امنیت در شبکه هاي بي سيم

تهیه و تدوین : محمد رضا غلامی

از آن جا که شبکه های بی سیم، در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه ها، که بر اساس سیگنال های رادیویی اند، مهم ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نقاط قوت و ضعف آن ست. نظر به لزوم آگاهی از خطرات استفاده از این شبکه ها، با وجود امکانات نهفته در آن ها که به مدد پیکربندی صحیح می توان به سطح قابل قبولی از بعد امنیتی دست یافت، بنا داریم در این سری از مقالات با عنوان «امنیت در شبکه های بی سیم» ضمن معرفی این شبکه ها با تأکید بر ابعاد امنیتی آن ها، به روش های پیکربندی صحیح که احتمال رخ داد حملات را کاهش می دهند بپردازیم.

شبکه های بی سیم، کاربردها، مزایا و ابعاد

تکنولوژی شبکه های بی سیم، با استفاده از انتقال داده ها توسط اموج رادیویی، در ساده ترین صورت، به تجهیزات سخت افزاری امکان می دهد تا بدون استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه های بی سیم بازه ی وسیعی از کاربردها، از ساختارهای پیچیده یی چون شبکه های بی سیم سلولی -که اغلب برای تلفن های همراه استفاده می شود- و شبکه های محلی بی سیم (WLAN – Wireless LAN) گرفته تا انوع ساده یی چون هدفون های بی سیم، را شامل می شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می کنند، مانند صفحه کلید ها، ماوس ها و برخی از گوشی های همراه، در این دسته بندی جای می گیرند. طبیعی ترین مزیت استفاده از این شبکه ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این گونه شبکه ها و هم چنین امکان ایجاد تغییر در ساختار مجازی آن هاست. از نظر ابعاد ساختاری، شبکه های بی سیم به سه دسته تقسیم می گردندWWAN : ، WLANو.WPAN

مقصود ازWWAN ، که مخفف Wireless WAN است، شبکه هایی با پوشش بی سیم بالاست. نمونه یی از این شبکه ها، ساختار بی سیم سلولی مورد استفاده در شبکه های تلفن همراه است .WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می کند. کاربرد شبکه های WPAN یا Wireless Personal Area Network برای موارد خانه گی است .ارتباطاتی چون Bluetoothو مادون قرمز در این دسته قرار می گیرند .

شبکه های WPAN از سوی دیگر در دسته ی شبکه های Ad Hoc نیز قرار می گیرند .

در شبکه هایAd hoc ، یک سخت افزار، به محض ورود به فضای تحت پوشش آن، به صورت پویا به شبکه اضافه می شود. مثالی از این نوع شبکه ها، Bluetoothاست. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرارگرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده ها با دیگر تجهیزات متصل به شبکه را می یابند. تفاوت میان شبکه های Ad hoc با شبکه های محلی بی سیم (WLAN) در ساختار مجازی آن هاست. به عبارت دیگر، ساختار مجازی شبکه های محلی بی سیم بر پایه ی طرحی ایستاست درحالی که شبکه های Ad hoc از هر نظر پویا هستند .طبیعی ست که در کنار مزایایی که این پویایی برای استفاده کننده گان فراهم می کند، حفظ امنیت چنین شبکه هایی نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حل های موجود برای افزایش امنیت در این شبکه ها، خصوصاً در انواعی همچونBluetooth ، کاستن از شعاع پوشش سیگنال های شبکه است. در واقع مستقل از این حقیقت که عمل کرد Bluetooth بر اساس فرستنده و گیرنده های کم توان استوار است و این مزیت در کامپیوترهای جیبی برتری قابل توجه یی محسوب می گردد، همین کمی توان سخت افزار مربوطه، موجب وجود منطقه ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب می گردد .به عبارت دیگر این مزیت به همراه استفاده از کدهای رمز نه چندان پیچیده، تنها حربه های امنیتی این دسته از شبکه ها به حساب می آیند.

منشأ ضعف امنیتی در شبکه های بی سیم و خطرات معمول

خطر معمول در کلیه ی شبکه های بی سیم مستقل از پروتکل و تکنولوژی مورد نظر، بر مزیت اصلی این تکنولوژی که همان پویایی ساختار، مبتنی بر استفاده از سیگنال های رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه چندان قدرت مند این شبکه ها، خود را به عنوان عضوی از این شبکه ها جازده و در صورت تحقق این امر، امکان دست یابی به اطلاعات حیاتی، حمله به سرویس دهنده گان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره های شبکه با یکدیگر، تولید داده های غیرواقعی و گمراه کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت های مخرب وجود دارد .

در مجموع، در تمامی دسته های شبکه های بی سیم، از دید امنیتی حقایقی مشترک صادق است:

- تمامی ضعف های امنیتی موجود در شبکه های سیمی، در مورد شبکه های بی سیم نیز صدق می کند. در واقع نه تنها هیچ جنبه یی چه از لحاظ طراحی و چه از لحاظ ساختاری، خاص شبکه های بی سیم وجود ندارد که سطح بالاتری از امنیت منطقی را ایجاد کند، بلکه همان گونه که ذکر شد مخاطرات ویژه یی را نیز موجب است.
- نفوذگران، با گذر از تدابیر امنیتی موجود، می توانند به راحتی به منابع اطلاعاتی موجود بر روی سیستم های رایانه یی دست یابند.
- اطلاعات حیاتی یی که یا رمز نشده اند و یا با روشی با امنیت پایین رمز شده اند، و میان دو گره در شبکه های بی سیم در حال انتقال می باشند، می توانند توسط نفوذگران سرقت شده یا تغییر یابند .
- حمله های DoS به تجهیزات و سیستم های بی سیم بسیار متداول است.
- نفوذگران با سرقت کدهای عبور و دیگر عناصر امنیتی مشابه کاربران مجاز در شبکه های بی سیم، می توانند به شبکه ی مورد نظر بدون هیچ مانعی متصل گردند.
- با سرقت عناصر امنیتی، یک نفوذگر می تواند رفتار یک کاربر را پایش کند. از این

طریق می توان به اطلاعات حساس دیگری نیز دست یافت.
•کامپیوترهای قابل حمل و جیبی، که امکان و اجازه ی استفاده از شبکه ی بی سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت افزارهایی، می توان اولین قدم برای نفوذ به شبکه را برداشت.
•یک نفوذگر می تواند از نقاط مشترک میان یک شبکه ی بی سیم در یک سازمان و شبکه ی سیمی آن (که در اغلب موارد شبکه ی اصلی و حساس تری محسوب می گردد (استفاده کرده و با نفوذ به شبکه ی بی سیم عملاً راهی برای دست یابی به منابع شبکه ی سیمی نیز بیابد.
•در سطحی دیگر، با نفوذ به عناصر کنترل کننده ی یک شبکه ی بی سیم، امکان ایجاد اختلال در عمل کرد شبکه نیز وجود دارد.

پیشینه

تکنولوژی و صنعت WLAN به اوایل دهه ی ۸۰ میلادی باز می گردد. مانند هر تکنولوژی دیگری، پیشرفت شبکه های محلی بی سیم به کندی صورت می پذیرفت. با ارایه ی استانداردIEEE 802.11b ، که پهنای باند نسبتاً بالایی را برای شبکه های محلی امکان پذیر می ساخت، استفاده از این تکنولوژی وسعت بیشتری یافت. در حال حاضر، مقصود از WLAN تمامی پروتکل ها و استانداردهای خانواده ی IEEE 802.11 است.
جدول زیر اختصاصات این دسته از استانداردها را به صورت کلی نشان می دهد

اولین شبکه ی محلی بی سیم تجاری توسط Motorola پیاده سازی شد. این شبکه، به عنوان یک نمونه از این شبکه ها، هزینه یی بالا و پهنای باندی پایین را تحمیل می کرد که ابداً مقرون به صرفه نبود. از همان زمان به بعد، در اوایل دهه ی ۹۰ میلادی، پروژه ی استاندارد ۸۰۲.۱۱ در IEEE شروع شد. پس از نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای ۸۰۲.۱۱ aو ۸۰۲.۱۱ bتوسط IEEE نهایی شده و تولید محصولات بسیاری بر پایه ی این استانداردها آغاز شد. نوعa ، با استفاده از فرکانس حامل GHz۵، پهنای باندی تا ٥٤ Mbpsرا فراهم می کند. در حالی که نوع b با استفاده از فرکانس حامل GHz۲.٤، تا ۱۱ Mbpsپهنای باند را پشتیبانی می کند. با این وجود تعداد کانال های قابل استفاده در نوع b در مقایسه با نوعa ، بیش تر است. تعداد این کانال ها، با توجه به کشور مورد نظر، تفاوت می کند. در حالت معمول، مقصود از WLANاستاندارد ۸۰۲.۱۱ bاست .

استاندارد دیگری نیز به تاز ه گی توسط IEEE معرفی شده است که به ۸۰۲.۱۱ g شناخته می شود. این استاندارد بر اساس فرکانس حامل ۲.٤ GHzعمل می کند ولی با استفاده از روش های نوینی می تواند پهنای باند قابل استفاده را تا 54Mbps بالا ببرد. تولید محصولات بر اساس این استاندارد، که مدت زیادی از نهایی شدن و معرفی آن نمی گذرد، بیش از یک سال است که آغاز شده و با توجه سازگاری آن با استاندارد ۸۰۲.۱۱ b، استفاده از آن در شبکه های بی سیم آرام آرام در حال گسترش است.

معماری شبکه های محلی بی سیم

استاندارد ۸۰۲.۱۱ bبه تجهیزات اجازه می دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارت اند از برقراری ارتباط به صورت نقطه به نقطه– همان گونه در شبکه های Ad hoc به کار می رود- و اتصال به شبکه از طریق نقاط تماس یا

دسترسی .(AP=Access Point)

معماری معمول در شبکه های محلی بی سیم بر مبنای استفاده از AP است. با نصب یکAP ، عملاً مرزهای یک سلول مشخص می شود و با روش هایی می توان یک سخت افزار مجهز به امکان ارتباط بر اساس استاندارد ۸۰۲.۱۱ bرا میان سلول های مختلف حرکت داد. گستره یی که یک AP پوشش می دهد را BSS(Basic Service Set)می نامند. مجموعه ی تمامی سلول های یک ساختار کلی شبکه، که ترکیبی ازBSS های شبکه است، را ESS(Extended Service Set) می نامند. با استفاده از ESS می توان گستره ی وسیع تری را تحت پوشش شبکه ی محلی بی سیم درآورد .

در سمت هریک از سخت افزارها که معمولاً مخدوم هستند، کارت شبکه یی مجهز به یک مودم بی سیم قرار دارد که با AP ارتباط را برقرار می کند .AP علاوه بر ارتباط با چند کارت شبکه ی بی سیم، به بستر پرسرعت تر شبکه ی سیمی مجموعه نیز متصل است و از این طریق ارتباط میان مخدوم های مجهز به کارت شبکه ی بی سیم و شبکه ی اصلی برقرار می شود. شکل زیر نمایی از این ساختار را نشان می دهد:

همان گونه که گفته شد، اغلب شبکه های محلی بی سیم بر اساس ساختار فوق، که به نوع Infrastructure نیز موسوم است، پیاده سازی می شوند. با این وجود نوع دیگری از شبکه های محلی بی سیم نیز وجود دارند که از همان منطق نقطه به نقطه استفاده می کنند. در این شبکه ها که عموماً Ad hoc نامیده می شوند یک نقطه ی مرکزی برای دسترسی وجود ندارد و سخت افزارهای همراه – مانند کامپیوترهای کیفی و جیبی یا گوشی های موبایل – با ورود به محدوده ی تحت پوشش این شبکه، به دیگر تجهیزات مشابه متصل می گردند. این شبکه ها به بستر شبکه ی سیمی متصل نیستند و به همین منظور IBSS (Independent Basic Service Set)نیز خواند می شوند. شکل زیر شمایی ساده از یک شبکه ی Ad hoc را نشان می دهد :

شبکه های Ad hoc از سویی مشابه شبکه های محلی درون دفتر کار هستند که در آنها نیازی به تعریف و پیکربندی یک سیستم رایانه یی به عنوان خادم وجود ندارد. در این صورت تمامی تجهیزات متصل به این شبکه می توانند پرونده های مورد نظر خود را با دیگر گره ها به اشتراک بگذارند.

عناصر فعال شبکه های محلی بی سیم

در شبکه های محلی بی سیم معمولاً دو نوع عنصر فعال وجود دارد:

ایستگاه بی سیم

ایستگاه یا مخدوم بی سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه ی بی سیم به شبکه ی محلی متصل می شود. این ایستگاه می تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پویش گر بارکد نیز باشد. در برخی از کاربردها برای این که استفاده از سیم در پایانه های رایانه یی برای طراح و مجری دردسر ساز است، برای این پایانه ها که معمولاً در داخل

کیوسک هایی به همین منظور تعبیه می شود، از امکان اتصال بی سیم به شبکه ی محلی استفاده می کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به صورت سرخود مجهز هستند و نیازی به اضافه کردن یک کارت شبکه ی بی سیم نیست .
کارت های شبکه ی بی سیم عموماً برای استفاده در چاک های PCMCIA است. در صورت نیاز به استفاده از این کارت ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت ها را بر روی چاک های گسترش PCI نصب می کنند.

نقطه ی دسترسی

نقاط دسترسی در شبکه های بی سیم، همان گونه که در قسمت های پیش نیز در مورد آن صحبت شد، سخت افزارهای فعالی هستند که عملاً نقش سوییچ در شبکه های بی سیم را بازی کرده، امکان اتصال به شبکه های سیمی را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سیمی است و توسط این نقاط دسترسی، مخدوم ها و ایستگاه های بی سیم به شبکه ی سیمی اصلی متصل می گردد.

برد و سطح پوشش

شعاع پوشش شبکه ی بی سیم بر اساس استاندارد ۸۰۲.۱۱ به فاکتورهای بسیاری بسته گی دارد که برخی از آن ها به شرح زیر هستند:

-پهنای باند مورد استفاده
-منابع امواج ارسالی و محل قرارگیری فرستنده ها و گیرنده ها
-مشخصات فضای قرارگیری و نصب تجهیزات شبکه ی بی سیم

قدرت امواج

نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین ۲۹متر (برای فضاهای بسته ی داخلی) و ۴۸۵متر)برای فضاهای باز) در استاندارد ۸۰۲.۱۱ bمتغیر است. با این وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده ها و فرستنده های نسبتاً قدرت مندی که مورد استفاده قرار می گیرند، امکان استفاده از این پروتکل و گیرنده ها و فرستنده های آن، تا چند کیلومتر هم وجود دارد که نمونه های عملی آن فراوان اند.

با این وجود شعاع کلی یی که برای استفاده از این پروتکل (۸۰۲.۱۱ (bذکر می شود چیزی میان ۵۰ تا ۱۰۰متر است. این شعاع عمل کرد مقداری ست که برای محل های بسته و ساختمان های چند طبقه نیز معتبر بوده و می تواند مورد استناد قرار گیرد.

یکی از عمل کردهای نقاط دسترسی به عنوان سوییچ های بی سیم، عمل اتصال میان حوزه های بی سیم است. به عبارت دیگر با استفاده از چند سوییچ بی سیم می توان عمل کردی مشابه Bridge برای شبکه های بی سیم را به دست آورد.

اتصال میان نقاط دست رسی می تواند به صورت نقطه به نقطه، برای ایجاد اتصال میان دو زیرشبکه به یکدیگر، یا به صورت نقطه یی به چند نقطه یا بالعکس برای ایجاد اتصال میان زیرشبکه های مختلف به یکدیگر به صورت همزمان صورت گیرد.

نقاط دسترسی یی که به عنوان پل ارتباطی میان شبکه های محلی با یکدیگر استفاده می شوند از قدرت بالاتری برای ارسال داده استفاده می کنند و این به

معنای شعاع پوشش بالاتر است. این سخت افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمان هایی به کار می روند که فاصله ی آن ها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصله یی متوسط بر اساس پروتکل ۸۰۲.۱۱ bاست. برای پروتکل های دیگری چون ۸۰۲.۱۱ aمی توان فواصل بیشتری را نیز به دست آورد.

از دیگر استفاده های نقاط دسترسی با برد بالا می توان به امکان توسعه ی شعاع پوشش شبکه های بی سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه ی بی سیم، می توان از چند نقطه ی دست رسی بی سیم به صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می توان با استفاده از یک فرستنده ی دیگر در بالای هریک از ساختمان ها، سطح پوشش شبکه را تا ساختمان های دیگر گسترش داد .

امنیت در شبکه های محلی بر اساس استاندارد ۸۰۲.۱۱

استاندارد ۸۰۲.۱۱ سرویس های مجزا و مشخصی را برای تأمین یک محیط امن بی سیم در اختیار قرار می دهد. این سرویس ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy)تأمین می گردند و وظیفه ی آن ها امن سازی ارتباط میان مخدوم ها و نقاط دسترسی بی سیم است. درک لایه یی که این پروتکل به امن سازی آن می پردازد اهمیت ویژه یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه های دیگر، غیر از لایه ی ارتباطی بی سیم که مبتنی بر استاندارد ۸۰۲.۱۱ است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه ی بی سیم به معنی استفاده از قابلیت درونی استاندارد شبکه های محلی بی سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.

شکل بالا محدوده ی عمل کرد استانداردهای امنیتی ۸۰۲.۱۱ (خصوصاً WEP) را نشان می دهد.

قابلیت ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه های بی سیم بر اساس استاندارد ۸۰۲.۱۱ فراهم می کند WEP است. این پروتکل با وجود قابلیت هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه های بی سیم را به نحوی، ولو سخت و پیچیده، فراهم می کند. نکته یی که باید به خاطر داشت این ست که اغلب حملات موفق صورت گرفته در مورد شبکه های محلی بی سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می گذارد، هرچند که فی نفسه دچار نواقص و ایرادهایی نیز هست.
بسیاری از حملاتی که بر روی شبکه های بی سیم انجام می گیرد از سویی است که نقاط دسترسی با شبکه ی سیمی دارای اشتراک هستند. به عبارت دیگر

نفوذگران بعضاً با استفاده از راه های ارتباطی دیگری که بر روی مخدوم ها و سخت افزارهای بی سیم، خصوصاً مخدوم های بی سیم، وجود دارد، به شبکه ی بی سیم نفوذ می کنند که این مقوله نشان دهنده ی اشتراکی هرچند جزءیی میان امنیت در شبکه های سیمی و بی سیم یی ست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه های محلی بی سیم تعریف می گردد:

Authentication

هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی سیم است. این عمل که در واقع کنترل دست رسی به شبکه ی بی سیم است. این مکانیزم سعی دارد که امکان اتصال مخدوم هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

Confidentiality

محرمانه گی هدف دیگر WEP است. این بُعد از سرویس ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه ی محلی بی سیم است.

Integrity

هدف سوم از سرویس ها و قابلیت های WEP طراحی سیاستی است که تضمین کند پیام ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم های بی سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه های ارتباطاتی دیگر نیز کم وبیش وجود دارد .

نکته ی مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس های معمول Auditingو Authorization در میان سرویس های ارایه شده توسط این پروتکل است.

استاندارد ۸۰۲.۱۱ سرویس های مجزا و مشخصی را برای تأمین یک محیط امن بی سیم در اختیار قرار می دهد. این سرویس ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy)تأمین می گردند و وظیفه ی آن ها امن سازی ارتباط میان مخدوم ها و نقاط دسترسی بی سیم است. درک لایه یی که این پروتکل به امن سازی آن می پردازد اهمیت ویژه یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه های دیگر، غیر از لایه ی ارتباطی بی سیم که مبتنی بر استاندارد ۸۰۲.۱۱ است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه ی بی سیم به معنی استفاده از قابلیت درونی استاندارد شبکه های محلی بی سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.

شکل بالا محدوده ی عمل کرد استانداردهای امنیتی ۸۰۲.۱۱ (خصوصاً WEP) را نشان می دهد.

قابلیت ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه های بی

سیم بر اساس استاندارد ۸۰۲.۱۱ فراهم می کند WEP است. این پروتکل با وجود قابلیت هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه های بی سیم را به نحوی، ولو سخت و پیچیده، فراهم می کند. نکته یی که باید به خاطر داشت این ست که اغلب حملات موفق صورت گرفته در مورد شبکه های محلی بی سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می گذارد، هرچند که فی نفسه دچار نواقص و ایرادهایی نیز هست.
بسیاری از حملاتی که بر روی شبکه های بی سیم انجام می گیرد از سویی است که نقاط دسترسی با شبکه ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه های ارتباطی دیگری که بر روی مخدوم ها و سخت افزارهای بی سیم، خصوصاً مخدوم های بی سیم، وجود دارد، به شبکه ی بی سیم نفوذ می کنند که این مقوله نشان دهنده ی اشتراکی هرچند جزءیی میان امنیت در شبکه های سیمی و بی سیم یی ست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه های محلی بی سیم تعریف می گردد:

Authentication
هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی سیم است. این عمل که در واقع کنترل دست رسی به شبکه ی بی سیم است. این مکانیزم سعی دارد که امکان اتصال مخدوم هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

Confidentiality
محرمانه گی هدف دیگر WEP است. این بُعد از سرویس ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه ی محلی بی سیم است.

Integrity
هدف سوم از سرویس ها و قابلیت های WEP طراحی سیاستی است که تضمین کند پیام ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم های بی سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه های ارتباطاتی دیگر نیز کم وبیش وجود دارد .

نکته ی مهمی که در مورد سه سرویس WEP وجود دارد نبود سرویس های معمول Auditingو Authorization در میان سرویس های ارایه شده توسط این پروتکل است.

استاندارد ۸۰۲.۱۱ دو روش برای احراز هویت کاربرانی که درخواست اتصال به شبکه ی بی سیم را به نقاط دسترسی ارسال می کنند، دارد که یک روش بر مبنای رمزنگاری ست و دیگری از رمزنگاری استفاده نمی کند.

شکل زیر شَمایی از فرایند Authentication را در این شبکه ها نشان می دهد:

همان گونه که در شکل نیز نشان داده شده است، یک روش از رمزنگاری RC4 استفاده می کند و روش دیگر از هیچ تکنیک رمزنگاری یی استفاده نمی کند.

در روشی که مبتنی بر رمزنگاری نیست، دو روش برای تشخیص هویت مخدوم وجود دارد. در هر دو روش مخدومِ متقاضی پیوستن به شبکه، درخواست ارسال هویت از سوی نقطه ی دسترسی را با پیامی حاوی یک SSID (Service Set Identifier) پاسخ می دهد.

در روش اول که به Open System Authentication موسوم است، یک SSID خالی نیز برای دریافت اجازه ی اتصال به شبکه کفایت می کند. در واقع در این روش تمامی مخدوم هایی که تقاضای پیوستن به شبکه را به نقاط دسترسی ارسال می کنند با پاسخ مثبت روبه رو می شوند و تنها آدرس آن ها توسط نقطه ی دسترسی نگاه داری می شود. به همین دلیل به این روش NULL Authentication نیز اطلاق می شود.

در روش دوم از این نوع، بازهم یک SSID به نقطه ی دسترسی ارسال می گردد با این تفاوت که اجازه ی اتصال به شبکه تنها در صورتی از سوی نقطه ی دسترسی صادر می گردد کهSSID ی ارسال شده جزوSSID های مجاز برای دسترسی به شبکه باشند. این روش به Closed System Authentication موسوم است.

نکته یی که در این میان اهمیت بسیاری دارد، توجه به سطح امنیتی ست که این روش در اختیار ما می گذارد. این دو روش عملاً روش امنی از احراز هویت را ارایه نمی دهند و عملاً تنها راهی برای آگاهی نسبی و نه قطعی از هویت درخواست کننده هستند. با این وصف از آن جایی که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران کم تجربه و مبتدی، به شبکه هایی که بر اساس این روش ها عمل می کنند، رخ می دهد، لذا این دو روش تنها در حالتی کاربرد دارند که یا شبکه یی در حال ایجاد است که حاوی اطلاعات حیاتی نیست، یا احتمال رخداد حمله به آن بسیار کم است. هرچند که با توجه پوشش نسبتاً گسترده ی یک شبکه ی بی سیم – که مانند شبکه های سیمی امکان محدودسازی دسترسی به صورت فیزیکی بسیار دشوار است – اطمینان از شانس پایین رخ دادن حملات نیز خود تضمینی ندارد!

این روش که به روش «کلید مشترک» نیز موسوم است، تکنیکی کلاسیک است که بر اساس آن، پس از اطمینان از اینکه مخدوم از کلیدی سری آگاه است، هویتش تأیید می شود. شکل زیر این روش را نشان می دهد:

در این روش، نقطه ی دسترسی (AP) یک رشته ی تصادفی تولید کرده و آن را به مخدوم می فرستد. مخدوم این رشته ی تصادفی را با کلیدی از پیش تعیین شده (که کلید WEP نیز نامیده می شود) رمز می کند و حاصل را برای نقطه ی دسترسی ارسال می کند. نقطه ی دسترسی به روش معکوس پیام دریافتی را رمزگشایی کرده و با رشته ی ارسال شده مقایسه می کند. در صورت هم سانی این دو پیام، نقطه ی

دسترسی از اینکه مخدوم کلید صحیحی را در اختیار دارد اطمینان حاصل می کند . روش رمزنگاری و رمزگشایی در این تبادل روش RC4 است .

در این میان با فرض اینکه رمزنگاری RC4 را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش است:
الف) در این روش تنها نقطه ی دسترسی ست که از هویت مخدوم اطمینان حاصل می کند. به بیان دیگر مخدوم هیچ دلیلی در اختیار ندارد که بداند نقطه ی دسترسی یی که با آن در حال تبادل داده های رمزی ست نقطه ی دسترسی اصلی ست.

ب) تمامی روش هایی که مانند این روش بر پایه ی سئوال و جواب بین دو طرف، با هدف احراز هویت یا تبادل اطلاعات حیاتی، قرار دارند با حملاتی تحت عنوان man-in-the-middle در خطر هستند. در این دسته از حملات نفوذگر میان دو طرف قرار می گیرد و به گونه یی هریک از دو طرف را گمراه می کند.

این سرویس که در حوزه های دیگر امنیتی اغلب به عنوان Confidentiality از آن یاد می گردد به معنای حفظ امنیت و محرمانه نگاه داشتن اطلاعات کاربر یا گره های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه گی عموماً از تکنیک های رمزنگاری استفاده می گردد، به گونه یی که در صورت شنود اطلاعات در حال تبادل، این اطلاعات بدون داشتن کلیدهای رمز، قابل رمزگشایی نبوده و لذا برای شنودگر غیرقابل سوء استفاده است.

در استاندارد b۸۰۲.۱۱، از تکنیک های رمزنگاری WEP استفاده می گردد که برپایه ی RC4است .یک الگوریتم رمزنگاری متقارن است که در آن یک رشته ی نیمه تصادفی تولید می گردد و توسط آن کل داده رمز می شود. این رمزنگاری بر روی تمام بسته ی اطلاعاتی پیاده می شود. به بیان دیگر داده های تمامی لایه های بالای اتصال بی سیم نیز توسط این روش رمز می گردند، از IP گرفته تا لایه های بالاتری مانند .HTTP از آنجایی که این روش عملاً اصلی ترین بخش از اعمال سیاست های امنیتی در شبکه های محلی بی سیم مبتنی بر استاندارد 802.11b است، معمولاً به کل پروسه ی امن سازی اطلاعات در این استاندارد به اختصار WEP گفته می شود.

کلیدهای WEP اندازه هایی از ۴۰ بیت تا ۱۰۴ بیت می توانند داشته باشند. این کلیدها با) IV مخفف Initialization Vector یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی RC4 را تشکیل می دهند. طبیعتاً هرچه اندازه ی کلید بزرگ تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان می دهد که استفاده از کلیدهایی با اندازه ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک brute-force را برای شکستن رمز غیرممکن می کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه ی ۸۰ بیت (که تعدد آن ها از مرتبه ی ۲۴ است) به اندازه یی بالاست که قدرت پردازش سیستم های رایانه یی کنونی برای شکستن کلیدی مفروض در زمانی معقول کفایت نمی کند .

هرچند که در حال حاضر اکثر شبکه های محلی بی سیم از کلیدهای ۴۰ بیتی برای رمزکردن بسته های اطلاعاتی استفاده می کنند ولی نکته یی که اخیراً، بر اساس یک سری آزمایشات به دست آمده است، این ست که روش تأمین محرمانه گی توسط WEP در مقابل حملات دیگری، غیر از استفاده از روشbrute-force ، نیز آسیب

پذیر است و این آسیب پذیری ارتباطی به اندازه ی کلید استفاده شده ندارد.

نمایی از روش استفاده شده توسط WEP برای تضمین محرمانه گی در شکل زیر نمایش داده شده است:

مقصود از Integrity صحت اطلاعات در حین تبادل است و سیاست های امنیتی یی که Integrity را تضمین می کنند روش هایی هستند که امکان تغییر اطلاعات در حین تبادل را به کم ترین میزان تقلیل می دهند.

در استاندارد ۸۰۲.۱۱ bنیز سرویس و روشی استفاده می شود که توسط آن امکان تغییر اطلاعات در حال تبادل میان مخدوم های بی سیم و نقاط دست رسی کم می شود. روش مورد نظر استفاده از یک کد CRC است. همان طور که در شکل قبل نیز نشان داده شده است، یک CRC-32 قبل از رمزشدن بسته تولید می شود. در سمت گیرنده، پس از رمزگشایی، CRCداده های رمزگشایی شده مجدداً محاسبه شده و با CRCنوشته شده در بسته مقایسه می گردد که هرگونه اختلاف میان دو CRC به معنای تغییر محتویات بسته در حین تبادل است. متأسفانه این روش نیز مانند روش رمزنگاری توسطRC4 ، مستقل از اندازه ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب پذیر است.

متأسفانه استاندارد ۸۰۲.۱۱ bهیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی که برای حفظ امنیت کلیدها انجام می گیرد باید توسط کسانی که شبکه ی بی سیم را نصب می کنند به صورت دستی پیاده سازی گردد. از آنجایی که این بخش از امنیت یکی از معضل های اساسی در مبحث رمزنگاری است، با این ضعف عملاً روش های متعددی برای حمله به شبکه های بی سیم قابل تصور است. این روش ها معمولاً بر سهل انگاری های انجام شده از سوی کاربران و مدیران شبکه مانند تغییرندادن کلید به صورت مداوم، لودادن کلید، استفاده از کلیدهای تکراری یا کلیدهای پیش فرض کارخانه و دیگر بی توجهی ها نتیجه یی جز درصد نسبتاً بالایی از حملات موفق به شبکه های بی سیم ندارد. این مشکل از شبکه های بزرگ تر بیش تر خود را نشان می دهد. حتا با فرض تلاش برای جلوگیری از رخ داد چنین سهل انگاری هایی، زمانی که تعداد مخدوم های شبکه از حدی می گذرد عملاً کنترل کردن این تعداد بالا بسیار دشوار شده و گه گاه خطاهایی در گوشه و کنار این شبکه ی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می شود.

ضعف های اولیه ی امنیتیWEP

همان گونه که گفته شد، عملاً پایه ی امنیت در استاندارد ۸۰۲.۱۱ بر اساس پروتکل WEPاستوار است WEP .در حالت استاندارد بر اساس کلیدهای ۴۰ بیتی برای رمزنگاری توسط الگوریتم RC4 استفاده می شود، هرچند که برخی از تولیدکننده گان نگارش های خاصی از WEP را با کلیدهایی با تعداد بیت های بیش تر پیاده سازی کرده اند .

نکته یی که در این میان اهمیت دارد قائل شدن تمایز میان نسبت بالارفتن امنیت و اندازه ی کلیدهاست. با وجود آن که با بالارفتن اندازه ی کلید (تا ۱۰۴ بیت) امنیت بالاتر می رود، ولی از آن جاکه این کلیدها توسط کاربران و بر اساس یک کلمه ی عبور تعیین می شود، تضمینی نیست که این اندازه تماماً استفاده شود. از سوی دیگر

همان طور که در قسمت های پیشین نیز ذکر شد، دست یابی به این کلیدها فرایند چندان سختی نیست، که در آن صورت دیگر اندازه ی کلید اهمیتی ندارد.

متخصصان امنیت بررسی های بسیاری را برای تعیین حفره های امنیتی این استاندارد انجام داده اند که در این راستا خطراتی که ناشی از حملاتی متنوع، شامل حملات غیرفعال و فعال است، تحلیل شده است .

حاصل بررسی های انجام شده فهرستی از ضعف های اولیه ی این پروتکل است :

یکی از ابتدایی ترین ضعف ها که عموماً در بسیاری از شبکه های محلی بی سیم وجود دارد استفاده از کلیدهای مشابه توسط کاربران برای مدت زمان نسبتاً زیاد است. این ضعف به دلیل نبود یک مکانیزم مدیریت کلید رخ می دهد. برای مثال اگر یک کامپیوتر کیفی یا جیبی که از یک کلید خاص استفاده می کند به سرقت برود یا برای مدت زمانی در دست رس نفوذگر باشد، کلید آن به راحتی لو رفته و با توجه به تشابه کلید میان بسیاری از ایستگاه های کاری عملاً استفاده از تمامی این ایستگاه ها ناامن است.
از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانال های ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

این بردار که یک فیلد ۲۴ بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده فرستاده می شود. از آن جایی که کلیدی که برای رمزنگاری مورد استفاده قرار می گیرد بر اساس IV تولید می شود، محدوده ی IV عملاً نشان دهنده ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه است .به عبارت دیگر در صورتی که IV کوتاه باشد در مدت زمان کمی می توان به کلیدهای مشابه دست یافت .
این ضعف در شبکه های شلوغ به مشکلی حاد مبدل می شود. خصوصاً اگر از کارت شبکه ی استفاده شده مطمئن نباشیم. بسیاری از کارت های شبکه ازIV های ثابت استفاده می کنند و بسیاری از کارت های شبکه ی یک تولید کننده ی واحدIV های مشابه دارند. این خطر به همراه ترافیک بالا در یک شبکه ی شلوغ احتمال تکرار IV در مدت زمانی کوتاه را بالاتر می برد و در نتیجه کافی ست نفوذگر در مدت زمانی معین به ثبت داده های رمز شده ی شبکه بپردازد وIV های بسته های اطلاعاتی را ذخیره کند. با ایجاد بانکی ازIV های استفاده شده در یک شبکه ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت زمانی نه چندان طولانی وجود خواهد داشت.

از آن جایی که IV در تمامی بسته های تکرار می شود و بر اساس آن کلید تولید می شود، نفوذگر می تواند با تحلیل و آنالیز تعداد نسبتاً زیادی ازIV ها و بسته های رمزشده بر اساس کلید تولید شده بر مبنای آنIV ، به کلید اصلی دست پیدا کند. این فرایند عملی زمان بر است ولی از آن جاکه احتمال موفقیت در آن وجود دارد لذا به عنوان ضعفی برای این پروتکل محسوب می گردد.

در پروتکلWEP ، کد CRC رمز نمی شود. لذا بسته های تأییدی که از سوی نقاط دست رسی بی سیم به سوی گیرنده ارسال می شود بر اساس یک CRC رمزنشده ارسال می گردد و تنها در صورتی که نقطه ی دست رسی از صحت بسته اطمینان حاصل کند تأیید آن را می فرستد. این ضعف این امکان را فراهم می کند که نفوذگر برای رمزگشایی یک بسته، محتوای آن را تغییر دهد و CRC را نیز به دلیل این که رمز نشده است، به راحتی عوض کند و منتظر عکس العمل نقطه ی دست رسی بماند که آیا بسته ی تأیید را صادر می کند یا خیر.

ضعف های بیان شده از مهم ترین ضعف های شبکه های بی سیم مبتنی بر پروتکل WEPهستند. نکته یی که در مورد ضعف های فوق باید به آن اشاره کرد این است که در میان این ضعف ها تنها یکی از آن ها (مشکل امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز می گردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می گردد و بقیه ی مشکلات امنیتی کماکان به قوت خود باقی هستند.

جدول زیر ضعف های امنیتی پروتکل WEP را به اختصار جمع بندی کرده است:

خطرها، حملات و ملزومات امنیتی

همان گونه که گفته شد، با توجه به پیشرفت های اخیر، در آینده یی نه چندان دور باید منتظر گسترده گی هرچه بیش تر استفاده از شبکه های بی سیم باشیم .این گسترده گی، با توجه به مشکلاتی که از نظر امنیتی در این قبیل شبکه ها وجود دارد نگرانی هایی را نیز به همراه دارد. این نگرانی ها که نشان دهنده ی ریسک بالای استفاده از این بستر برای سازمان ها و شرکت های بزرگ است، توسعه ی این استاندارد را در ابهام فرو برده است. در این قسمت به دسته بندی و تعریف حملات، خطرها و ریسک های موجود در استفاده از شبکه های محلی بی سیم بر اساس استاندارد IEEE 802.11x می پردازیم.

شکل زیر نمایی از دسته بندی حملات مورد نظر را نشان می دهد:

مطابق درخت فوق، حملات امنیتی به دو دسته ی فعال و غیرفعال تقسیم می گردند.

حملات غیرفعال

در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوال اطلاعات منبع نمی کند. این نوع حمله می تواند تنها به یکی از اشکال شنود ساده یا آنالیز ترافیک باشد.

-شنود
در این نوع، نفوذگر تنها به پایش اطلاعات ردوبدل شده می پردازد. برای مثال شنود ترافیک روی یک شبکه ی محلی یا یک شبکه ی بی سیم (که مد نظر ما است (نمونه هایی از این نوع حمله به شمار می آیند.

-آنالیز ترافیک

در این نوع حمله، نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده ها می پردازد. به عبارت دیگر بسته یا بسته های اطلاعاتی به همراه یکدیگر اطلاعات معناداری را ایجاد می کنند.

حملات فعال

در این نوع حملات، برخلاف حملات غیرفعال، نفوذگر اطلاعات مورد نظر را، که از منابع به دست می آید، تغییر می دهد، که تبعاً انجام این تغییرات مجاز نیست. از آن جایی که در این نوع حملات اطلاعات تغییر می کنند، شناسایی رخ داد حملات فرایندی امکان پذیر است. در این حملات به چهار دسته ی مرسوم زیر تقسیم بندی می گردند :

-تغییر هویت

در این نوع حمله، نفوذگر هویت اصلی را جعل می کند. این روش شامل تغییر هویت اصلی یکی از طرف های ارتباط یا قلب هویت و یا تغییر جریان واقعی فرایند پردازش اطلاعات نیز می گردد .

-پاسخ های جعلی

نفوذگر در این قسم از حملات، بسته هایی که طرف گیرنده ی اطلاعات در یک ارتباط دریافت می کند را پایش می کند. البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می گردد ولی اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می گردند. این نوع حمله بیش تر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می کند. در این حالت بسته های پاسخی که برای فرستنده به عنوان جواب به سؤالات فرستنده ارسال می گردند به معنای پرچمی برای شناسایی گیرنده محسوب می گردند. لذا در صورتی که نفوذگر این بسته ها را ذخیره کند و در زمانی که یا گیرنده فعال نیست، یا فعالیت یا ارتباط آن به صورت آگاهانه –به روشی- توسط نفوذگر قطع شده است، می تواند مورد سوء استفاده قرار گیرد. نفوذگر با ارسال مجدد این بسته ها خود را به جای گیرنده جازده و از سطح دسترسی مورد نظر برخوردار می گردد.

-تغییر پیام

در برخی از موارد مرسوم ترین و متنوع ترین نوع حملات فعال تغییر پیام است .از آن جایی که گونه های متنوعی از ترافیک بر روی شبکه رفت وآمد می کنند و هریک از این ترافیک ها و پروتکل ها از شیوه یی برای مدیریت جنبه های امنیتی خود استفاده می کنند، لذا نفوذگر با اطلاع از پروتکل های مختلف می تواند برای هر یک از این انواع ترافیک نوع خاصی از تغییر پیام ها و در نتیجه حملات را اتخاذ کند. با توجه به گسترده گی این نوع حمله، که کاملاً به نوع پروتکل بسته گی دارد، در این جا نمی توانیم به انواع مختلف آن بپردازیم، تنها به یادآوری این نکته بسنده می کنیم که این حملات تنها دست یابی به اطلاعات را هدف نگرفته است و می تواند با اعمال تغییرات خاصی، به گمراهی دو طرف منجر شده و مشکلاتی را برای سطح مورد نظر دست رسی – که می تواند یک کاربر عادی باشد – فراهم کند.

-حمله های(DoS (Denial-of-Service

این نوع حمله، در حالات معمول، مرسوم ترین حملات را شامل می شود. در این نوع حمله نفوذگر یا حمله کننده برای تغییر نحوه ی کارکرد یا مدیریت یک سامانه ی ارتباطی یا اطلاعاتی اقدام می کند. ساده ترین نمونه سعی در از کارانداختن خادم های نرم افزاری و سخت افزاری ست. پیرو چنین حملاتی، نفوذگر پس از از کارانداختن یک سامانه، که معمولاً سامانه پی ست که مشکلاتی برای نفوذگر برای دست رسی به اطلاعات فراهم کرده است، اقدام به سرقت، تغییر یا نفوذ به منبع اطلاعاتی می کند. در برخی از حالات، در پی حمله ی انجام شده، سرویس مورد نظر به طور کامل قطع نمی گردد و تنها کارایی آن مختل می گردد .در این حالت نفوذگر می تواند با سوءاستفاده از اختلال ایجاد شده به نفوذ از طریق/به همان سرویس نیز اقدام کند .
Authentication Authenticationبدون رمزنگاری Authentication با رمزنگاری RC4
. ۳. Initialization Vector (IV) ۲ WEPاستفاده از کلیدهای ثابت Privacy Integrity 1.
ضعف در الگوریتم.4 استفاده از CRC رمز نشده.

پایان