افزایش کیفیت و محدوده شبکه بی‌سیم

استفاده از شبکه بی‌سیم این روزها دیگر خیلی ساده شده است. تنها کافی است یک روتر بیسیم را خریداری کنید و سپس پورت اینترنت آن را به دستگاه مودم ADSL خود وصل کنید. حال می توانید از تمامی دستگاه ها و سیستم هایی که در اختیار دارید به روتر خود وصل شوید و از اینترنت در تمامی آن سیستم ها استفاده کنید.

اما با وجود رشد استفاده از شبکه های بی سیم در خانه ها و شرکت ها بعضی از کاربران از کیفیت و محدوده‌ای که می توانند با آن به شبکه های بی سیم اتصال پیدا کنند ناراضی هستند. در این آموزش از تورتک با هم یاد می گیریم که چگونه شبکه بی‌سیم خانگی خود را تقویت کرده و با این کار کیفیت دریافت سیگنال و محدوده قابل دسترس بودن سیگنال ها را افزایش دهیم.

چگونگی تقویت قدرت سیگنال های WiFi شبکه بی‌سیم

قبل از اینکه با انجام ترفندهایی قدرت و محدوده سیگنال های شبکه بی‌سیم خود را افزایش دهیم بهتر از با نکته‌ای آشنا شوید که در هنگام خرید روترهای خانگی به آن نیاز دارید. در هنگام خرید دستگاه روتر توجه داشته باشید که دستگاه مورد نظر از ارتباط بر مبنای استاندارد ۸۰۲.۱۱n پشتیبانی کند. در اینگونه ارتباط برخلاف نسخه قدیمی تر خود یعنی ۸۰۲.۱۱g که در بازار ایران نیز به راحتی پیدا می شود قدرت سیگنال و همچنین سرعت تبادل اطلاعات تغییر چشمگیری کرده است و شما با در اختیار داشتن یک روتر بر پایه ۸۰۲.۱۱n کمتر به مشکلاتی مانند قطعی در هنگام تبادل فایل های حجیم و ویدئو ها در بین دستگاه های متصل به شبکه بر می‌خورید.

اما در هر صورت ترفندهایی نیز برای افزایش کیفیت و محدوده سیگنال دهی شبکه های بی‌سیم خانگی وجود دارد که با آن ها در زیر آشنا می شویم.

1. **استفاده از DD-WRT :** در صورتی که نام مودم و یا دستگاه روتر شما در لیست دستگاه های سازگار با DD-WRT firmware وجود داشته باشد (مشاهده لیست) می توانید با دانلود این firmware (لینک دانلود DD-WRT) و نصب آن از طریق پنل مدیریتی روتر خود حداقل چند متری را به محدوده شبکه بیسیم خود اضافه کنید و با این کار همچنین کیفیت سیگنال های شما هیچ تغییر خاصی نیز نمی کنند. در صورتی که دستگاه شما با این firmware سازگاری نداشت پیشنهاد می کنم از Tomato firmware استفاده کنید.
2. **استفاده از ورق های آلمینیومی :** اکثر روترها بر روی خود یک آنتن دارند که اطلاعات و سیگنال ها را به تمامی جهت های ممکنه ارسال می کنند مانند یک لامپ معمولی که نور را پخش می کند. در صورتی که از دستگاه روتر خود در مرکز محدوده و یا خانه خود استفاده می کنید این ویژگی می تواند خیای مفید باشد اما اگر روتر شما در گوشه ای از خانه شما قرار دارد می توانید با استفاده از یک ورق آلمینیومی و حتی یک قوطی نوشابه آهنی باز شده بین دیوار و دستگاه روتر خود از هدر رفتن سگنال‌ها جلوگیری کنید و آن ها را دوباره به سمت محدوده کاری خود برگردانید. البته اگر می خواهید بهترین

نتیجه ممکنه را از این ترفند بگیرید بهتر است کمی بر روی حالت ورق آلمینیومی در پشت روتر خود کار کنید و با انتخاب شکل های مختلف به بهترین حالت ممکن دست یابید.

3. **استفاده از نرم افزار InSSIDer :** این نرم افزار کاملاً رایگان می تواند وجود و قدرت سیگنال های شبکه بی‌سیم خانگی شما را نمایش دهد. بهتر است این نرم افزار را بر روی لپ تاپ خود نصب بکنید و سپس در نقاط مختلف خانه از دسترسی و کیفیت سیگنال های شبکه با خبر شوید. با کنار هم گذاشتن اطلاعات به دست آمده خود می توانید بهترین مکان قرار گیری دستگاه روتر را تشخیص دهید. برای دانلود این نرم افزار از لینک InSSIDer استفاده کنید.
4. **انتخاب بهترین مکان برای روتر :** یکی دیگر از مواردی که می‌تواند در بهبود کیفیت و محدوده شبکه های بیسیم تاثیر بگذارد انتخاب یک مکان صحیح برای دستگاه روتر شبکه شما است. توجه داشته باشید که در کنار روتر بی سیم خود نباید دستگاه بی‌سیم دیگری وجود داشته باشد و سعی کنید از اجسام آهنی که ممکن است سیگنال ها را در جهت بی استفاده ای بازتاب کنند دستگاه روتر شما دور باشد. همچنین سعی کنید در وسط محل استفاده از شبکه بی سیم و همچنین در نقطه بالایی نسبت به دیگر دستگاه ها روتر شما قرار بگیرد.
5. **استفاده از آنتن‌های uni-directional :** معمولاً دستگاه های روتر با یک آنتن از نوع omni-directional که کیفیت معمولی نیز دارد فروخته می شوند ، پس اگر می خواهید محدوده و جهات پخش شدن سیگنال های شبکه بی‌سیم خود را افزایش دهید می توانید با خرید یک آنتن uni-directional قوی‌تر و نصب آن بر روی دستگاه روتر خود این کار را انجام دهید. اگر آنتن بهتری را در بازار برای خرید پیدا نکردید حداقل می توانید از آنتن های بهتر از مدل فعلی آنتن روتر خود که از تکنولوژی omni-directional در آن ها استفاده می شود را به راحتی پیدا کنید.

افزایش محدوده شبکه های بی‌سیم با

استفاده از سخت افزارهای جانبی

یکی دیگر از مواردی که کاربران شبکه های بی سیم خانگی به آن نیاز پیدا می کنند این است که محدوده قابل دسترس بودن شبکه خود را افزایش دهند که برای اینکار بهترین روش ممکن استفاده از سخت افزارهای جانبی است که کمپانی های معروف ارائه می دهند. در زیر با تاثیر گذار ترین روش های ممکن برای افزایش محدوده شبکه های بیسیم WiFi آشنا می شویم.

1. **استفاده از دستگاه WiFi Repeater :** این دستگاه همانطور که از اسم آن پیدا است قابلیت این را دارد که سیگنال های ارسالی دستگاه روتر بی سیم شما را دریافت کند و آن ها را با کیفیت و قدرت اولیه در محدوده ای که قرار دارد دوباره در تمامی جهات بحش کند. بهترین حالت استفاده از این دستگاه در زمانی است که آن را در نقاطی قرار دهیم که بعد از آن ها دیگر سیگنال های دستگاه روتر ما در دسترس نیست تا بتوانیم محدوده شبکه خود را بدون نیاز به هیچ سیمی افزایش دهیم.
2. **استفاده از یک روتر دیگر :** یکی دیگر روش هایی که برای افزایش محدوده های شبکه بی سیم به شما پیشنهاد می کنیم خرید و استفاده از یک روتر دیگر در کنار روتر فعلی شما است. تنها کافی است روتر اصلی خود را به اینترنت متصل کنید اگر می خواهید در شبکه اینترنت قابل دسترس باشد و سپس با یک کابل به شیوه LAN دستگاه روتر دوم را به روتر اصلی وصل کنید. جالب است بدانید در این روش می توانید تا ۱۰۰ پا دورتر دستگاه روتر دوم را قرار دهید چون برای دریافت اطلاعات از شبکه شما از یک سیم استفاده می شود.
3. **استفاده از یک Access Point :** با استفاده از یک دستگاه Access Point نیز می توانید به محدوده شبکه بی سیم خود وسعت بیشتری را بدهید مانند استفاده از WiFi Repeater که در بالا با آن آشنا شدیم. از مزایای این روش می توان به قابلیت اتصال سیستم های بیشتر به شبکه و از معایب آن می توان به قیمت بالای این دستگاه نسبت به یک روتر اشاره کرد.

تفاوت بین روش‌های رمزنگاری WEP، WPA و WPA2 در شبکه‌های بی سیم

امروزه با گسترش استفاده از اینترنت برای انجام فعالیت‌های خانگی و اداری و همچنین گسترش نفوذ تلفن‌های هوشمند در میان کاربران، مودم‌های بی سیم جز جدایی ناپذیر بسیاری از منازل و دفاتر در کشور شده‌اند. یکی از اولین مواردی که باید پس از نصب مودم‌های بی سیم به آنها توجه کرد، رمزگذاری روی آنها به منظور جلوگیری از سوء استفاده از سرویس اینترنت توسط کاربران ناخواسته است؛ اما حتی اگر شما به اهمیت استفاده از رمز روی مودم هم واقف باشید باز هم ممکن است بررسی تفاوت بین روش‌های مختلف رمزنگاری برایتان پیچیده بوده و خارج از حوصله شما باشد. در هر صورت به احتمال بسیار زیاد حتی اگر این تفاوت‌ها را هم ندانید با اسامی مخفی نظیر WEP، WPA و WPA2 آشنا هستید؛ اما هر کدام از این موارد به چه معنی هستند و کدام یک امنیت بیشتری را برای شبکه شما فراهم می‌کنند؟

تفاوت‌های واقعی یا ظاهری؟

اگر دستگاه مودم را از فروشنده ای با حوصله خریداری کرده باشید یا اینکه در مراحل نصب آن از افراد با تجربه کمک گرفته باشید حتما از آنها شنیده‌اید که اولین کار پس از روشن کردن مودم و در حال راه اندازی آن، در نظر گرفتن یک رمز عبور است. برای دانستن اهمیت رمزگذاری کافی است شرایطی را در نظر بگیرید که شخصی به صورت غیر قانونی به شبکه شما دسترسی پیدا کرده و به وسیله آن، فعالیت مجرمانه ای را انجام می‌دهد. اگر بتوان این جرم را رهگیری کرد، پلیس مستقیما به منزل یا محل کار شما راهنمایی خواهد شد؛ در حالی که روح شما از اتفاقاتی که افتاده بی اطلاع است. فرضا که تصمیم بگیرید روی شبکه رمز هم بگذارید؛ اما واقعا یک اسم مخفف در کنار این رمز عبور چه تفاوتی می‌تواند ایجاد کند؟ باید بدانید روش‌های مختلف رمزنگاری در واقع سطوح و کارکردهای بسیار متفاوتی با یکدیگر دارند. در درجه اول، با گسترش دسترسی افراد مختلف به شبکه اینترنت، استانداردهای قدیمی به تدریج کاربری خود را از دست داده و در معرض خطر بیشتری قرار می‌گیرند. دانستن تفاوت بین پروتکل‌های مختلف و به کار گیری کاربردی‌ترین و پیشرفته‌ترین آنها بدون شک فرآیندی کلیدی در حفظ اطلاعات شخصی و پشتیبانی از شبکه شما به حساب می‌آید. از اواخر دهه ۹۰ میلادی، الگوریتم‌های امنیتی WiFi شاهد پیشرفت‌های چشمگیر و به روز رسانی‌های گسترده ای بوده‌اند که تقریبا تمامی آنها در ارتباط با کنار گذاشتن الگوریتم‌های قدیمی و بازنگری در راهبردهای امنیتی برای دسترسی به الگوریتم‌های پیشرفته تر و جدیدتر بوده‌اند. به همین دلیل بهترین راه برای شناخت روش‌های رمزنگاری گوناگون، بررسی تاریخچه آنهاست.

Wired Equivalent Privacy – WEP

WEP یا «امنیت مشابه با شبکه‌های با سیم» پر استفاده ترین الگوریتم امنیتی در جهان به شمار می‌رود. دلیل چنین اتفاقی قابلیت Backward Compatibility (سازگاری با شرایط قدیمی تر) و البته این نکته است که WEP اولین گزینه در فهرست روبه روی کاربران برای برقراری یک رمز است. اولین بار در سپتامبر سال ۱۹۹۹ بود که WEP به عنوان یک استاندارد امنیتی WiFi شناخته شد. اولین نسخه‌های WEP حتی در دهه ۹۰ هم آنقدرها قدرتمند نبودند، زیرا محدودیت‌های ایالات متحده روی صادرات تکنولوژی‌های مختلف رمزنگاری باعث شده بود تولید کنندگان محصولات خود را تنها به رمزگذاری‌های ۶۴ بیتی محدود کنند.

پس از کنار گذاشتن این محدودیت‌ها، رمزگذاری به ۱۲۸ بیتی ارتقا پیدا کرد و در حال حاضر هم با وجود معرفی رمزگذاری WEP به صورت ۲۵۶ بیتی، باز هم مدل ۱۲۸ بیتی است که بیشترین استفاده را در بین کاربران دارد. رمزی که در حالت ۶۴ بیتی انتخاب می‌کنید، می‌تواند ۵ کاراکتر ASCII (کد استاندارد آمریکا برای تبادل اطلاعات یا آن طور که در زبان فارسی گفته می‌شود؛ اَسکی) یا ۱۰ کاراکتر هگزادسیمال (hex یا دستگاه اعداد پایه ۱۶) باشد، همچنین رمز ۱۲۸ بیتی نیز ۱۳ کاراکتر ASCII یا ۲۶ کاراکتر هگزادسیمال است. با اینکه WEP یک روش رمزگذاری به حساب می‌آید، اما شکستن آن به اندازه ای راحت است که در واقع یک شبکه با رمز WEP تفاوت خاصی با یک شبکه باز ندارد. باوجود باز نگری در این الگوریتم و معرفی حالت ۲۵۶ بیتی، نقص‌ها و ایرادات متعددی در استاندارد WEP کشف شد و بعد تر نیز با افزایش قدرت محاسباتی رایانه‌ها، عبور کردن از WEP آسان تر از قبل شد. در سال ۲۰۰۵ بود که FBI برای آگاه سازی کاربران از ضعف‌های WEP نمایشی عمومی برگزار کرد که در آن به کمک نرم افزارهای رایگان، تنها در عرض کمتر از یک دقیقه رمزهای WEP شکسته می‌شد. در حال حاضر نیز با وجود بهبودهای صورت گرفته، باز هم WEP به شدت آسیب پذیر بوده و به همین دلیل در سال ۲۰۰۴ این روش بازنشسته اعلام شد.

WiFi Protected Access – WPA

دسترسی حفاظت شده به WiFi یا همان WPA یک سال پیش از بازنشستگی WEP و برای جایگزینی آن ارائه شد. پر کاربردترین ساختار استفاده از WPA را می توان WPA-PSK نامید که توسط آن می توان بین ۸ تا ۶۳ کاراکتر ASCII را به عنوان رمز در نظر گرفت. کلیدهای استفاده شده توسط WPA به صورت ۲۵۶ بیتی بوده که پیشرفت چشمگیری نسبت به حالت‌های ۶۴ و ۱۲۸ بیتی WEP به حساب می‌آیند. برخی از مهم‌ترین تغییرات صورت گرفته توسط WPA عبارتند از بررسی یکپارچگی پیام برای مشخص کردن اینکه آیا مهاجمی توانسته بسته‌های اطلاعاتی رد و بدل شده بین access point و client را تصاحب کند یا خیر و پروتکل یکپارچگی کلیدهای موقت (TKIP). البته بعدتر TKIP با استاندارد رمزنگاری پیشرفته یا AES جایگزین شد. با وجود اینکه WPA برای راحت کردن خیال کاربران و خلاص شدن از WEP طراحی شده بود، اما به دلیل اینکه به وسیله به‌روزرسانی‌های firmware روی دستگاه‌های دارای WEP ارائه می‌شد، باید عناصر مشخصی از آن را تغییر می‌داد که همین موارد در نهایت باعث آسیب پذیری آن می‌شدند. پس از مدتی WPA هم به سرنوشت WEP دچار شد و نمایشی عمومی برای

اثبات آسیب پذیری آن اجرا شد.

WiFi Protected Access II – WPA2

در سال ۲۰۰۶ بود که WPA با WPA2 جایگزین شد. یکی از بزرگ ترین تغییرات صورت گرفته در این جایگزینی، استفاده اجباری از الگوریتم‌های AES و همچنین معرفی CCMP (حالت ضد رمز به همراه پروتکل کد اعتبارسنجی پیام تغییر بلوک) به عنوان جایگزینی برای TKIP بود. در حال حاضر استفاده از WPA2 برای کاربران خانگی تقریبا بدون نقطه ضعف بزرگ بوده و عمده نگرانی‌های پیرامون آن به امنیت بخش‌های تجاری مربوط می‌شود. متاسفانه بزرگ ترین نگرانی‌های موجود در WPA همچنان در WPA2 هم حاضرند و با وجود اینکه شکستن دیوار ایجاد شده توسط WPA2 به زمانی بین ۲ تا ۱۲ ساعت کار مداوم در یک رایانه حرفه ای نیاز دارد، اما باز هم ضرورت بازنگری و برطرف کردن حفره‌های امنیتی در آن احساس می‌شود.

کدام را انتخاب کنیم؟

حالا که با اسامی مختلف این روش‌های رمزگذاری آشنا شدیم باید به این پرسش پاسخ دهیم که در یک شبکه خانگی باید از کدام یک از آنها استفاده کرد؟ اگر بخواهیم خیلی ساده به این سوال پاسخ دهیم، می توان روش‌های رمزگذاری را بر حسب میزان نفوذناپذیری آنها به این صورت در نظر گرفت: قوی‌ترین و امن‌ترین حالت در شبکه‌های خانگی توسط WPA2+AES حاصل خواهد شد. پس از آن به ترتیب می توان WPA+AES، سپس WPA+TKIP/AES، بعد از آن WPA+TKIP، پس از آن WEP و در نهایت شبکه باز و بدون رمزگذاری را نام برد. البته برای استفاده از این روش‌ها باید یک نکته را در نظر داشت و آن، پشتیبانی تجهیزات شبکه شما از روش‌های مختلف رمزگذاری است. برای مثال اگر از یک مودم قدیمی استفاده می‌کنید ممکن است شرایط به کار گرفتن روش‌های WPA یا WPA2 در آن موجود نباشد و به همین دلیل مجبور شوید از تنظیمات نا امن WEP استفاده کنید. به همین دلیل اگر از این نوع مودم‌ها استفاده می‌کنید حتما به‌روزرسانی‌های امنیتی آن را در وب سایت تولید کننده دنبال کنید و همچنین پیش از خرید یک مودم جدید مطمئن شوید دستگاهی که انتخاب می‌کنید قابلیت به کار گیری روش‌های رمزگذاری جدید را دارد.

منبع:سخت افزار مگ