بخش ها سازگار باشد و باید یک هویت داشته باشد.

چهار نوع انجمن امنیتی که توسط *RSN STA* پشتیبانی می شود، وجود دارد.

1) PMKSA (Pairwise Master Key Security Association) : نتیجه یک تبادل تصدیق هویت موفق در *IEEE802.1 x* مابین یک ایستگاه و یک سرویس دهنده تصدیق هویت*(AS)* یا از یک*PSK* ، اطلاعات*PMK* یا *PMK* ی کش شده توسط دیگر مکانیزم ها.

2) PTKSA (Pairwise Transient Key Security Association) : نتیجه حاصل از یک *4Handshake* طرفه که مابین ایستگاه و تصدیق هویت کننده رد و بدل می شوند.

3) GTKSA (Group Temporal Key Security Association) : نتیجه حاصل از پخش موفقِ *GTR (Group Temporal Key)*که از طریق*Handshake* کلید گروهی و یا یک *4Handshake* طرفه مبادله می شود.

4) STA KEY SA (STA Key Security Association) : زمینه امنیتی برای ارتباط مستقیم ایستگاه به ایستگاه در یک مجموعه از خدمات پایه ای زیر بنایی

۳-۸-روش های امنیتی*Pre-RSNA*

در یک مجموعه سرویس توسعه یافته*ESS* (دو یا تعداد بیشتری نقطه دسترسی بیسیم، در حالی که نقاط دسترسی به شبکه سیمی متصل هستند)، هر ایستگاه بیسیم باید یک مبادله تصدیق هویت*IEEE 802.11* را با شبکه کامل کند . چنین تبادلی در یک شبکه *IBSS* انتخابی است .(مجموعه خدمات پایه ای مستقل، حداقل از دو ایستگاه بیسیم ، بدون نقطه دسترسی، تشکیل شده است).

۳-۹-پروتکل های محرمانگی داده در *RSNA*

IEEE 802.11i دو پروتکل برای تامین محرمانگی و صحت آن در *RSNA* تعریف می کند: *TKIP* (همانند *WPA*) و *CCMP* .اجرا *CCMP* برای تمام دستگاه های سازگار با *RSNA* اجباری خواهد بود .اجرای *TKIP* برای یک *RSNA* اختیاری است .برای *TKIP* هدف آن بود که الگوریتم باید برای دستگاه هایی که فقط از *WEP* پشتیبانی می کنند ، سازگار باشد . تنها بروزرسانیسیستم عامل برای پشتیبانی *TKIP* لازم است .وسایل *RSNA* باید در هنگام ارتباط با دستگاه هایی که قادر به ارتباط با *CCMP* نیستند، فقط از *TKIP* استفاده کنند.

۳-۱۰-*(CTR with CBC-Mac Protocol) CCMP*

CCMP، محرمانگی، تصدیق هویت، صحت و محافظت در برابر پاسخ جعلی را تامین می نماید.*CCMP* یک پروتکل رمزنگاری *IEEE 802.11i* است که برای جانشین شدن همراه با *TKIP* در پروتکل ناامن *WEP* ساخته شده است و از الگوریتم رمزنگاری *AES* استفاده می کند. *CCMP* ،*CTR* را برای محرمانگی و *CBC-Mac* را برای تصدیق هویت و صحت ترکیب می نماید. *CCMP* از جامعیت و صحت داده های انتقالی محافظت می کند .برای قبول *RSN* ،اجرای *CCMP* اجباری است.

همه پردازش *AES* ، استفاده شده توسط *CCMP*، از یک کلید *128* بیتی و یک بلوک با اندازه *128* بیت استفاده می کند. *CCMP* یک حالت عمومی است که می تواند با هر الگوریتم رمزنگاری بلوک گرا استفاده شود.

*CCMP*برای هر نشست ، نیاز به یک کلید موقت تازه دارد .همچنین *CCMP* برای هر فریمی که توسط کلید موقتی محافظت می شود، نیاز به یک مقدار واحد دارد .برای این هدف *CCMP* از یک شماره بسته *(PN) 48*بیتی استفاده می کند .استفاده مجدد از *PN* با یک کلید موقت مشابه، امنیت *CCMP* را مختل می کند.

پردازش *CCMP* ، اندازه اصلی *MPDU (Medium access control Protocol Data Unit)*را توسعه می دهد، که واحدداده های مبادله شده بین دو *MAC* نظیر هم است. *16* بایت و *8* بایت برای سرآیند *CCMP* و *8* بایت

برای فیلد*MIC* .فیلد سرآیند*CCMP* از شماره بسته،*EXTIV* و زیر فیلد*Key ID* تشکیل شده است.*CCMP* از *WEP ICV* استفاده نمی کند.*CCMP* قسمت اصلی متن*MPDU* را رمز کرده و متن رمزی حاصل را کپسوله می نماید .که این کار در مراحل زیر انجام می شود:

۱) افزایش*PN* با یک شماره مثبت برای هر*MPDU* . شماره بسته برای یک سری از*MPDU*ها که از کلید موقت یکسانی استفاده می کنند، تکرار نخواهد شد.

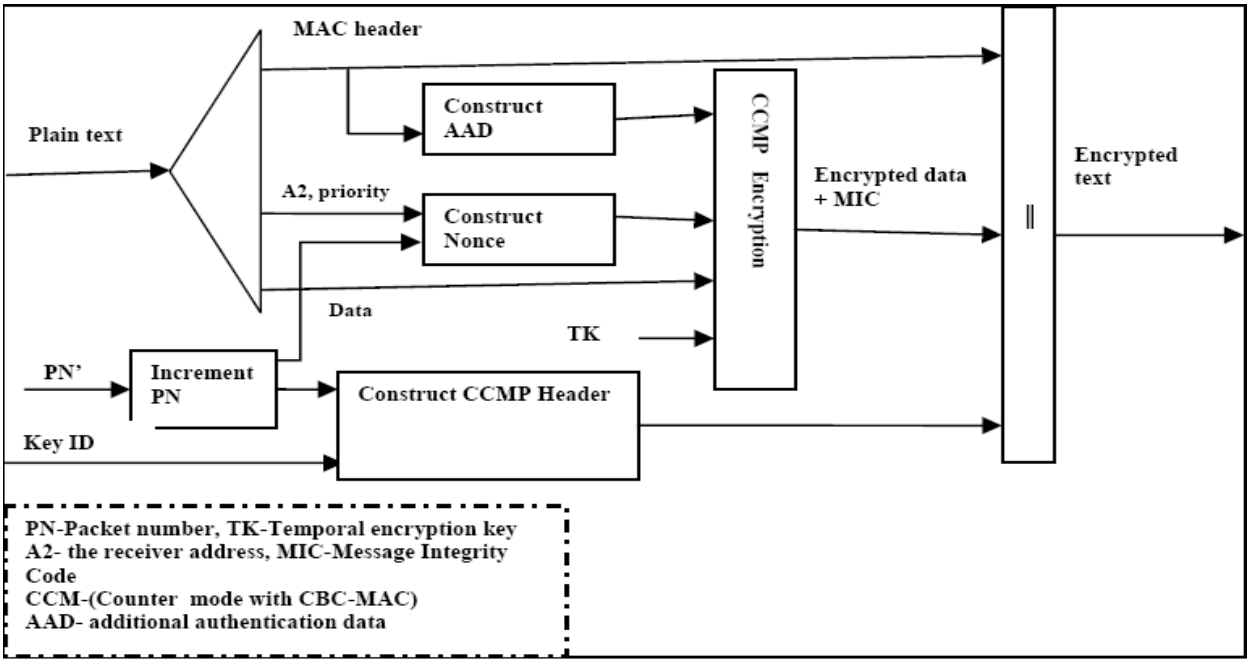
۲) استفاده از فیلدهای موجود در سرآیند*MPDU* ،به منظور ساخت داده تصدیق اضافی *AAD* *(Authentication Data Additional)*برای *CCM*. الگوریتم*CCM* برای فیلدهای موجود در*AAD* جامعیت و صحت را فراهم می کند.

۳) ساخت بلوک*CCM* از شماره بسته،*A 2* و فیلد اولویت*MPDU* . که*A 2* برابر با آدرس *MPDU 2* است . فیلد اولویت، یک مقدار رزرو شده که مقدار اولیه صفر می گیرد دارد.

۴) قرار دادن شماره بسته جدید و شناسه کلیدی در سرآیند*CCMP* .

۵) استفاده کردن از کلید موقتی،*AAD*،*nonce* و داده*MPDU* برای ایجاد متن رمزی و*MIC* . این مرحله به عنوان پردازش تولید کننده*CCM* شناخته می شود .پردازش تولید کننده*CCM* تصدیق هویت و صحت بدنه فریم را تامین می محرمانگی نماید و همچنین*AAD* فریم را تامین می نماید .خروجی پردازش تولید کننده *CCM* از داده رمز شده و*8* بایت اضافی رمز شده*MIC* ، تشکیل شده است.

۶) شکل دهی*MPDU* رمز شده با ترکیب کردن سرآیند*MPDU* اصلی ، سرآیند*CCMP* ، داده رمزنگاری شده و*MIC* . فرایند رمزنگاری*CCMP* در شکل ۳-۵ نشان داده شده است.



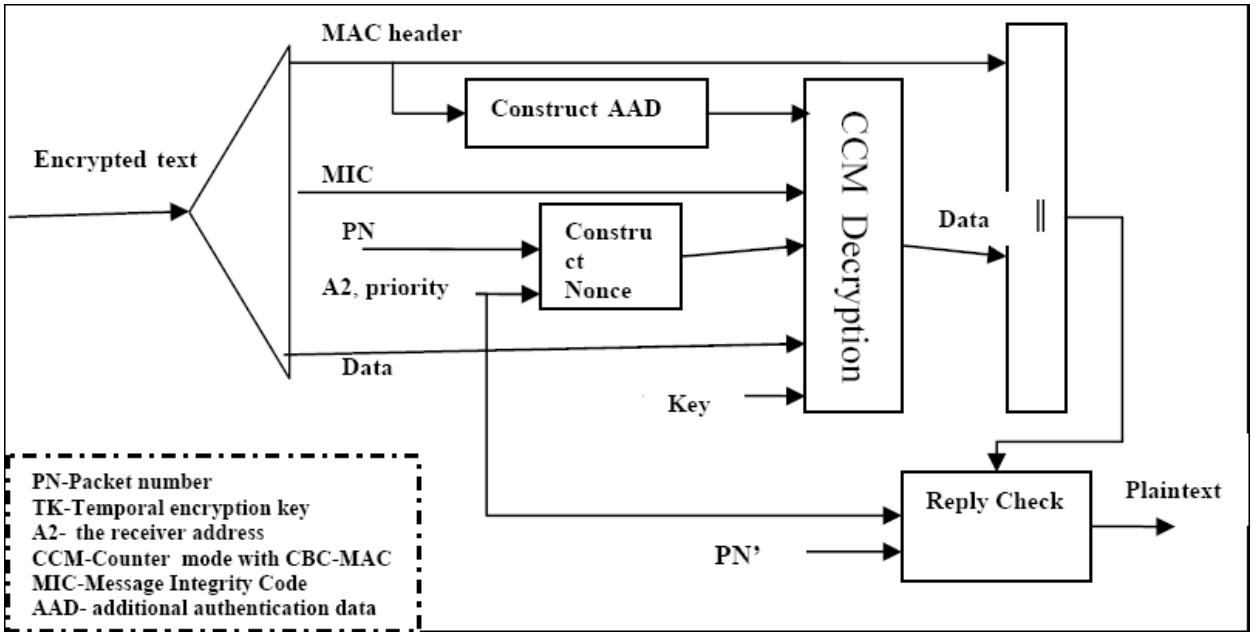
شکل ۳-۵ فرایند رن*CCMP*

CCMP قسمت اصلی از متن *MPDU* رمزی را رمزگشایی کرده و آن را از حالت کپسوله خارج می کند .این مراحل عبارتند از:

1) *MPDU* رمز شده برای ساخت *AAD* و مقادیر *nonce* ، تجزیه می شود.
۲) *AAD* از سرآیند *MPDU* رمز شده شکل می گیرد.
۳) مقدار *nonce* از فیلدهای *PN*، *A 2* و اولویت ساخته می شود .
۴) *MIC* برای استفاده در بررسی جامعیت و صحت *CCM* ، استخراج می شود.
۵) پردازشِ گیرنده *CCM* ، از کلید موقتی، *AAD* ، *nonce* ، *MIC* و متن رمزی *MPDU* استفاده می کند تا متن اصلی *MPDU* را بازیابی کرده و همچنین صحت *AAD* و *MPDU* را بررسی نماید.

سرآیند *MPDU* و متن اصلی *MPDU* از پردازش گیرنده *CCM* ، ممکن است برای ساخت متن اصلی *MPDU* با هم الحاق شوند.پردازش رمزگشایی از *Replay* کردن *MPDU* جلوگیری می نماید .این کار با بررسی *PN* مربوط به *MPDU* انجام می شود که بزرگتر از شمارنده *Replay* نگهداشته شده می باشد.

فرایند *Decapsulation* زمانی اتفاق می افتد که *MIC* محاسبه شده ، با مقدار *MIC* بدست آمده از رمزگشایی *MPDU* رمز شده رسیده ، برابر باشد .سرآیند *MPDU* اصلی با متن اصلی حاصل از پردازش گیرنده *CCM* موفق الحاق شده، متن اصلی *MPDU* را می سازد .فرایند رمزگشایی *CCMP* در شکل ۳-۶ نشان داده شده است.



شکل ۳-۶ فرایند رمزگشایی *CCMP*

۳-۱۱-آسیب پذیری

آسیب پذیری احتمالی *IEEE 802.11i* مربوط به حملات *DoS* می باشد .تا زمانی که فریم های مدیریتی و فر یم های کنترلی محافظت نشده باشند، مهاجمان می توانند به راحتی این فریم ها را جعل نموده و یک حمله *DoS* را انجام دهند .در میان حملات فریم مدیریت ، کارآمدترین حمله ، جعل و ارسال چندین باره فریم های عدم تصدیق یا قطع همکاری می باشد .این آسیب پذیری را می توان با استفاده از یک مدیریت مرکزی که به امور فریم ها رسیدگی می کند و فریم های جعلی را با رفتار غیرمعمول آنها شناسایی می نماید، کاهش داد .جدول ۳-۱ مقیسه ای بین پروتکل های امنیتی مورد استفاده در *WLAN* را از نقطه نظر آسیب پذیری های امنیتی نشان می دهد.

Security threat	Does the protocol open to the threat		
	WEP	WPA	IEEE 802.11i
Weak encryption	Yes	No (TKIP and AES are strong Encryption protocols	No (TKIP and AES are strong Encryption protocols
Off line dictionary attacks	Yes	Pre-shared key Mode is exposed	No((IEEE820.1x is used)
Illegitimate message Deletion and insertion	Yes	No (MIC is used)	No (CCMP is used)
Man in the Middle attack (MITM)	Yes	Pre-shared key Mode is exposed	No (IEEE820.1x is used)
Media Access Control (MAC) spoofing	Yes	Pre-shared key Mode is exposed	No (IEEE820.1x is used)
Man in the Middle attack (MITM):	Yes	Pre-shared key Mode is exposed	No (IEEE820.1x is used)
Rouge Access point	Yes	Yes (unless IEEE802.1x is used)	No
Denial-of-Service attacks (DoS)	Yes	Yes	Yes

جدول۳-۱ آسیب پذیری های امنیتی پروتکل های امنیتی مختلف

۳-۱۲ -مقایسه پروتکل های امنیتی

هنگامی که بررسی پروتکل های امنیتی$WLAN$ می پردازیم، معیارهای مختلفی وجود دارند که بایستی مد نظر قرار گیرند.

- سطح امنیتی که پروتکل های امنیتی مختلف تامین می کنند.
- این پروتکل ها چه میزان از کارایی شبکه می کاهند.
- ارتقاهای نرم افزاری و سخت افزاری مورد نیاز برای اجرای پروتکل های امنیتی مختلف.
- امکان اجرای این ها روی سخت افزار بیسیم قدیمی.
- چه پروتکل امنیتی برای یک اندازه بخصوص از شبکه مناسب است.

از بحث بالا در مورد پروتکل های امنیتی می توانیم به این نتیجه برسیم که اجرایWEP آسان استو نیازی به ارتقاء سخت افزار یا نرم افزار ندارد .اماWEP ضعیف ترین پروتکل امنیتی است و چندین نقطه ضعف دارد .مانند: فضای محدودIV ، حملات فعال و غیر فعال و حمله اعتماد موقت گذرا .WEP فقط برای استفاده خانگی مناسب است . WPA دفاع های مناسبی در برابر تهدیدات وارده بهWEP فراهم می نماید .زیرا:

- شمارنده توالی *TKIP (TSC)* به ازای هر بسته افزایش می یابد تا از حمله *Replay* جلوگیری کند.
- با *TSC* طولانی *48* بیتی، مشکل فضای محدود *IV* حل می شود.
- در برابر حملات فعال و غیر فعال محافظت می کند، زیرا هیچ دو بسته ای با شماره *IV* یکسان نخواهند بود.

برای رمزنگاری *WPA* از الگوریتم رمزنگاری *TKIP* با *RC4* و *IV* استفاده می کند. (به طریقی مشابه *WEP*)، اما فضای بیشتر کلید *TKIP* باعث می شود که از *WEP* قوی تر باشد. *TKIP* از الگوریتم *MIC* برای جلوگیری از تغییر پیام در طول انتقال استفاده می نماید.

آسیب پذیری احتمالی *WPA* هنگامی که از حالت *PSK* استفاده می کند، حمله فرهنگ لغت بروت از خط می باشد . این حمله می تواند با استفاده از پروتکل *WPS* کاهش یابد .که به طور اتوماتیک کلیدها و پیکربندی شبکه را توزیع می نماید . این فرایند خودکار ، امن است . زیرا از تصدیق *Diffe-Hellman* استفاده می کند. *WPA* برای استفاده در شبکه های کوچک و متوسط مناسب است.

در نهایت *IEEE 802.11i* بهترین سطح امنیتی را در میان همه پروتکل ها ارائه می دهد .زیرا از یک الگوریتم قوی در رمزنگاری استفاده می کند *(AES* بر پایه *CCMP)*، صحت داده *(CBC-MAC)*،محافظت در برابر تکرار *(PN)* و تصدیق هویت قوی تر *(IEEE 802.1x/EAP-TLS)*. به علاوه *IEEE 802.11i* خصوصیات امنیتی دیگری نیز دارد . نظیر : رد کردن سریع، عدم تصدیق سریع، قطع همکاری و پشتیبانی *Roaming* .

از سوی دیگر *IEEE 802.11i* از دستگاه های قدیمی پشتیبانی نکرده و برای اجرا نیاز به سخت افزار و نرم افزار اضافی دارد.تاثیر پروتکل های امنیتی مختلف بر کارایی شبکه از لحاظ مختلف قابل بررسی است .بر روی شبکه های با بار کاری مختلف (معمولی و متراکم)، با اندازه بسته های مختلف(*100* بایت تا *1500* بایت)و ... .نتایج بررسی ها نشان می دهد که برای انواع شبکه از لحاظ حجم کاری و اندازه بسته مختلف، *WEP* بهترین کارایی را دارد .استفاده از *WPA* منجر به کارایی متوسط (استفاده از رمزنگاری *TKIP)* و کارایی یکسان با *WEP* با استفاده از رمزنگاری *AES* به جای *TKIP* می شود.

در نهایت *IEEE 802.11i* به دلیل پردازش های بیش از حد مورد نیاز برای تصدیق ، رمزنگاری و ایجاد انجمن های امنیتی، ضعیف ترین کارایی شبکه را ارائه می دهد. *IEEE 802.11i* یک انتخاب بسیار خوب برای امنیت *WLAN* های بسیار بزرگ است .جدول۳-۲ شامل مقایسه ای بین فاکتورهای اصلی در پروتکل های امنیتی استفاده شده در *WLA* ها است.

	WEP	WPA	IEEE 802.11i
Encryption	WEP (RC4)	TKIP (RC4)	CCMP (AES)
Key length	40 bits or104 bits	128 bits encryption	128 bits or higher
Data integrity	CRC-32	Michael	CBC-MAC
Replay protection	N/A	Packet number	Packet number
Authentication	Open or Shared Key	IEEE 802.1x or Pre-shared Key	IEEE 802.11X
Network performance	High network performance than WPA and IEEE 802.11i	Less than or almost the same as WEP performance and higher than IEEE 802.11i	Less network performance than WEP, WPA

جدول ۳-۲ مقایسه بین فاکتورهای اصلی پروتکل های امنیتی مختلف

۳-۱۳-نتیجه گیری

استفاده از شبکه های محلی بیسیم به سرعت در حال رشد است .اگر چه*WLAN* های اولیه برای افزایش امنیت قوی طراحی نشده بودند، با این حال استانداردها و روش هایی برای امنیت*WLAN* ها در حال پیدایش هستند .پروتکل ها *IEEE 802.1x*و*IEEE802.11* هم اکنون راه حل های مناسبی برای رمزنگاری و تصدیق هویت هستند .این خصوصیات امنیتی نوظهور به منظور تضمین امنیت اطلاعات باید بر روی شبکه های بیسیم اجرا شوند.

در این مقاله ما پروتکل های امنیتی*WLAN* را ارائه دادیم*(WEP ، WPA ،IEEE 802.11i)* و مزایا و معاب آنها را از نقطه نظر امنیتی شناختیم .در انتخاب پروتکل امنیتی مناسب ، نباید کارایی شبکه فراموش شود.

ما به این نتیجه رسیدیم که انتخاب پروتکل امنیتی مناسب به سه فاکتور وابسته است :اندازه سازمان (زیر ساخت شبکه، سخت افزار و نرم افزار در دسترس)، سطح امنیتی مورد نظر و کارایی مورد قبول در شبکه .با انتخاب *IEEE 802.11i* به بالاترین سطح امنیتی و پایین ترین سطح کارایی می رسیم. *WPA* یک سطح امنیتی متوسط فراهم می کند(با استفاده از رمزنگاری*AES* ، سطح امنیتی قوی تر و کارایی بالاتر قابل حصول است) .در نهایت به دلیل ضعف امنیتی*WEP* توصیه می شود که از این روش فقط برای دستگاه های قدیمی و برای دستگاه های خانگی استفاده کنید.

۳-۱۴ -جدول کلمات مخفف

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption standard
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
EAP	Extensible Authentication Protocol
EAP-TLS	EAP-Transport Layer Security
GTK	Group Temporal Key
ICV	Integrity Check Vector
IV	Initialization Vector
KCK	Key confirmation Key
KDK	Key Derivation Key
KEK	Key Encryption Key
MIC	Message Integrity Code
NFC	Near Field Communication
PIN	Personal Identification Number
PMK	Pairwise Master Key
PTK	Pairwise Transient Key
PSK	Preshared Key
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
TK	Temporal Key
TKIP	Temporary Key Integrity Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

*متاسفانه نام گردآورنده ی اصلی مشخص نیست. لطفا اگر کسی از دوستان گردآورنده اصلی این اثر را می‌شناسند در انجمن ذکر نمایند تا رسما مورد تشکر قرار گرفته و نامشان در ذیل مطلب ذکر گردد.

کتابها

1- Giese, Xenia. Cisco Networking Academy Program. Indianapolis, Ind: Cisco press, 2005.

2- Network+ certification training kit. Redmond, Washington:Microsoft press, 2007.

3-"Computer Networks", Andrew S. Tanenbaum, 4th Edition, 2004

4- Network+ certification training kit. Redmond, Washington:Microsoft press, 2004.

5- Pohlmann,Thomas and Szall,Karen.NETWORK CERTIFICATION.Washington:Microsoft press,2001

مقالات

معرفی ومقایسه پروتکل های امنیتی در شبکه های بیسیم،نویسنده:مهندس امین علیمردانی

معرفی شبکه بیسیم ،نویسنده :سهراب نیازی ، وب سایت :*www.niazisoft.blogfa.com*

شبکه های بیسیم و انواع آن، نویسنده:علی اکبر سرداری

سایت ها

http://www.mtaghiloo.persianblog.ir

http://www.ee.sharif.ir

http://www.sciengacademy.com

http://www.manet.blogsky.com

http://www.daneshjui.ir

http://www.itshenas.com

http://www.it-rasht.blogfa.com

http://www.ramzetoosi.com

http://www.irantarjomeh.com

http://www.forum.persianadmins.ir

http://www.sosacom.blogfa.com

http://www.daneshju.ir

http://www.itshenas.com

http://compnenteorking.about.com http://Fcit.usf.edu/network/chap5/chap5.htm

http://Fcit.usf.edu/network/chap2/chap2.htm

http://www.Webopedia.com/Term/T/Tcp_Ip.htm

http://wwwinterworks.org/conference/Tcptutorial

http://www.pcwebopedia.com/quick_ref/osi_layers.asp

http://www.user_emea.com/education http://www.pcweopedia.com/concentrators.htm

http://www.alaska.net/~research/netrout.htm

http://www.cisco.com/univered/cc/td/doc/cisintwk/ito_doc

http://www.lantronix.com/htmfiles/catalog/et.htm