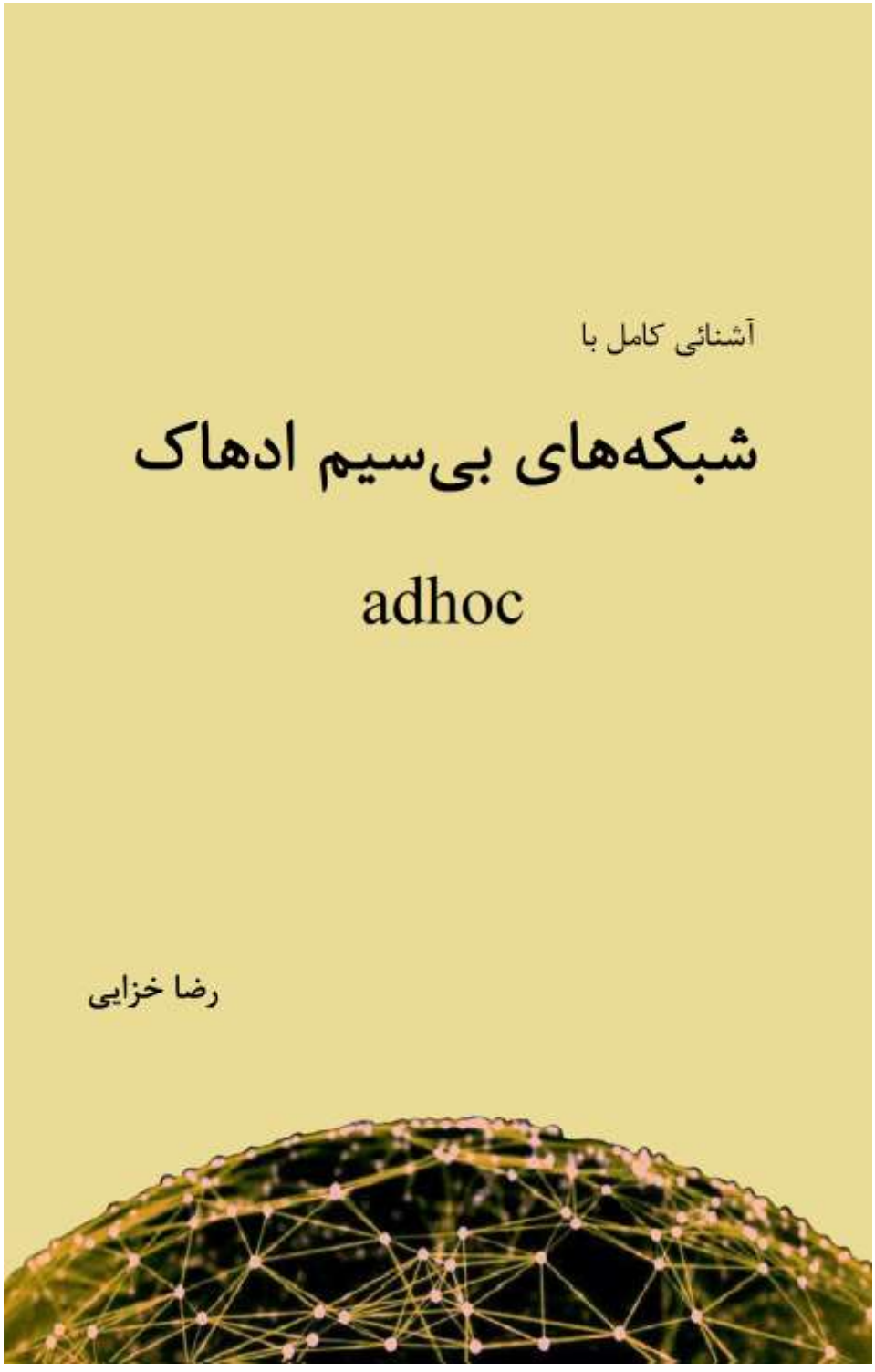


سرشناسه : خزایی، رضا، ۱۳۵۴
عنوان و نام پدیدآور: آشنایی کامل با شبکه‌های بیسیم ادهاک / رضا خزایی
مشخصات نشر : قائمشهر: مهرالنبی، ۱۳۹۸
مشخصات ظاهری : ۱۹۴ ص
شابک : ۹۷۸-۶۰۰-۷۹۸۵-۳۷-۳
وضعیت فهرست نویسی: فیپا
موضوع : شبکه‌های موردی
موضوع : Ad hoc networks (Computer networks)
رده بندی کنگره : TK ۱۰۵/۷۷
رده بندی دیویی : ۰۰۴/۶۸
شماره کتابشناسی ملی : ۶۰۵۵۳۸۵

شابک: ۹۷۸-۶۰۰-۷۹۸۵-۳۷-۳

آشنائی کامل با شبکه های بی سیم ادهاک

گردآوری : رضا خزایی

چاپ و صحافی: صدف

شمارگان: ۱۰۰۰ نسخه

بهاء: ۴۵۰۰۰۰ ریال

چاپ اول: زمستان ۱۳۹۸

ناشر: مهرالنبی

آدرس: ساری

تلفن: ۰۹۱۱۲۲۲۰۰۶۳ - ۰۹۳۶۵۴۰۹۳۲۳

تارنما: WWW.REZAKHAZAI.IR

رایانامه: rezakhazai135@yahoo.com - rezakhazai155@gmail.com

آشنائی کامل با

شبکه‌های بی‌سیم ادهاک adhoc

تهیه و تنظیم: رضا خزایی

WWW.REZAKHAZAI.IR

Rezakhazai۷۲@yahoo.com – rezakhazai۷۲@gmail.com

۰۹۱۱۲۲۲۰۰۳ - ۰۹۳۶۵۴۰۹۳۲۳

فهرست

روش شایعه پراکنی

روش اسپین

روش انتشار هدایت شده

شبکه بی سیم

توسعه رادیویی و موانع

ایمنی در داخل شبکه

توپولوژی دنیامیکی و عضویت

لینک بی سیم آسیب پذیر

پر سه زدن در محیط خطرناک

مسائل و چالشهای اصلی

ایمنی سطح لینک

مسیر یابی ایمن

خصوصی سازی

ایمن سازی شبکه

معرفی کامل شبکه

اهداف امنیتی

قابلیت دسترسی ، محرمانگی ، جامعیت تصدیق هویت

چالش ها و دغدغه ها

Scope and roadmap

مسیر یابی امن secure routing

کارهای مربوطه Related work

مسیر یابی امن Secure routing

سرویس های تکرار امن Replicadedsecare service

امنیت در شبکه های ad hoc

شبکه های کامپیوتری بی سیم

Personal Arean Network یا PAN

استاندارد مورد استفاده در این محدوده کاربرد

LAN کاربری معادل محدوده شبکه های

قوانین ومحدودیت ها

Wimax و Wifi

روش های ارتباطی بی سیم

Indoor شبکه های بی سیم

Outdoor شبکه های بی سیم

انواع ارتباط

انواع شبکه های بی سیم

سه روش امنیتی در شبکه های بی سیم

نقاط دسترسی نامطلوب

رسیدگی های منظم به سایت

استفاده غیرمجاز از سرویس

طراحی و نظارت برای تأیید هویت محکم

محدودیت های سرویس و کارایی

دیدبانی شبکه

حملات سطح بالاتر

تحلیل ترافیک و استراق سمع

انجام تحلیل خطر

امنیت تجهیزات شبکه

تأمین امنیت تجهزات بر روی شبکه DoS

امنیت فیزیکی

افزونگی در محل استقرار شبکه

توپولوژی شبکه

بررسی سه طراحی که معمول هستند

محل های امن برای تجهیزات

انتخاب لایه کانال ارتباطی امن

منابع تغذیه

آشنائی کامل با شبکه‌های بی‌سیم ادهاک adhoc

مقدمه و کلیات:

شبکه‌های بی‌سیم ادهاک، شامل مجموعه‌ای از گره‌های توزیع شده‌اند که با همدیگر به طور بی‌سیم ارتباط دارند. نودها می‌توانند کامپیوتر میزبان یا مسیریاب باشند. نودها به طور مستقیم بدون هیچگونه نقطه دسترسی با همدیگر ارتباط برقرار می‌کنند و سازمان ثابتی ندارند و بنابراین در یک توپولوژی دلخواه شکل گرفته‌اند. هر نودی مجهز به یک فرستنده و گیرنده می‌باشد. مهم‌ترین ویژگی این شبکه‌ها وجود یک توپولوژی پویا و متغیر می‌باشد که نتیجه تحرک نودها می‌باشد. نودها در این شبکه‌ها به طور پیوسته موقعیت خود را تغییر می‌دهند که این خود نیاز به یک پروتکل مسیریابی که توانایی سازگاری با این تغییرات را داشته، نمایان می‌کند. مسیریابی و امنیت در این شبکه از چالش‌های امروز این شبکه هاست. شبکه‌های بی سیم ادهاک خود بر دو نوع می‌باشند: شبکه‌های حسگر هوشمند و شبکه‌های موبایل

ادهاک. در مسیریابی در شبکه‌های ادهاک نوع حسگر سخت‌افزار محدودیت‌هایی را بر شبکه اعمال می‌کند که باید در انتخاب روش مسیریابی مد نظر قرار بگیرند ازجمله اینکه منبع تغذیه در گره‌ها محدود می‌باشد و در عمل، امکان تعویض یا شارژ مجدد آن مقدور نیست؛ لذا روش مسیریابی پیشنهادی در این شبکه‌ها بایستی از انرژی موجود به بهترین نحو ممکن استفاده کند یعنی باید مطلع از منابع گره باشد و اگر گره منابع کافی نداشت بسته را به آن برای ارسال به مقصد نفرستد. خودمختاربودن و قابلیت انطباق گره‌ها را ایجاد کند. بعضی از این روش‌ها در این مقاله بحث شده‌اند.

پیشینه:

شبکه‌های ادهاک عمر ۷۰ ساله دارند و به دلایل نظامی به وجود آمدند. اما بعدها در دیگر رشته ها نیز کابرد و کارآئی خود را نشان داده اند. یک مثال کلاسیک از شبکه‌های ادهاک، شبکه جنگنده‌های جنگ و پایگاههای موبایل آنها در میدان جنگ می‌باشد. بعداً مشخص شد در قسمت‌های تجاری و صنعتی نیز می‌توانند مفید واقع شوند. این شبکه‌ها شامل مجموعه‌ای از گره‌های توزیع شده‌اند که بدون پشتیبانی مدیریت مرکزی یک شبکهٔ موقت را می‌سازند.

طبیعی‌ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و امکان ایجاد تغییر در ساختار مجازی آنهاست. این ویژگی‌های خاصی که دارند پروتکل‌های مسریابی و روشهای امنیتی خاصی را می‌طلبد.

انواع شبکه‌های ادهاک

شبکه‌های حسگر هوشمند: متشکل از چندین حسگر هستند که در محدوده جغرافیایی معینی قرار گرفته‌اند. هر حسگر دارای قابلیت ارتباطی بی سیم و هوش کافی برای پردازش سیگنال‌ها و امکان شبکه سازی است. شبکه‌های موبایل ادهاک :مجموعه مستقلی شامل کاربران متحرک است که از طریق لینک‌های بی سیم با یکدیگر ارتباط برقرار می‌کنند. برای اتفاقات غیرقابل پیش بینی اتصالات و شبکه‌های متمرکز کارا نبوده و قابلیت اطمینان کافی را ندارند؛ لذا شبکه‌های ادهاک موبایل راه حل مناسبی است، گره‌های واقع در شبکه‌های ادهاک موبایل مجهز به گیرنده و فرستنده‌های بی سیم بوده و از آنتن‌هایی استفاده می‌کنند که ممکن است از نوع Broad cast و یا peer to peer باشند.

کاربردها:

به طور کلی زمانی که زیرساختاری قابل دسترس نیست و ایجاد و احداث زیرساختار غیرعملی بوده و همچنین مقرون به صرفه نباشد، استفاده از شبکه ادهاک مفید است. از جمله این کاربردها می‌توان به موارد زیر اشاره نمود:

شبکه‌های شخصی (تلفن‌های سلولی، کامپیوترهای کیفی، ساعت‌های مچی، ear phone و کامپیوترهای wearable)

محیط‌های نظامی

سربازها و تانکها و هواپیماها

در نبردهایی که کنترل از راه دور صورت می‌گیرد

برای ارتباطات نظامی

توانایی باقی‌ماندن در میدان منازعه

محیط‌های غیرنظامی

شبکه تاکسی رانی

اتاق‌های ملاقات

میادین یا ورزشگاه‌های ورزشی

قایق‌ها، هواپیماهای کوچک

کنفرانس‌ها جلسات

عملکردهای فوری

عملیات جستجو و نجات

موقعیت‌های امدادی برای حادثه‌های بد و فوری

برای ترمیم و بدست آوردن اطلاعات در حوادث بد و غیرمترقبه مانند وقوع بلایای طبیعی چون سیل و طوفان و زلزله

محیط‌های علمی

در محیط‌های علمی و تحقیقاتی در برخی از مناطق که دانشمندان برای نخستین بار اقدام به بررسی می‌کنند، به علت عدم وجود زیرساختار، شبکه ادهاک بسیار مفید می‌باشد.

Sensor webs

یک دسته مخصوص از شبکه‌های ادهاک را می‌توان Sensor webs دانست. شبکه‌ای از گره‌های حسگر که یک گره، سیستمی است که دارای باتری می‌باشد. توانایی مخابره بی سیم محاسبات و حس کردن محیط در آن وجود دارد. نقش آن مانیتور کردن و تعامل با محیط و دنیای اطراف است. کاربردهای آن شامل آزمایشات اقیانوسی و فضایی می‌باشد.

خصوصیات شبکه‌های ادهاک

شبکه‌های بی سیم دارای نیازمندی‌ها و مشکلات امنیتی ویژه‌ای هستند. این مشکلات ناشی از ماهیت و خواص شبکه‌های بی سیم است که در بررسی هر راه حل امنیتی باید به آنها توجه نمود:

فقدان زیرساخت: در شبکه‌های بی سیم ساختارهای متمرکز و مجتمع مثل سرویس دهنده‌ها، مسیریابها و... لزوماً موجود نیستند (مثلاً در شبکه‌های ادهاک)، به همین خاطر راه حل‌های امنیتی آنها هم معمولاً غیر متمرکز، توزیع شده و مبتنی بر همکاری همه نودهای شبکه‌است.

استفاده از لینک بی سیم: در شبکه بی سیم، خطوط دفاعی معمول در شبکه‌های سیمی (مثلاً فایروال به عنوان خط مقدم دفاع) وجود

ندارد. نفوذگر از تمام جهت‌ها و بدون نیاز به دسترسی فیزیکی به لینک، می‌تواند هر نودی را هدف قرار دهد.

چند پرشی بودن: در اغلب پروتکل‌های مسیریابی بی سیم، خود نودها نقش مسیریاب را ایفا می‌کنند (به خصوص در شبکه‌های ادهاک)، و بسته‌ها دارای چند hop مختلف هستند. طبیعتاً به هر نودی نمی‌توان اعتماد داشت آن هم برای وظیفه‌ای همچون مسیریابی!

خودمختاری نودها در تغییر مکان: نودهای سیار در شبکه بی سیم به دلیل تغییر محل به خصوص در شبکه‌های بزرگ به سختی قابل ردیابی هستند.

از دیگر ویژگیهای طبیعی شبکه بی سیم که منبع مشکلات امنیتی آن است می‌توان به فقدان توپولوژی ثابت و محدودیت‌های منابعی مثل توان، پردازنده و حافظه اشاره کرد.

امنیت در شبکه‌های بی سیم

این شبکه‌ها به شدت در مقابل حملات آسیب پذیرند و امروزه مقاومت کردن در برابر حملات از چالش‌های توسعه این شبکه هاست. دلایل اصلی این مشکلات عبارتند از:

کانال رادیویی اشتراکی انتقال داده

محیط عملیاتی ناامن

قدرت مرکزی ناکافی

منابع محدود

آسیب پذیر بودن از لحاظ فیزیکی

کافی نبودن ارتباط نودهای میانی.

منشأ ضعف امنیتی در شبکه‌های بی‌سیم و خطرات معمول

ساختار این شبکه‌ها مبتنی بر استفاده از سیگنال‌های رادیویی به جای سیم و کابل، استوار است. با استفاده از این سیگنال‌ها و در واقع بدون مرز ساختن پوشش ساختار شبکه، نفوذگران قادرند در صورت شکستن موانع امنیتی نه‌چندان قدرتمند این شبکه‌ها، خود را به عنوان عضوی از این شبکه‌ها جازده و در صورت تحقّق این امر، امکان دست‌یابی به اطلاعات حیاتی، حمله به سرویس‌دهندگان سازمان و

مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره‌های شبکه با یکدیگر، تولید داده‌های غیرواقعی و گمراه‌کننده، سوءاستفاده از پهنای باند مؤثر شبکه و دیگر فعالیت‌های مخرب وجود دارد. در مجموع، در تمامی دسته‌های شبکه‌های بی‌سیم، از دید امنیتی حقایقی مشترک صادق است:

نفوذگران، با گذر از تدابیر امنیتی موجود، می‌توانند به راحتی به منابع اطلاعاتی موجود بر روی سیستم‌های رایانه‌ای دست یابند.

حمله‌های DOS به تجهیزات و سیستم‌های بی سیم بسیار متداول است.

کامپیوترهای قابل حمل و جیبی، که امکان استفاده از شبکهٔ بی سیم را دارند، به راحتی قابل سرقت هستند. با سرقت چنین سخت‌افزارهایی، می‌توان اولین قدم برای نفوذ به شبکه را برداشت.

یک نفوذگر می‌تواند از نقاط مشترک میان یک شبکهٔ بی‌سیم در یک سازمان و شبکهٔ سیمی آن (که در اغلب موارد شبکهٔ اصلی و حساس‌تری محسوب می‌گردد) استفاده کرده و با نفوذ به شبکهٔ بی‌سیم عملاً راهی برای دست یابی به منابع شبکه سیمی نیز بیابد.

سه روش امنیتی در شبکه‌های بی سیم

WEP

در این روش از شنود کاربرهایی که در شبکه مجوز ندارند جلوگیری به عمل می‌آید که مناسب برای شبکه‌های کوچک بوده زیرا نیاز به تنظیمات دستی مربوطه در هر سرویس گیرنده می‌باشد. اساس رمز نگاری WEP بر مبنای الگوریتم RC۴ بوسیله RSA می‌باشد.

SSID

شبکه‌های WLAN دارای چندین شبکه محلی می‌باشند که هر کدام آنها دارای یک شناسه یکتا می‌باشند این شناسه‌ها در چندین نقطه دسترسی قرار داده می‌شوند. هر کاربر برای دسترسی به شبکه مورد نظر بایستی تنظیمات شناسه SSID مربوطه را انجام دهد.

MAC

لیستی از MAC آدرس‌های مورد استفاده در یک شبکه به نقطه دسترسی مربوطه وارد شده بنابراین تنها کامپیوترهای دارای این MAC آدرس‌ها اجازه دسترسی دارند به عبارتی وقتی یک کامپیوتر درخواستی را ارسال می‌کند MAC آدرس آن با لیست MAC آدرس مربوطه در نقطه دسترسی مقایسه شده و اجازه دسترسی یا عدم دسترسی آن مورد بررسی قرار می‌گیرد.

این روش امنیتی مناسب برای شبکه‌های کوچک بوده زیرا در شبکه‌های بزرگ امکان ورود این آدرس‌ها به نقطه دسترسی بسیار مشکل می‌باشد. در کل می‌توان به کاستن از شعاع تحت پوشش سیگنال‌های شبکه کم کرد و اطلاعات را رمزنگاری کرد.

مسیریابی

در شبکه‌های ادهاک، نودهای شبکه دانش قبلی از توپولوژی شبکه‌ای که درآن قرار دارند، ندارند به همین دلیل مجبورند برای ارتباط با

سایر نودها، محل مقصد را در شبکه کشف کنند. در اینجا ایده اصلی این است که یک نود جدید به طور اختیاری حضورش را در سراسر شبکه منتشر می‌کند وبه همسایه‌هایش گوش می‌دهد. به این ترتیب نود تا حدی ازنودهای نزدیکش اطلاع بدست می‌آورد و راه رسیدن به آنها را یاد می‌گیرد به همین ترتیب که پیش رویم همه نودهای دیگر را می‌شناسد و حداقل یک راه برای رسیدن به آنها را می‌داند.

پروتکل‌های مسیریابی

پروتکل‌های مسیریابی بین هر دو نود این شبکه به دلیل اینکه هر نودی می‌تواند به طور تصادفی حرکت کند و حتی می‌تواند در زمانی از شبکه خارج شده باشد، مشکل می‌باشند. به این معنی یک مسیری که در یک زمان بهینه‌است ممکن است چند ثانیه بعد اصلاً این مسیر وجود نداشته باشد. در زیر سه دسته از پروتکل‌های مسیر یابی که در این شبکه‌ها وجود دارد را معرفی می‌کنیم.

Table Driven Protocols

در این روش مسیریابی هرنودی اطلاعات مسیریابی را با ذخیره اطلاعات محلی سایر نودها در شبکه استفاده می‌کند و این اطلاعات سپس برای انتقال داده از طریق نودهای مختلف استفاده می‌شوند.

On Demand Protocols

روش ایجاب می‌کند مسیرهایی بین نودها تنها زمانی که برای مسیریابی بسته موردنیاز است تا جایی که ممکن است بروزرسانی روی مسیرهای درون شبکه ندارد به جای آن روی مسیرهایی که ایجاد شده و استفاده می‌شوند وقتی مسیری توسط یک نود منبع به مقصدی نیاز می‌شود که آن هیچ اطلاعات مسیریابی ندارد، آن فرایند کشف مسیر را از یک نود شروع می‌کند تا به مقصد برسد. همچنین ممکن است یک نود میانی مسیری تا مقصد داشته باشد. این پروتکل‌ها زمانی موثرند که فرایند کشف مسیر کمتر از انتقال داده تکرار شود زیرا ترافیک ایجاد شده توسط مرحله کشف مسیر در مقایسه با پهنای باند ارتباطی کمتر است.

Hybrid Protocols

ترکیبی از دو پروتکل بالاست. این پروتکل‌ها روش مسیریابی بردار-فاصله را برای پیدا کردن کوتاه‌ترین به کار می‌گیرند و اطلاعات مسیریابی را تنها وقتی تغییری در توپولوژی شبکه وجود دارد را گزارش می‌دهند. هر نودی در شبکه برای خودش یک zone مسیریابی دارد و رکورد اطلاعات مسیریابی در این zoneها نگهداری می‌شود. مثل ZRP (zone routing protocol)

پروتکل‌های روش اول

DSDV: این پروتکل بر مبنای الگوریتم کلاسیک Bellman-Ford بنا شده‌است. در این حالت هر گره لیستی از تمام مقصدها و نیز تعداد پرش‌ها تا هر مقصد را تهیه می‌کند. هر مدخل لیست با یک عدد شماره گذاری شده‌است. برای کم کردن حجم ترافیک ناشی از بروز رسانی مسیرها در شبکه از incremental -packets استفاده می‌شود. تنها مزیت این پروتکل اجتناب از به وجود آمدن حلقه‌های

مسیریابی در شبکه‌های شامل مسیریاب‌های متحرک است. بدین ترتیب اطلاعات مسیرها همواره بدون توجه به این که آیا گره در حال حاضر نیاز به استفاده از مسیر دارد یا نه فراهم هستند.

معایب:

پروتکل DSDV نیازمند پارامترهایی از قبیل بازه زمانی بروزرسانی اطلاعات و تعداد بروزرسانی‌های مورد نیاز می‌باشد.

WRP:

این پروتکل بر مبنای الگوریتم path-finding بنا شده با این استثنا که مشکل شمارش تا بینهایت این الگوریتم را برطرف کرده‌است. در این پروتکل هر گره، چهار جدول تهیه می‌کند: جدول فاصله، جدول مسیر یابی، جدول هزینه لینک و جدولی در مورد پیام‌هایی که باید دوباره ارسال شوند. تغییرات ایجاد شده در لینک‌ها از طریق ارسال و دریافت پیام میان گره‌های همسایه اطلاع داده می‌شوند.

CSGR:

در این نوع پروتکل گره‌ها به دسته‌ها تقسیم بندی می‌شوند. هر گروه یک سر گروه دارد که می‌تواند گروهی از میزبان‌ها را کنترل و مدیریت کند. از جمله قابلیت‌هایی که عمل دسته بندی فراهم می‌کند می‌توان به اختصاص پهنای باند و دسترسی به کانال اشاره کرد. این پروتکل از DSDV به عنوان پروتکل مسیریابی زیر بنایی خود استفاده می‌کند. نیز در این نوع هر گره دو جدول یکی جدول مسیریابی و دیگری جدول مربوط به عضویت در گره‌های مختلف را فراهم می‌کند.

معایب: گره‌ای که سر واقع شده سربار محاسباتی زیادی نسبت به بقیه دارد و به دلیل اینکه بیشتر اطلاعات از طریق این سرگروه‌ها برآورده می‌شوند در صورتی که یکی از گره‌های سرگروه دچار مشکل شود کل و یا بخشی از شبکه آسیب می‌بینند.

STAR:

این پروتکل نیاز به بروز رسانی متداوم مسیرها نداشته و هیچ تلاشی برای یافتن مسیر بهینه بین گره‌ها نمی‌کند.

پروتکل‌های روش دوم

SSR: این پروتکل مسیرها را بر مبنای قدرت و توان سیگنال‌ها بین گره‌ها انتخاب می‌کند؛ بنابراین مسیرهایی که انتخاب می‌شوند نسبتاً قوی تر هستند. می‌توان این پروتکل را به دو بخش DRP و SRP تقسیم کرد.

DRP مسئول تهیه و نگهداری جدول مسیریابی و جدول مربوط به توان سیگنال‌ها می‌باشد.SRP نیز بسته‌های رسیده را بررسی می‌کند تا در صورتی که آدرس گره مربوط به خود را داشته باشد آن را به لایه‌های بالاتر بفرستد.

DSR:

در این نوع، گره‌های موبایل بایستی حافظه‌هایی موقت برای مسیرهایی که از وجود آنها مطلع هستند فراهم کنند. دو فاز اصلی برای این پروتکل در نظر گرفته شده‌است:کشف مسیر و بروز رسانی مسیر. فاز کشف مسیر از route request/reply packetها و فاز بروز رسانی مسیر از تصدیق‌ها و اشتباهای لینکی استفاده می‌کند.

:TORA

بر اساس الگوریتم مسیریابی توزیع شده بنا شده و برای شبکه‌های موبایل بسیار پویا طراحی شده‌است. این الگوریتم برای هر جفت از گره‌ها چندین مسیر تعیین می‌کند و نیازمند کلاک سنکرون می‌باشد. سه عمل اصلی این پروتکل عبارتند از: ایجاد مسیر. بروز رسانی مسیر و از بین بردن مسیر.

:AODV

بر مبنای الگوریتم DSDV بنا شده با این تفاوت که به دلیل مسیریابی تنها در زمان نیاز میزان انتشار را کاهش می‌دهد. الگوریتم کشف مسیر تنها زمانی آغاز به کار می‌کند که مسیری بین دو گره وجود نداشته باشد.

:RDMAR

این نوع از پروتکل فاصله بین دو گره را از طریق حلقه‌های رادیویی و الگوریتم‌های فاصله یابی محاسبه می‌کند. این پروتکل محدوده جستجوی مسیر را مقدار مشخص و محدودی تایین می‌کند تا بدین وسیله از ترافیک ناشی از سیل آسا در شبکه کاسته باشد.

مسیریابی چند مسیری

برخی از الگوریتم‌های مسیریابی در شبکه‌های موردی، عمل مسیریابی را به طور چندمسیری انجام می‌دهند، به این معنا که به طور همزمان چندین مسیر را بین مبدا و مقصد برقرار می‌کنند. در حالت کلی می‌توان مزایای زیر را برای الگوریتم‌های چندمسیری در برابر الگوریتم‌های تک‌مسیری، برشمرد:

۱. افزایش تحمل پذیری در برابر خطا و خرابی. ۲. متعادل کردن بار در شبکه و کنترل ازدحام و ترافیک. ۳. افزایش پهنای باند انتها به انتها. ۴. کاهش تاخیر انتها به انتها. الگوریتم‌های مسیریابی چند مسیری در واقع چندین مسیر را بین مبدا و مقصد کشف می‌کنند، که استفاده از این مسیرها معمولاً به دو صورت انجام می‌شود.

در رویکرد اول همواره یکی از این مسیرهای به عنوان مسیرِ اصلی جهت ارسال اطلاعات انتخاب می‌شود و ارسال اطلاعات به سمت مقصد، فقط از طریق مسیرِ اصلی صورت می‌گیرد و مابقی مسیرها به عنوان مسیر جایگزین نگهداری می‌شوند تا در صورت ناکارآمد شدن یا از بین روفتن مسیر اصلی، از یکی از آنها جهت ارسال اطلاعات

استفاده شود. به این ترتیب در صورت خرابی، تاخیر بسیار کمتری به شبکه تحمیل می‌شود. اما در رویکرد دیگر، مبدا همزمان از چندین مسیر برای ارسال اطلاعات به سمت مقصد استفاده می‌کند که در این صورت می‌توان به مزایایی از قبیل متعادل کردن بار در شبکه و کنترل ترافیک و ازدحام دست یافت. در نهایت در این رویکرد نیز به خاطر ارسال موازی داده‌ها، تاخیر انتها به انتها به شدت کاهش می‌یابد.

در بین الگوریتم‌های مسیریابی چند مسیری می‌توان به SMR، AOMDV، AODVM، ZD-AOMDV و IZM-DSR اشاره کرد.

محدودیت‌های سخت‌افزاری یک گره حسگر

عواملی چون اقتصادی بودن سیستم، قابلیت مورد انتظار، تعداد انبوه گره‌ها و نهایتاً عملی شدن ایده‌ها در محیط واقعی، موجب گشته هر گره یکسری محدودیت‌های سخت‌افزاری داشته باشد. این محدودیت‌ها در ذیل اشاره شده و در مورد هرکدام توضیحی ارائه گردیده‌است :

- هزینه پائین: بایستی سیستم نهایی از نظر اقتصادی مقرون به صرفه باشد. چون تعداد گره‌ها خیلی زیاد بوده و برآورد هزینه هر گره در تعداد زیادی (بالغ بر چند هزار) ضرب می‌گردد، بنابراین هر چه از هزینه هر گره کاسته شود، در سطح کلی شبکه، صرفه جویی زیادی صورت خواهد گرفت و سعی می‌شود هزینه هر گره به کمتر از یک دلار برسد.

- حجم کوچک: گره‌ها به نسبت محدوده‌ای که زیر نظر دارند، بخشی را به حجم خود اختصاص می‌دهند؛ لذا هر چه این نسبت کمتر باشد به همان نسبت کارایی بالاتر می‌رود و از طرفی در اکثر موارد برای اینکه گره‌ها جلب توجه نکند و یا بتوانند در برخی مکان‌ها قرار بگیرند نیازمند داشتن حجم بسیار کوچک می‌باشند.

- توان مصرفی پائین: منبع تغذیه در گره‌ها محدود می‌باشد و در عمل، امکان تعویض یا شارژ مجدد آن مقدور نیست؛ لذا بایستی از انرژی وجود به بهترین نحو ممکن استفاده گردد.

نرخ بیت پائین: به خاطر وجود سایر محدودیت‌ها، عملاً میزان نرخ انتقال و پردازش اطلاعات در گره‌ها، نسبتاً پایین می‌باشد.

- خودمختار بودن: هر گره‌ای بایستی از سایر گره‌ها مستقل باشد و بتواند وظایف خود را طبق تشخیص و شرایط خود، به انجام برساند.

- قابلیت انطباق: در طول انجام نظارت بر محیط، ممکن است شرایط در هر زمانی دچار تغییر و تحول شود. مثلاً برخی از گره‌ها خراب گردند؛ لذا هر گره بایستی بتواند وضعیت خود را با شرایط بوجود آمده جدید تطبیق دهد.

روش‌های مسیریابی در شبکه‌های حسگر

در مسیریابی در شبکه‌های ادهاک نوع حسگر سخت‌افزار محدودیت‌هایی را بر شبکه اعمال می‌کند که باید در انتخاب روش مسیریابی مد نظر قرار بگیرند ازجمله اینکه منبع تغذیه در گره‌ها محدود می‌باشد و در عمل، امکان تعویض یا شارژ مجدد آن مقدور نیست؛ لذا روش مسیریابی پیشنهادی در این شبکه‌ها بایستی از انرژی موجود به بهترین نحو ممکن استفاده کند یعنی باید مطلع از

منابع گره باشد و اگر گره منابع کافی نداشت بسته را به آن برای ارسال به مقصد نفرستد.

روش سیل آسا

در این روش یک گره جهت پراکندن قسمتی از داده‌ها در طول شبکه، یک نسخه از داده مورد نظر را به هر یک از همسایگان خود ارسال می‌کند. هر وقت یک گره، داده جدیدی دریافت کرد، از آن نسخه برداری می‌کند و داده را به همسایه‌هایش (به جز گرهی که داده را از آن دریافت کرده‌است) ارسال می‌کند.

الگوریتم زمانی همگرا می‌شود یا پایان می‌یابد که تمامی گره‌ها یک نسخه از داده را دریافت کنند. زمانی که طول می‌کشد تا دسته‌ای از گره‌ها مقداری از داده‌ها را دریافت و سپس ارسال کنند، یک دور نامیده می‌شود. الگوریتم سیل آسا در زمان $O(d)$ دور، همگرا می‌شود که d قطر شبکه‌است چون برای یک قطعه داده d دور طول می‌کشد تا از یک انتهای شبکه به انتهای دیگر حرکت کند. سه مورد

از نقاط ضعف روش ارسال ساده جهت استفاده از آن در شبکه‌های حسگر در زیر آورده شده‌است :

انفجار: در روش سنتی سیل آسا، یک گره همیشه داده‌ها را به همسایگانش، بدون در نظر گرفتن اینکه آیا آن همسایه، داده را قبلاً دریافت کرده یا خیر، ارسال می‌کند. این عمل باعث بوجود آمدن مشکل انفجار می‌شود.

هم پوشانی: حسگرها معمولاً نواحی جغرافیایی مشترکی را پوشش می‌دهند و گره‌ها معمولاً قطعه داده‌هایی از حسگرها را دریافت می‌کنند که با هم هم پوشانی دارند.

عدم اطلاع از منابع: در روش سیل آسا، گره‌ها بر اساس میزان انرژی موجودی خود در یک زمان، فعالیت‌های خود را تغییر نمی‌دهند در صورتی که یک شبکه از حسگرهای خاص منظوره، می‌تواند از منابع موجود خود آگاهی داشته باشد و ارتباطات و محاسبات خود را با شرایط منابع انرژی خود مطابقت دهد.

روش شایعه پراکنی

این روش یک جایگزین برای روش سیل آسا سنتی محسوب می‌شود که از فرایند تصادف برای صرفه جویی در مصرف انرژی بهره می‌برد. به جای ارسال داده‌ها به صورت یکسان، یک گره شایعه پراکن، اطلاعات را به صورت تصادفی تنها به یکی از همسایگانش ارسال می‌کند. اگر یک گره شایعه پراکن، داده‌ای را از همسایه اش دریافت کند، می‌تواند در صورتی که همان همسایه به صورت تصادفی انتخاب شد، داده را مجدداً به آن ارسال کند.

روش اسپین

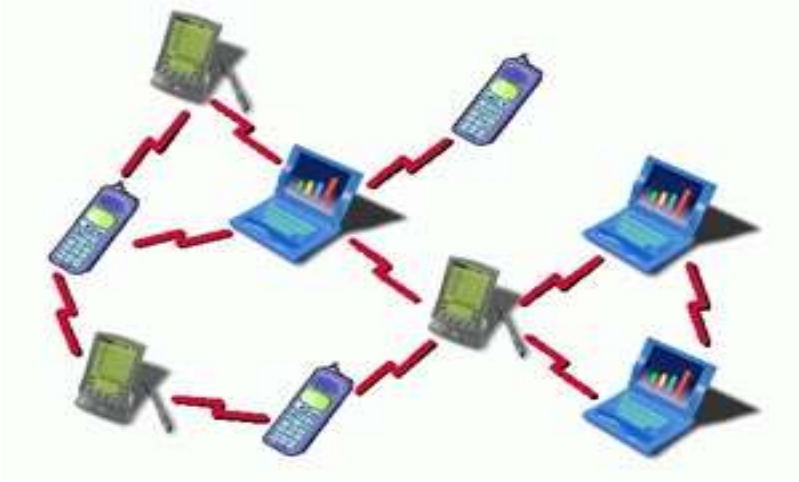
روش SPIN خانواده‌ای از پروتکل‌های وقفی است که می‌توانند داده‌ها را به صورت موثری بین حسگرها در یک شبکه حسگر با منابع انرژی محدود، پراکنده کنند. همچنین گره‌های SPIN می‌توانند تصمیم گیری جهت انجام ارتباطات خود را هم بر اساس اطلاعات مربوط به برنامه کاربردی و هم بر اساس اطلاعات مربوط به منابع موجود خود به انجام برسانند. این کار باعث می‌شود که حسگرها بتوانند داده‌ها را با وجود منابع محدود خود، به صورت کارآمدی

پراکنده کنند. گره‌ها در SPIN برای ارتباط با یکدیگر از سه نوع پیغام استفاده می‌کنند:

– ADV: برای تبلیغ داده‌های جدید استفاده می‌شود. وقتی یک گره SPIN، داده‌هایی برای به اشتراک گذاشتن در اختیار دارد، این امر را می‌تواند با ارسال شبه -داده مربوطه تبلیغ کند.

– REQ: جهت درخواست اطلاعات استفاده می‌شود. یک گره SPIN می‌تواند هنگامی که می‌خواهد داده حقیقی را دریافت کند از این پیغام استفاده کند.

– DATA: شامل پیغام‌های داده‌ای است. پیغام‌های DATA محتوی داده حقیقی جمع‌آوری شده توسط حسگرها هستند.



روش انتشار هدایت شده

در این روش منابع و دریافت کننده‌ها از خصوصیات، برای مشخص کردن اطلاعات تولید شده یا موردنظر استفاده می‌کنند و هدف روش انتشار هدایت شده پیدا کردن یک مسیر کارآمد چندطرفه بین فرستنده و گیرنده هاست. در این روش هر وظیفه به صورت یک علاقه‌مندی منعکس می‌شود که هر علاقه‌مندی مجموعه‌ای است از زوج‌های خصوصیت-مقدار. برای انجام این وظیفه، علاقه‌مندی در ناحیه موردنظر منتشر می‌شود. در این روش هر گره، گره‌ای را که

اطلاعات از آن دریافت کرده به خاطر می‌سپارد و برای آن یک گرادیان تشکیل می‌دهد که هم مشخص کننده جهت جریان اطلاعات است و هم وضعیت درخواست را نشان می‌دهد (که فعال یا غیرفعال است یا نیاز به بروز شدن دارد).

در صورتی که گره از روی گرادیان‌های قبلی یا اطلاعات جغرافیایی بتواند مسیر بعدی را پیش بینی کند تنها درخواست را به همسایه‌های مرتبط با درخواست ارسال می‌کند و در غیر این صورت، درخواست را به همه همسایه‌های مجاور ارسال می‌کند. وقتی یک علاقه‌مندی به گره‌ای رسید که داده‌های مرتبط با آن را در اختیار دارد، گره منبع، حسگرهای خود را فعال می‌کند تا اطلاعات موردنیز را جمع‌آوری کنند و اطلاعات را به صورت بسته‌های اطلاعاتی ارسال می‌کند. داده‌ها همچنین می‌توانند به صورت مدل خصوصیت-نام ارسال شوند. گرهی که داده‌ها را ارسال می‌کند به عنوان یک منبع شناخته می‌شود. داده هنگام ارسال به مقصد در گره‌های میانی ذخیره می‌شود که این عمل در اصل برای جلوگیری از ارسال داده‌های تکراری و جلوگیری از به وجودآمدن حلقه استفاده می‌شود.

همچنین از این اطلاعات می‌توان برای پردازش اطلاعات درون شبکه و خلاصه سازی اطلاعات استفاده کرد. پیغام‌های اولیه ارسالی به

عنوان داده‌های اکتشافی برچسب زده می‌شوند و به همه همسایه‌هایی که به گره دارای داده، گرادیان دارند ارسال می‌شوند یا می‌توانند از میان این همسایه‌ها، یکی یا تعدادی را برحسب اولویت جهت ارسال بسته‌های اطلاعات انتخاب کنند. (مثلاً همسایه‌هایی که زودتر از بقیه پیغام را به این گره ارسال کرده‌اند) برای انجام این کار، یرنده یا سینک همسایه‌ای را جهت دریافت اطلاعات ترجیح می‌دهد تقویت می‌کند.

اگر یکی از گره‌ها در این مسیر ترجیحی از کار بیفتد، گره‌های شبکه به طور موضعی مسیر از کار افتاده را بازیابی می‌کنند. در نهایت گیرنده ممکن است همسایه جاری خود را تقویت منفی کند در صورتی که مثلاً همسایه دیگری اطلاعات بیشتری جمع‌آوری کند. پس از ارسال داده‌های اکتشافی اولیه، داده‌های بعدی تنها از طریق مسیرهای تقویت شده ارسال می‌شوند. منبع اطلاعات به صورت متناوب هر چند وقت یکبار داده‌های اکتشافی ارسال می‌کند تا گرادیان‌ها در صورت تغییرات پویای شبکه، بروز شوند.

مشکلات چندی در زمینه ارتباطات ، پویایی ، قابل حمل و جابجایی بدون ابزار mobile computingو ادوات شبکه ، تطابق رفتار استفاده کننده با محیط جدید ایجاد می کند . زمانی که یک واحد

موبایل Ad-Hoc بدون زیر ساختی واحد و ثابت با دیگر دستگاهها و کاربر در تعامل است شکلی از شبکه ایجاد شده که معماری شبکه ای عمومی وپیچیده را مدیریت می کند مسیریابی منابع به صورت پیدا mobile یکی از راههایی است که برای مسیریابی در این نوع معماری به کار می رود تحقیقات در زمینه ایجاد می کند به خاطر اینکه Expiration مهم است به خاطر اینکه مرزهای جدیدی در زمینه com باید ابتدا mobile computing اوج یک کار کامل در شبکه ای است . در واقع برای حل مشکلات مشکلات شبکه های معمولی را مرتفع کرد .

شبکه بی سیم

مجموعه ای ازنودهای Adhoc یا به طور ساده تر یک شبکه Adhoc شبکه بی سیم پراکنده از نظر جغرافیایی است که با یکدیگر از طریق یک بستر بی سیم ارتباط دارند یک سلولی) تفاوت دارد و تفاوتش این است که هیچ) cellular با شبکه Adhoc شبکه چارچوب سیم کش ای وجود ندارد و ارتباطات شبکه از طریق نیروی باطری ها محدود می شبکه جنگنده ها در جنگ در میدان رزم Adhoc شوند . یک نمونه کلاسیک از شبکه های packet است .

به علاوه توانایی بررسی های جدید در این حوزه شامل توسعه شبکه های و شبکه های رادیویی ماندگار است .

از آنجا که حوزه های کاربردی (PRNS) radio در بر می گیرد ولی Adhoc نظامی هنوز اصلی ترین حوزه مطالعاتی را در شبکه های توسعه سریع تلفن های موبایل و افزایش کامپیوترهای دستی ، موضوع جدیدی در مطالعات به وجود آورده است برای مثال بلایای زندگی ، کنفرانس ها ، Adhoc تجاری شبکه های شبکه های خانگی ، شبکه های حسی ، شبکه های محلی شخصی و ... مشخص می کند که هر محاسبه در Adhoc فقدان یک چارچوب ثابت در شبکه های شبکه ، نیاز به انجام در یک حالت غیر متمرکز دارد .

به علاوه بسیاری از مشکلات اساسی وجود ندارد به عنوان مشکلات محاسبات توزیع شده معرفی Adhoc که در شبکه های شده است .

ویژگی های به خصوصی دارند که مطالعه آنها را متمایز از سایر Adhoc البته شبکه های مشکلات و ، Adhoc شبکه ها می سازد در این مقاله ما به بعضی ویژگی های شبکه های یک نمونه بررسی شده می پردازیم.

ما به ۲ حوزه مشکل توجه داریم :

کنترل شکل محاسبه و پشتیبانی از نودهای به هم متصل در شبکه و مسیریابی. Topology یک شبکه < Modeling Adhoc ned ۲ works> Adhoc مدل سازی شبکه های را می توان یک مجموعه ای از نقاط در فضای ۲ بعدی (یا سه بعدی) اقلیدسی Adhoc در نظر گرفت که هر نقطه یک نود شبکه را نمایش می دهد . هر نود می تواند به وسیله قدرت محاسباتی و ارتباطی اش شناسایی شود . قدرت محاسباتی یک نود عبارت است از سطح کد گذاری و رمزنگاری ای که نود می تواند انجام دهد ، ۲ کار کلیدی در شبکه های بی سیم و خصوصیات ارتباطی شبکه ها به وسیله ویژگی های کانال رادیویی و محیط و قدرت باطری و کنترل نیروی نودهای اختصاصی مدیریت می شود .

۳ ۲ توسعه رادیویی و موانع

pathloss مدلسازی کانال رادیویی بی سیم کار پیچیده ای است محیط انتقال بی سیم به نسبت pathloss . مسیر ، صدا ، کانه و قفل شدن به دلیل مشکلات فیزیکی حساس است به قدرت دریافت به قدرت ارسال است . آن بر کیفیت سیگنال های دریافتی تاثیر می گذارد قدرت ارسال باشد سپس PT قدرت دریافت سیگنال و PR و تابع فاصله ارسال است اگر در فضای آزاد (پاک و در خط مستقیم) خواهیم داشت :

۱ ۴ Adhoc ایمنی در داخل شبکه چیست ؟

۱ - Adhoc شبکه

مفهوم جدید Bluetooth , Leee۸۰۲,۱۱ , Hiperlan با پیشرفت در فناوریهای رادیود نظیر است که در آن جا Adhoc شبکه ای به وجود آمده است . این امر معروف به شبکه سازی ویژه یا کاربران بسیار از پیرامون مشترک لینک رادیویی می رسند و در تنظیم توپولوژی شبکه برای ارتباطات سیار هستند و در گستره

رادیویی از طریق لینک , Adhoc شرکت می کنند. گروههای داخل شبکه های مستقیم بی سیم یا مسیر یابی چند جهتی با یکدیگر ارتباط برقرار می کنند .

۲ - Adhoc کمبود ایمنی در شبکه های :

طوری مجسم می شود که در آن جا پشتیبانی دستیابی بی سیم یا پشتیبان Adhoc ساختار شبکه سیم دار , میسر نیست – شبکه تک کاره , هیچ پایه و اساس از پیش تعریف شده ندارد و تمام خدمات شبکه ای در موقع اجرا پیکر بندی می شوند و به وجود می آیند . از این رو بدیهی است که نقطه , Adhoc با فقدان پشتیبانی زیر بنایی و حملات لینک بی سیم آسیب پذیر , ایمنی در شبکه بنا به دلایل ذیل مشکل آفرین Adhoc ضعف ذاتی است . دستیابی به ایمنی در داخل شبکه سازی است :

- توپولوژی دنیامیکی و عضویت :

خیلی دنیامیک است به طوریکه متحرک بودن گروهها یا عضویت Adhoc - توپ ولوژی شبکه ای گره ها خیلی تصادفی و سریع است این امر به دینامیکی بودن نیاز برای راه حل های ایمن تاکید می کند.

- لینک بی سیم آسیب پذیر :

حملات لینک فعال / غیر فعال نظیر استراق سمع , کلک زدن , انکار خدمات رسانی , تقلید و جعل هویت امکان پذیر هستند .

- پر سه زدن در محیط خطرناک :

هر گونه بدرفتاری بدخواهی می تواند سبب ایجاد حملات خصمانه شود یا تمام گروهها را از فراهم نمودن خدمات محروم کند .

Adhoc گره های موجود در محیط متحرک با دستیابی به لینک رادیویی مشترک در تنظیم به آسانی مشارکت می کنند . اما ارتباطات ایمن در میان گره ها مستلزم ایجاد infrastructu ارتباط در لینک ارتباطات ایمن است . قبل از تعیین لینک ارتباطات ایمن , گره باید بتواند گره دیگر را شناسایی کند . در نتیجه گره , گره هویت خود و نیز مدارک مربوطه به گره دیگر را فراهم می سازد .

اما مدارک و احراز هویت ارائه شده باید مورد تایید و حفاظت قرار گیرند به طوری که اصالت یکپارچگی مدارک و هویت ارائه شده را نمی توان طبق گره گیرنده مورد سوال قرار داد هر گره می خواهد مطمئن شود که مدارک و هویت ارائه شده به گروههای دریافت کننده تطبیق داده نمی شود . از این رو لازم است ساختار ایمن برای شبکه ای سازی تک کاره و ایمن فراهم شود .

مساله هویت فوق الذکر فورا به مساله خصوصی سازی منجر می شود به طور کلی گره سیار از انواع هویت ها استفاده می کند و آن از سطح لینک تا سطح کاربر / کاربر تغییر می کند همچنین در محیط سیار بصورت مکرر گره سیار آماده نیست تا مدارک یا هویتش را به گره سیار دیگر از نقطه نظر خصوصی سازی آشکار سازد هر گونه هویت سازگار شده باعث می شود که حمله کننده ها تهدید و

خصوصی سازی برای دستگاه کاربر ایجاد کند متاسفانه استانداردهای سیار جاری هیچ گونه خصوصی سازی ممکن فراهم نمی کند و در بسیاری از موارد آشکار ساختن هویت برای تولید لینک ارتباطات اجتناب ناپذیر است از این رو حفاظت خصوصی سازی بی درز برای مهار کردن کاربرد شبکه ای سازی تک کاره مورد نیاز است .

۳ - مسائل و چالشهای اصلی :

۳-۱ ایمنی سطح لینک :

در محیط بی سیم لینک ها نسبت به حملاتی که استراق سمع کننده به آسانی می تواند ارتباطات پیوسته را دست اندازد آسیب پذیر هستند چون هیچ حفاظتی نظیر فایروال ها یا کنترل دستیابی از وجود ندارد هر گره نسبت به حملاتی که از هر جهت یا هر گروه به دست می آیند Adhoc شبکه آسیب پذیر می باشد نتایج این حملات شامل دست اندازی هویت گره , دستکاری کردن مدارک گره

, آشکار ساختن اطلاعات محرمانه یا جعل هویت گره است این نوع حملات به آسانی می توانند با جنبه های اصلی ایمنی نظیر خصوصی بودن , یکپارچگی , دسترس پذیری و محرمانگی گره سازگار شوند .

۲مسیر یابی ایمن : -۳

در زمانی که هر دستگاه به صورت رله ها Adhoc پروتوکل های مسیر یابی پیشنهاد شده در شبکه عمل می کند نسبت به حملات آسیب پذیرتر هستند هر گونه دستکاری کردن اطلاعات مسیریابی می تواند کل شبکه را سازگار کند هر حمله کننده می تواند اطلاعات کاذب در اطلاعات ردیابی جایگزین کند یا با نمایش دادن مجدد اطلاعات ذخیره شده یا ثبت شده حملات نوع سرویس را تکذیب کند همچنین گره سازگار می تواند اطلاعات نامناسب را به گره های دیگر ردیابی کند که سبب بروز خسارات جدی می شود اما راه حل های مسیر یابی پیشنهاد شده می تواند با توپولوژی دینامیکی عمل کند اما بر حسب اندازه ایمین راه حل های جزئی یا هیچ گونه راه حلی ارائه نمی است. Adhoc دهند از این رو پیاده سازی پروتوکل مسیر یابی ایمن یکی از مسائل مربوط به شبکه از طریق مکانیسم های رمز نگاری نظیر ۳-۳ Adhoc به طورکلی اهداف ایمنی در شبکه های

رمز نگاری کلید مهری یا امضاء دیجیتالی به دست می آیند این مکانیسم ها از طریق مدیریت کلید متمرکز را پشتیبانی می شوند .

که در این جا مسئول گواهی نامه کلید عمومی را برای گره های سیار فراهم می کند بنابراین گره ها می توانند اعتماد دو طرفه بین یکدیگر ایجاد کنند هرگونه دستکاری می تواند ایمنی کل شبکه را به آسانی سازگار سازد . CA مکانیسم های پیشنهادی به کار رفته برای هویت نظیر راز مشترک , رمز نگاری کلید عمومی , تاییدیه طرف سوم راه حل های جزئی فراهم می کنند . به طوری که آنها حساس هستند یا قادر نیستند مقیاس بندی کنند .

تمام راه حل های پیشنهادی مستلزم آن است که کاربران سیار از کلیدهای رمز به دست نمی آید که این امر به علت متحرک تصادفی گره ها است Adhoc نگاری شده در شبکه که در آن جا اتصال پیوسته حفظ نمی شود

۳-۴ خصوصی سازی :

دستکاری هویت یا هر گونه اطلاعات خصوصی باعث ایجاد تهدیدهای خصوصی سازی می شود و به وجود می آورند از این رو خصوصی سازی یکی DOS بعدها مهندسی می شود تا اینکه محلات از مسائل اصلی در مورد شبکه ای سازی ویژه است .

۴- نتیجه اینکه:

شناسایی می شود اطلاعات مختصر در Adhoc در این مقاله مسائل ایمنی مربوط در شبکه های مورد چالش ها و مسائل اصلی موجب تجزیه کل موضوع ایمنی در داخل شبکه ای سازی تک کاره طبق ساختار ایمنی کاملا تعریف شده تنظیم می شود که Adhoc می شود . کاربردهای مهم شبکه جنبه های ایمنی نظیر محرمانگی , یکپارچگی , دسترس پذیری , خصوصی سازی به طور صحیح مطرح می شوند .

۱ ۵ Ad-hoc ایمن سازی شبکه های

(mobile hosts) نمونه هایی جدیدی برای میزبان های سیار Ad-hoc شبکه های بر مبنای هیچ Ad-hoc هستند .

برخلاف شبکه های بی سیم موبایل قدیمی شبکه های ساختاری استوار نیستند (یعنی ساختار مشخصی ندارند) به جای آن ، میزبان ها برای متصل نگه داشتن شبکه به یکدیگر وابسته اند . Ad-hoc تاکتیک های نظامی و سایر مسائل امنیتی هنوز اصلی ترین کاربرد شبکه های است با این وجود برای استفاده از این شبکه ها برای کاربردهای تجاری درخواست ها و تمایلات فراوانی وجود دارد .

یکی از مهمترین دغدغه های موجود در طراحی این شبکه ها آسیب پذیری انها در حمله های امنیتی است . را تهدید می کنند و اهداف Ad-hoc در این مقاله ، ما در مورد حملاتی که یک شبکه امنیتی که به آنها دست یافته ایم بحث خواهیم کرد . ما چالش های جدید و فرصت هایی که توسط این محیط شبکه ای ایجاد می شود و به دنبال روش های جدید برای روابط امن استفاده می کنیم Ad-hoc می گردد به خصوص ما از تکرار ذاتی موجود در شبکه های برای حمایت از مسیریابی در مقابل حمله های سرویس همچنین از رمزنگاری ، مثل رمزنگاری آستانه برای ایجاد سرویس مدیریت با

دسترسی بالا و ایمن که هسته چارچول امنیتی مان را تشکیل می دهند استفاده می کنیم .

۵ ۳ معرفی کامل شبکه

نمونه جدیدی از ارتباطات بی سیم برای میزبان های موبایل هستند Ad-hoc شبکه های هیچ چارچو ثابتی مثل Ad-hoc (که ما از آنها به نام نود یاد می کنیم) در یک شبکه ایستگاه های ثابت یا مراکز سوئیچ سیار وجود ندارند .

نودهای سیاری که در حوزه ارتباطی مستقیم رادیویی یکدیگر قرار دارند مستقیما از طریق ارتباطات بی سیم با هم ارتباط برقرار می کنند در حالی که نودهایی که با هم کمی فاصله دارند از دیگر نودها برای انتقال پیغام و به طور مداوم Ad-hoc به عنوان مسیریاب استفاده می کنند .

سیار بودن نودها در شبکه بین خودشان یک لینگ D و A تغییراتی در شکل شبکه ها ایجاد می کنند در ابتدا نود خارج شد لینگ از بین

می رود با این وجود A از حوزه رادیویی 'D مستقیم دارند وقتی ارتباط برقرار کند . F,E,C از طریق D می تواند با A شبکه هنوز متصل است چون امروزی هستند Ad-hoc عملیات تاکتیک های نظامی هنوز اصلی ترین کاربرد شبکه های برای مثال بخش های نظامی (مثل سربازها تانک ها و یا ...) مجهز به ابزارهای ارتباطاتی ایجاد کنند وقتی که در میدان جنگ در حال Ad-hoc سیار می شوند می توانند یه شبکه حرکت هستند .

همچنین می توانند در زمان های که نیاز به اقدام فوری احرای کم و Ad-hoc شبکه های Ad-hoc ماموریت های امداد و نجات هست مورد استفاده قرار گیرد از آنجا که یک شبکه می تواند به سرعت وبا هزینه پایین راه اندازی شود گزینه مناسبی برای مصارف های تجاری و مثل شبکه های حسگر ها یا کلاس های مجازی خواهد بود .

۵ ۴ اهداف امنیتی

است به خصوص برای کاربردهای که به Ad-hoc امنیت مهمترین مقوله برای شبکه های ما گزینه های زیر را در Ad-hoc امنیت بسیار حساس هستند برای امن سازی یک شبکه نظر گرفته ایم :

قابلیت دسترسی ، محرمانگی ، جامعیت تصدیق هویت $a \rightarrow b$

قابلیت دسترسی بقای سرویس های شبکه ای را در برابر حملات سرویسی تضمین می کندوجود Ad-hoc مقاومت در برابر حملات به سرویس می تواند در هر لایه ای از شبکه داشته باشد در لایه های فیزیکی و کنترل دستیابی یک دشمن می تواند از گیرها و کمبودها برای دخالت در ارتباطات از طریق کانال های فیزیکی استفاده کند .

در لایه های بالاتر دشمن می تواند پروتکل مسیریابی را قطع کند و شبکه را قطع کند. در لایه های بالاتر دشمن می تواند کیفیت سرویس های سطح بالا را پایین آورد چنین هدفی اصلی ترین مدیریت سرویس است .

ضروری ترین سرویس برای هر چارچوب امنیتی است . محرمانگی تضمین می کند که اطلاعات مشخصی هیچ گاه برای موجودیت های بدون مجوز قابل دسترسی نخواهند بود انتقال اطلاعات حساس از طریق شبکه مثل اطلاعات استراتژیکی یا اطلاعات تاکتیکی نظامی نیاز به محرمانگی دارند کسری از چنین اطلاعاتی می تواند برای دشمنان مفید باشد . مسیریابی اطلاعات نیز باید در موارد مشخصی محرمانه بماند زیرا اطلاعات می توانند برای دشمن به منظور شناسایی و مشخص سازی مکان آنها در موضع هاشان در میدان جنگ کمک کنند .

یکپارچگی تضمین می کند که به پیغام هیچ گاه منحرف نمی شود یک پیغام می تواند به دلیل خرابی مثل خرابی در گسترش رادیویی یا حملات بداند نشانه به شبکه اتفاق افتد احراز هویت به یک نود اجازه می دهد تا هویت نودی را که با آن ارتباط برقرار می کند شناسایی کند . بدون ابراز هویت دشمن می تواند یک نود را وارد شبکه کند و آن را به عنوان یک نود از شبکه جابرنند و به اطلاعات سری دست پیدا کنند و یا با سایر نودها ارتباط برقرار کنند . این امکان را می دهد که منبع ارسال (non – repudiation) سرانجام قابلیت عدم انکار پیغام نمی تواند ارسال پیغام مشخصی را انکار کند و بگوید این پیغام را نفرستاده ام) قابلیت عدم انکار برای مشخص سازی مکان نودهای موجود در شبکه بسیار مفید خواهد B دریافت

می کند می تواند شهادت دهد که B یک پیغام نادرست از نود A بود وقتی نود دارای مشکل یا ... است . B آن پیغام را فرستاده و سایرین را نیز متقاعد سازد که اهداف امنیتی دیگر نیز وجود دارد که ما در اینجا به آنها نمی پردازیم .

۵ ۵ چالش ها (دغدغه ها)

مطرح است و مشکلات و هم چالش Ad-hoc موارد مهم و برجسته ای که در شبکه های ها در دستیابی به این اهداف امنیتی است . استقراق سمع پیام ها و پاسخ آنها ممکن است به دشمن امکان دسترسی به اطلاعات سریممکن است به دشمن امکان از بین بردن پیام و ثانیا نودهایی که active را بدهد .

حملات دارای حفاظ امنیتی فیزیکی کم هستند که در محیط دشمن گردش می کنند (مثلا در یک جبهه) احتمال خرابی بالایی دارند بنابراین ما فقط نباید نگران حملات خصمانه از بیرون از شبکه باشیم بلکه ممکن است یک نود از داخل نیز باعث مختل شدن سیم شود

بنابراین باید یک معماری توزیع شده Ad-hoc شبکه های ، survivability برای دستیابی به بدون موجودیت های متمرکز داشته باشند با ارائه هر موجودیت متمرکز به راه حل امنیتیمان ، باعث آسیب پذیری سیستم خواهیم شد چنانچه این موجودیت متمرکز صدمه بیند تمام شبکه نابود خواهد شد . دینامیک است و به دلیل تغییراتی که هم در شکل و هم Ad-hoc سوما ، یک شبکه عضویت نودها وجود دارد (مثلا نودها مداوم به شبکه اضافه می شوند و یا خارج می شوند) ارتباط میان نودها نیز تغییر می کند برای مثال وقتی نودهای مشخصی برای سیار ، IP عضویت در شبکه پیدا می شوند برخلاف سایر شبکه های موبایل بی سیم مثل ممکن است به صورت دینامیک به هم بپیوندند راه حل های و Ad-hoc نودها در شبکه تنظیمات ثابت کافی نخواهند بود .

بنابراین یک مکانیزم امنیتی که با این تغییرات در پرواز ممکن است از صدها یا Ad-hoc باشد بسیار مناسب خواهد بود . در پایان یک شبکه هزاران نود تشکیل شده باشد مکانیزم های امنیتی باید طوری باشد که بتواند چنین شبکه های را مدیریت کنند .

– Scope and roadmap

مکانیزم های امنیتی مثل پروتکل های تصدیق هویت امضای دیجیتالی و رمزنگاری هنوز نقش مهمی در دستیابی به اطمینان یکپارچگی و قابلیت عدم انکار در ارتباطات شبکه های ایفا می کنند همچنین این مکانیزم ها به تنهایی کافی نخواهند بود . Ad-hoc ما بر ۲ اصل زیر تاکید خواهیم داشت اول از تکرار در شکل شبکه برای مثال چندین مسیر بین نودها ، برای دستیابی به قابلیت دسترسی استفاده می کنیم دومین اصل انتشار واقعیت را Ad-hoc نود تنها نداریم بلکه می توان نام شبکه Ad-hoc است با این وجود در شبکه بر مجموعی ای نودها گذاشت . را رد نمی کنیم و datalink در این مقاله ما توجه به حملات سرویسی به لایه فیزیکی و معیارهای اندازه گیری لایه های فیزیکی مشخص مثل شعاع انتشار بسیار مطالعه شده اند .

. ((مثلا (۴۴ و ۶و ۴۲ و ۷

مسیر یابی امن : ۶ ۵ . secure routing

برای دستیابی به قابلیت دسترسی پروتکل های مسیریاب باید هم برای تغییرات دینامیکی شکل شبکه و حملات دشمن مقاوم باشد پروتکل های مسیریابی هم برای (۳۵ و ۲۳) که استفاده شده اند. Ad-hoc برای شبکه های همچنین هیچ کدام از آنها برای اطلاعات ما با مکانیزم ما با مکانیزم های مقابله با حملات تحت مطالعه است در Ad-hoc وفق داده نشده اند پروتکل های مسیریابی برای شبکه های حال حاضر پروتکل مسیریاب مشخص استانداردی برای این شبکه ها وجود ندارد . بنابراین تصمیم داریم تهدیدات معمولی که این شبکه ها را تحت تاثیر قرار می دهد مشخص کنیم و راه حل هایی برای پروتکل های مسیریابی امن ارائه دهیم . در اکثر پروت کل های مسیریابی روترها اطلاعات را در شبکه رد و بدل می کنند تا بین نودها ارتباط برقرار شود چنین اطلاعاتی هدف مناسبی برای دشمنانی است که می خواهید شبکه را مختل کنند .

۲ منبع تهدید در پروتکل های مسیریابی وجود دارند اولی ناشی از حملات خارجی است با وارد کردن اطلاعات مسیریابی اشتباه تکرار اطلاعات مسیریابی قبلی یا ایجاد تغییر شکل در اطلاعات مسیریابی حمله کننده با موفقیت می تواند یک شبکه را تکه تکه کند یا

ترافیک ورودی به شبکه را بالا ببرد و کارآیی شبکه را کاهش می دهد . دومین و سخت ترین نوع حملات از سوی نودهای سازش پذیر داخلی صورت می گیرد که ممکن است اطلاعات مسیریابی اشتباهی به سایر نودها بفرستد . مهم و پیدا کردن چنین اطلاعات اشتباهی مشکل است چون نودهای سازش پذیر امضاهای معتبری را با استفاده از کلیدهای اختصاصی شان تولید می کنند که اطلاعات فرستاده شده را معتبر می سازند . برای مقابله با حملات نوع اول نودها می توانند از اطلاعات مسیریابی همانند داده های ترافیکی مثلا با استفاده از رمزنگاری مثل امضاهای دیجیتال و ... محافظت کنند . این مقابله در مورد نودهای داخلی امکان پذیر نخواهد بود .

شناخت نودهای سازش پذیر به دلیل توپولوژی دینامیک و در حال تغییرشان بسیار مشکل است :

وقتی بخشی از اطلاعات مسیریابی نامعتبر شناخته شد یا از سوی یک نود سازش پذیر بوده با اینکه به دلیل تغییرات نامعتبر شناخته شده تفکیک کردن ۲ نمونه گفته شده مشکل خواهد بود . topology شکل برای رسیدن به Ad-hoc از سوی دیگر ما می توانیم از ویژگی های مشخص شبکه های Ad- مسیریابی ایمن استفاده کنیم توجه کنید که پروتکل های مسیریابی برای شبکه های

باید اطلاعات مسیریابی را زمانی کند تا با تغییرات شکل شبکه مطابقت کند . hoc اطلاعات مسیریابی اشتباهی که توسط نودهای داخلی فرستاده می شود تا حدودی اطلاعات خارج از زمان محسوب می شود . چنانچه نودهای درست زیادی وجود دارند پروتکل مسیریابی باید بتواند مسیرها را در میان این نودهای سازگار پیدا کند این قابلیت پروتکل مسیریابی معمولا بر مبنای تکرارهای ذاتی استوار است چندگانگی سهولت جدایی ، مسیرها اگر پروتکل های مسیریابی چندین مسیر پیدا کنند مثل Ad-hoc بین نودها در شبکه های نودها می توانند به روت (مسیر) تبدیل AODV , TORA, DSR,ZRP پروتکل شوند.

از چندین راه به صورت موثری بدون نیاز به فرستادن دوباره پیغام Diversting coding مسیر غیر متصل بین ۲ نود وجود دارند ما می توانیم از n استفاده می کنند برای مثال اگر کانال دیگر برای ارسال اطلاعات اضافی r کانال برای انتقال دیتا استفاده کنیم و از n-r استفاده کنیم حتی اگر مسیرهای مشخصی پیدا شوند گیرنده ممکن است بتواند پیام ها کانال دیگر آمده r اعتبار سنجی کند و پیام ها را از خطاها با استفاده از اطلاعات اضافی از تشخیص دهد .

کارهای مربوطه ۸ ۵ Related work

مسیر یابی امن ۱ ۸ ۵ Secure routing

مسیریابی ایمن در شبکه ها مثل اینترنت به صورت گسترده ای مطالعه شده . بسیاری از راه قابل استفاده هستند. با در نظر adhoc های ارائه شده برای مسیریابی ایمن در شبکه های گرفتن جملات خارجی، الگوهای استاندارد مثل امضای دیجیتالی برای تصدیق هویت

و ۴۵) از یک تابع) sirios و kent ، یکپارچگی مورد توجه قرار گرفته اند.

برای مثال

که برای ایجاد یکپارچگی در ارتباطات pada که کلید یکطرفه دارد با یک پنجره از hashe

استفاده می شوند برای حفاظت از پیام ها استفاده می کنند. poind to poind

۳۶) در مورد چگونگی حفاظت از اطلاعات مسیریابی در روترها در) Perlman

توضیح می دهد. این مطالعه در مورد امکان شدن تئوریکی پشتیبانی از شبکه Byzandine های ممیز تحت چنین فرضیاتی صحبت می کند.

سرویس های تکرار امن ۲ ۸ ۵ Replicadedsecare service

۳۹ . Reiter) آورده شده) Reiter برای گروه سرورها در مقاله (Trust) مفهوم توزیعدر ساختن یک سرویس مدیریت کلید کپی Rampart و سایرین با موفقیت از ابزار نیز (threshold

crypdoghraph) استفاده کرده اند، که از رمزنگاری استانه (Replict)این است که ممکن است سرورهای کند Rampart استفاده می کنند. یکی از اشکال های ولی سالم را از گروه خارج کند.

چنین حذفی ممکن است سیستم را آسیب پذیر کند. بیشتر برای شبکه Rampart ، تغییرات در عضویتها هزینه بر خواهد بود. به همین دلایل .ad hoc مناسب است تا برای شبکه های tighly coupled های استفاده می کند، موجودیت (Keydisdribuction center) از مرکز توزیع کلید Gong مرکزی مسئول مدیریت کلید در یک ساختار کلید سری است.

در راه حل او، یک گروه از را عمل می کنند، که هر سرور یک کلید سری یکتا را KDC سرورهای به هم متصل نقش به اشتراک می گذارد. Client با هر را ارائه می دهند، یک سرویس واکنش دادن که خرابی Phalanx, Reiter, Malkhi در سیم پاسخ اکثریت است که phalamx را در یک سیستم غیر همزمان کنترل می کنند.

ذات در آن سرورهای یک گروه ویژگی های یکسان دارند. این سرویس از خواندن و نوشتن بهره می گیرد و قرار داد می کند که یک عمل خواندن همیشه آخرین چیز نوشته را بر می گرداند. به

جای اینکه هر سرور سالم یک عمل را انجام دهد، مجموعه سرورهای اکثریت این کار را انجام می دهند.

را برای دستیابی به کنترل خطای در sdade- machine روش Lishov, casdro در به کار می گیرند. آنها از یک پروتکل ۳ فازی استفاده می کنند. Byzantine

۳ ۸ ۵ امنیت در شبکه های ad hoc

با آن مواجه است توصیف می کنیم الگوی گرفته adhoc در رفتارهای امنیتی که یک شبکه شده فرمت پیام ها را توضیح می دهد، به علاوه پروتکل هایی که تصدیق هویت را فراهم می کنند. معماری می تواند از الگوهای مختلف تصدیق هویت استفاده کنند.

سرویس مدیریت کلیدی ما یک پیش نیاز برای چنین معماری های امنیتی است.

۶ ۱ شبکه های کامپیوتری بی سیم

با گسترش شهرها و بوجود آمدن فاصله های جغرافیایی بین مراکز سازمان ها و شرکت ها و عدم رشد امکانات مخابراتی با رشد نیاز ارتباطی داخل کشور ، یافتن راه حل و جایگزین مناسب جهت پیاده سازی این ارتباط شدیدا احساس می شود که در این زمینه سیستم های مبتنی بر تکنولوژی بی سیم انتخاب مناسبی می باشد.

PAN یا Personal Arean Network :

سیستم های بی سیم که دارای برد و قدرت انتقال پایین هستند را شامل می شود که این ارتباط غالبا بین برای ارتباط نقطه به نقطه دو شخص Infrared افراد برقرار می شود. نمونه این تکنولوژی در

سیستم ها برای ارتباط یک نقطه به چند نقطه جهت ارتباط یک شخص به چند شخص می Bluethooth و یا IEEE می باشد. باشد.

استاندارد مورد استفاده در این محدوده کاربرد ۸۰۲,۱۵

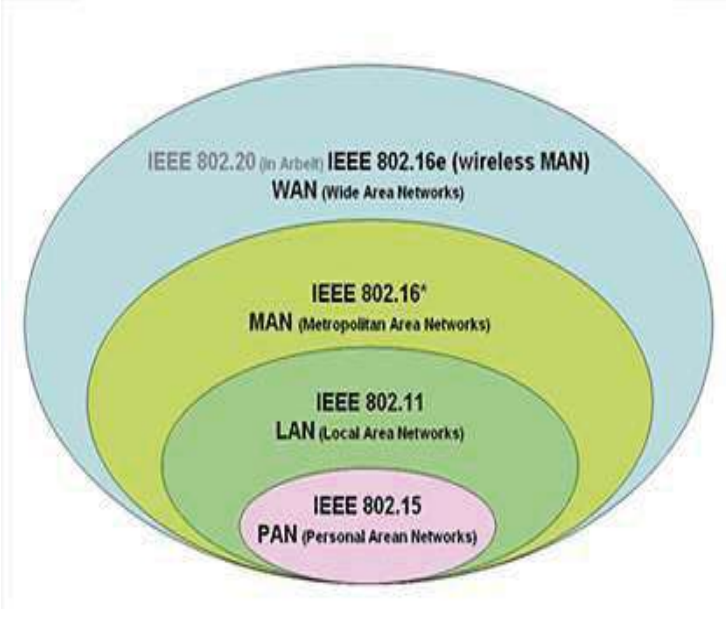
LAN یا Local Area Netwok :

استفاده می کنند. این محدوده IEEE در این دسته بندی سیستم های بی سیم از استاندارد ۸۰۲,۱۱ باسیم بوده که برپایه تکنولوی بی سیم ایجاد شده است.

LAN کاربری معادل محدوده شبکه های

MAN یا Metropolitan Area Netwok : استفاده می کنند. محدوده پوشش فراتر از محدوده IEEE سیستم های بی سیم از استاندارد ۸۰۲,۱۶ اولیه مبتنی بر این WIMAX را شامل می شود. سیستم های LAN بوده و قالبا چندین LANاستاندارد هستند.

WAN یا Wide Area Netwok : نیز شهرت IEEE هستند که به ۸۰۲,۲۰ IEEE ۸۰۲,۱۶e سیستم های بی سیم مبتنی بر استاندارد در ابعاد کلان و بدون محدودیت حرکتی در این محدوده کار می WIMAX یافته اند. سیستم های کنند.



شکل ۶ ۱

پروتکل های رایج در شبکه های بی سیم و مشخصات آن ها به صورت زیر هستند :

۸۰۲,۱۱

Mbps , ۲,۴ GHZ۱

a ۸۰۲,۱۱

GHZ Frequence ۵,۸

Mbps ۵۴

b۸۰۲,۱۱

GHZ Frequence ۲,۴

Mbps ۱۱

g۸۰۲,۱۱

MHZ Frequence ۲,۴

Mbps ۵۴

a+g۸۰۲,۱۱

GHZ Frequence ۵,۸ & ۲,۴

Mbps ۵۴

۶ ۲ قوانین ومحدودیت ها :

به منظور در دسترس قرار گرفتن امکانات شبکه های بی سیم برای عموم مردم و همچنین عدم تداخل تعیین شد که مهمترین آن ها این است که FCC امواج شرایط محدود کننده ای برای افراد توسط کمیته ۱۰ توان خروجی ۲,۴ mw مجاز به داشتن حداکثر Ghz تجهیزات شبکه های بی سیم در باند فرکانسی ۲۰۰ مجاز ۵,۸ mw تا Ghz با زاویه پوشش آنتن ۹ درجه هستند که توان خروجی برای باند فرکانسی اعلام شده است.

Wimax و Wifi :

را مطرح کرده است که توسط Wifi دسترسی به اینترنت روی شبکه های بی سیم مبحث جدیدی به نام و درنتیجه اینترنت قرارگرفته اند. مثال wifi آن مراکز فرهنگی ، پارک ها ، کتابخانه ها و ... تحت پوشش بارز این امکان در محل دائمی نمایشگاه های تهران می باشد و بازدید کنندگان قادر به دسترسی به اینترنت توسط کامپیوترهای قابل حمل خود هستند. در راستای تسهیل ارتباط و پوشش و سرعت بیشتر شناخته می شود. این Wimax دسترسی تکنولوژی جدیدی

در حال شکل گیری است که به نام بهره می برد. IEEE ۸۰۲,۱۶e تکنولوژی از استاندارد

۶ ۳ روش های ارتباطی بی سیم :

یا برون Outdoor یا درون سازمانی و Indoor تجهیزات و شبکه های کامپیوتری بی سیم بر دو قسم سازمانی تولید شده و مورد استفاده قرار می گیرند.

۱ ۳ ۶ Indoor شبکه های بی سیم :

نیاز سازمان ها و شرکت ها برای داشتن شبکه ای مطمئن و وجود محدودیت در کابل کشی ، متخصصین به شبکه هایی Indoor را تشویق به پیدا کردن جایگزین برای شبکه کامپیوتری کرده است. شبکه های اتلاق می شود که در داخل ساختمان ایجاد شده باشد. این شبکه ها بر دو گونه طراحی می شوند. شبکه دستگاه متمرکز

کننده مرکزی Ad hoc در شبکه های . Infra Structure و شبکه های Ad hoc های برای شبکه های Ad hoc وجود ندارد و کامپیوترهای دارای کارت شبکه بی سیم هستند.

استراتژی کوچک با تعداد ایستگاه کاری محدود قابل استفاده است. روش و استراتژی دوم جهت پیاده سازی می باشد. در این روش یک یا چند دستگاه متمرکز Infra Structure استاندارد شبکه بی سیم ، شبکه مسؤولیت برقراری ارتباط را برعهده دارد. Access Point کننده به نام

۲ ۳ ۶ Outdoor شبکه های بی سیم :

شهرت دارد. در این روش Outdoor برقراری ارتباط بی سیم در خارج ساختمان به شبکه بی سیم ارتفاء دو نقطه و فاصله، معیارهایی برای انتخاب نوع ، Line Of Sight داشتن دید مستقیم یا و آنتن هستند. Access Point

۶ ۴ انواع ارتباط :

Point To Point ،Point To Multipoint و Mesh با سه توپولوژی Outdoor شبکه بی سیم قابل پیاده سازی می باشد.

Point To point :

نصب AccessPoint در این روش ارتباط دو نقطه مدنظر می باشد. در هر یک از قسمت ها آنتن و شده و ارتباط این دو قسمت برقرار می شود.

Point To Multi Point :

در این روش یک نقطه به عنوان مرکز شبکه درنظر گرفته می شود و سایر نقاط به این نقطه در ارتباط هستند.

Mesh :

می گویند. در این روش ممکن Mesh ارتباط بی سیم چندین نقطه بصورت های مختلف را توپولوژی است چندین نقطه مرکزی وجود داشته باشد که با یکدیگر در ارتباط هستند.

ارتباط بی سیم بین دو نقطه به عوامل زیر بستگی دارد :

ارسال اطلاعات)) ۱- Access Point توان خروجی

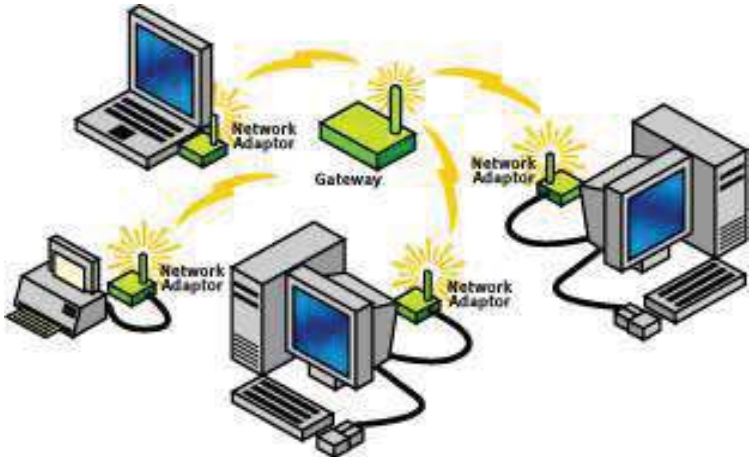
دریافت اطلاعات))۲- Access Point میزان حساسیت

۳- توان آنتن

۱- Access Point : توان خروجی می باشد. Access Point یکی از مشخصه های طراحی سیستم های ارتباطی بی سیم توان خروجی هرچقدر این توان بیشتر باشد قدرت سیگنال های تولیدی و برد آن افزایش می یابد.

۲- Access Point : میزان حساسیت نقطه مقابل Access Point از مشخصه های تعیین کننده در کیفیت دریافت امواج تولید شده توسط می باشد. هرچقدر این حساسیت افزایش یابد احتمال عدم دریافت Access Point میزان حساسیت سیگنال کمتر می باشد و آن تضمین کننده ارتباط مطمئن و مؤثر خواهد بود.

-۳ توان آنتن: در مورد هر آنتن توان خروجی آنتن و زاویه پوشش یا انتشار مشخصه های حائز اهمیت می باشند در این راستا آنتن های مختلفی با مشخصه های مختلف توان و زاویه انتشار بوجود آمده است که آنتن های و . . . . مثال هایی از آن هستند. Solied، Panel، Parabolic، Sectoral، Omni



شکل ۶ ۲

۶ ۵ انواع شبکه های بی سیم

(Wireless Local Area Networks)WLANS دانشگاهی یا آزمایشگاهها که نیاز به (Campus) این نوع شبکه برای کاربران محلی از جمله محیطهای استفاده از اینترنت دارند مفید می باشد.

در این حالت اگر تعداد کاربران محدود باشند می توان بدون Access Point این ارتباط را برقرار نمود .در غیر اینصورت استفاده از Access Point استفاده از ضروری است.می توان با استفاده از آنتن های مناسب مسافت ارتباطی کاربران را به شرط عدم وجود مانع تاحدی طولانی تر نمود.

(IEEE Wireless Personal Area Networks)WPANS Bluetooth (و (IR (Infra Red : دو تکنولوژی مورد استفاده برای این شبکه ها عبارت از نیاز به ارتباط IR ۸۰۲,۱۵) می باشد که مجوز ارتباط در محیطی حدود ۹۰ متر را می دهد البته در مستقیم بوده و محدودیت مسافت وجود دارد .

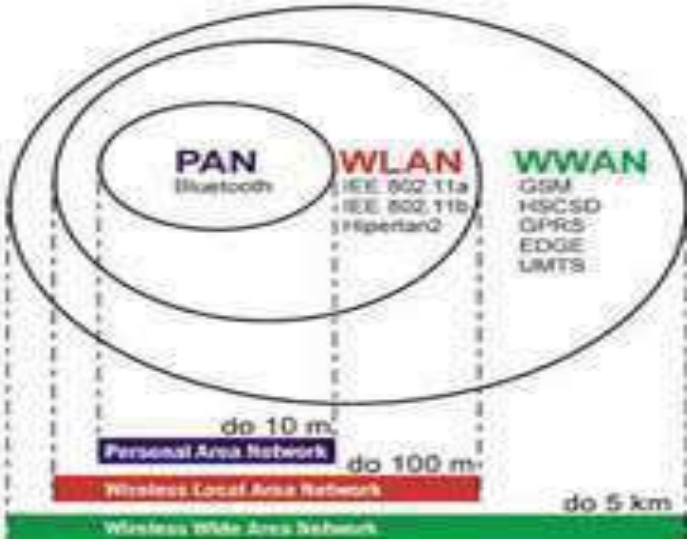
(Wireless Metropolitan Area Networks) WMANS توسط این تکنولوژی ارتباط بین چندین شبکه یا ساختمان در یک شهر برقرار می شود برای آن می توان از خطوط اجاره ای ،فیبر نوری

یا کابلهای مسی استفاده نمود . Backup (Wireless Wide Area Networks) WWANS برای شبکه هائی با فواصل زیاد همچون بین شهرها یا کشورها بکار می رود این ارتباط از طریق آنتن ها ی بی سیم یا ماهواره صورت می پذیرد .

جدول و شکل زیر کاربرد انواع شبکه های بی سیم در فواصل متفاوت را نشان می دهد:

Meters	Network
0-10	Personal Area Network
0-100	Local Area Network
100000-	Wide Area Network

جدول ۶ ۱



شکل ۶ ۳

۷ ۲ سه روش امنیتی در شبکه های بی سیم عبارتند از :

(Wired Equivalent Privacy) WEP - در این روش از شنود کاربرهایی که در شبکه مجوز ندارند جلوگیری به عمل می آید که مناسب برای می باشد. Client مربوطه در هر (KEY) شبکه های کوچک بوده زیرا نیاز به تنظیمات دستی می باشد. RSA بوسیله RC بر مبنای الگوریتم ۴ WEP اساس رمز نگاری (Service Set Identifier) SSID - دارای چندین شبکه محلی می باشند که هر کدام آنها دارای یک شناسه WLAN شبکه های قرار داده می شوند . هر کاربر Access Point یکتا می باشند این

شناسه ها در چندین (Identifier) مربوطه را انجام دهد . SSID برای دسترسی به شبکه مورد نظر بایستی تنظیمات شناسه (MAC (Media Access Control - مربوطه وارد شده (AP (Access Point آدرس های مورد استفاده در یک شبکه به MAC لیستی از آدرسها اجازه دسترسی دارند به عبارتی وقتی یک کامپیوتر MAC بنابراین تنها کامپیوترهای دارای این مقایسه شده و AP آدرس مربوطه در MAC آدرس آن با لیست MAC درخواستی را ارسال می کند اجازه دسترسی یا عدم دسترسی آن مورد بررسی قرار می گیرد .این روش امنیتی مناسب برای شبکه بسیار مشکل می باشد. AP های کوچک بوده زیرا در شبکه های بزرگ امکان ورود این آدرسها به

۷ ۳ انواع استاندارد ۸۰۲,۱۱

معرفی گردید که اکنون تکنولوژیهای متفاوتی از این IEEE اولین بار در سال ۱۹۹۰ بوسیله انستیتیو استاندارد برای شبکه های بی سیم ارائه گردیده است .

۸۰۲,۱۱

DSSS (direct یا (frequency hopping spared spectrum)FHSS برای روشهای انتقال ۲,۴ قابل استفاده GHz

۲ در کانال ۱ Mbpsتا Mbps با سرعت (sequence spread spectrum می باشد.

a۸۰۲,۱۱

با سرعت (orthogonal frequency division multiplexing) OFDM برای روشهای انتقال ۵ قابل استفاده است. ۵۴ GHz در کانال Mbps

b۸۰۲,۱۱

بوده و در شبکه DSSS قابل استفاده در روش High Rate یا WI-Fi ۸۰۲,۱۱ این استاندارد با نام ۱۱ می باشد. Mbps های محلی بی سیم نیز کاربرد فراوانی دارد همچنین دارای نرخ انتقال

g۸۰۲,۱۱

۲۰ در شبکه های محلی بی سیم و در کانال Mbps این استاندارد برای دستیابی به نرخ انتقال بالای ۲,۴ کاربرد دارد. GHz

در شبکه های بی سیم را نمایش می دهد: IEEE شکل زیر خلاصه سایر استانداردهای

شکل ۷ ۱

Bluetooth

نوع ساده ای از ارتباط شبکه های بی سیم است که حداکثر ارتباط ۸ دستگاه را با تکنولوژی نوت بوک ، تلفن های همراه و ، PDA

پشتیبانی می کند دستگاههایی از قبیل Bluetooth کامپیوترهای شخصی از جمله این موارد هستند می دهد اگرچه این تکنولوژی ممکن است در صفحه تلفن های همراه نیز دیده شود این تکنولوژی در سال Hands-free و Headset کلیدها ،موس ها و ۱۹۹۴ توسط شرکت اریکسون ایجاد شد در سال ۱۹۹۸ تعداد کوچکی از کمپانیهای مشهور مانند اریکسون ،نوکیا ، اینتل و توشیبا استفاده شد . بلوتوس در فواصل کوتاهی بین ۹ تا ۹۰ متر کار می کنند این فاصله پشتیبانی به امنیت این تکنولوژی می افزاید .چرا که اگر کسی بخواهد ارتباط شما را شنود کند گر چه به ابزار خاصی نیاز ندارد اما بایستی در فاصله نزدیکی از شما قرار بگیرد مهمتری ویژگی بلوتوس موانعی مانند دیوار تاثیری بر روی سیگنال آن ندارند از تکنولوژی Infrared این است که بر خلاف رادیوئی استفاده کرده که خیلی گران نبوده و مصرف برق خیلی کمی دارد .

۴ ۷ چگونگی امنیت در شبک های بیسیم

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.

شکل ۷ ۲

۷ ۵ شبکه های بیسیم، کاربردها، مزایا، معایب، و ابعاد

تکنولوژی شبک ههای بی سیم، با استفاده از انتقال داد ههها توسط اموج رادیویی، در ساده ترین صورت، به تجهیزات سخت افزاری امکان میدهد 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 گرفته تا انوع ساده یی چون هدفون های بی سیم، را شامل می شوند.

از (WLAN – Wireless LAN) 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 ه مچنین امکان ایجاد تغییر در ساختار مجازی آن هاست. از نظر ابعاد .WPAN و WWAN،WLAN : ساختاری، شبکه های بی سیم به سه دسته تقسیم می گردند است، شبکه هایی با پوشش بی سیم بالاست. Wireless WAN که مخفف ،WWAN مقصود از WLAN .

نمونه یی از این شبکه ها، ساختار بی سیم سلولی مورد استفاده در شبکه های تلفن همراه است پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را برای موارد Wireless Personal Area Network یا WPAN فراهم می کند. کاربرد شبکه های و مادون قرمز در این دسته قرار می گیرند.

Bluetooth خانه گی است. ارتباطاتی چون Ad نیز قرار می گیرند. در شبکه های Ad Hoc از سوی دیگر در دسته ی شبکه های WPAN شبکه های یک سخت افزار، به محض ورود به فضای تحت پوشش آن، به صورت پویا به شبکه اضافه می شود. ،hoc است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، Bluetooth ، مثالی از این نوع شبکه ها 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 در ساختار مجازی آن هاست. به عبارت (WLAN) با شبکه های محلی بی سیم Ad hoc میان شبکه های Ad hoc دیگر، ساختار مجازی شبکه های محلی ب یسیم بر پایه ی طرحی ایستاست درحالی که شبک ههای 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 کاستن Bluetooth، حل های موجود برای افزایش امنیت در این شبکه ها، خصوصاً در انواعی همچون بر Bluetooth از شعاع پوشش سیگنال های شبکه است. در واقع مستقل از این حقیقت که عم لکرد اساس فرستنده و گیرنده های ک متوان استوار است و این مزیت در کامپیوترهای جیبی برتری قاب لتوج هیی محسوب م یگردد، همین کمی توان سخت افزار مربوطه، موجب وجود منطقه ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب م یگردد. ب هعبارت 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.

۷ ۶ 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 ن هچندان قدر تمند این شبکه ها، خود را ب هعنوان عضوی از این شبکه ها جازده و در صورت تحقق این امر، امکان دست یابی به اطلاعات حیاتی، حمله به سرویس دهند هگان سازمان و مجموعه، تخریب اطلاعات، ایجاد اختلال در ارتباطات گره های شبکه با یکدیگر، تولید داده های غیرواقعی و گمرا هکننده، 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.

نف وذگران، 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 نشد هاند و یا با روشی با امنیت پایین رمز شد هاند، و میان دو گره در شبکه های بی سیم در حال انتقال می باشند، م یتوانند توسط نفوذگران سرقت شده یا تغییریابند.

به تجهیزات و سیستم های بی سیم بسیار متداول است. DoS حمله های نف وذگران 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.

ب ا سرقت عناصر امنیتی، یک نفوذگر م یتواند رفتار یک کاربر را پایش کند. از این طریق م یتوان به اطلاعات حساس دیگری نیز دست یافت.

ک امپیوترهای 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.

ی ک 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 م یگردد) استفاده کرده و با نفوذ به شبکه ی بی سیم عملاً راهی برای دس تیابی به منابع شبک هی 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.

نگاهی به گذشته شبکه های ادهاک و مقایسه با چالشهای پیش رو

به اوایل دهه ی ۸۰ میلادی باز م یگردد. مانند هر تکنولوژی دیگری، WLAN تکنولوژی و صنعت ،IEEE ۸۰۲,۱۱b پیشرفت شبکه های محلی بی سیم به کندی صورت می پذیرفت. با ارای هی استاندارد که پهنای باند نسبتاً بالایی را برای شبکه های محلی امکا نپذیر می ساخت، استفاده از این تکنولوژی تمامی پروتکل ها و استانداردهای خانواده ی WLAN وسعت بیشتری یافت.

در حال حاضر، مقصود از است. جدول زیر اختصاصات این دسته از استانداردها را به صورت کلی نشان می دهد IEEE ۸۰۲,۱۱

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), infrared (IR)
Frequency Band	2.4GHz (ISM band) and 5GHz
Data Rates	1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a), 54Mbps (11g)
Data and network security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management.
Operating Range	About 150 feet indoors and 1500 feet outdoors
Throughput	Up to 11Mbps (54Mbps planned)
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

جدول ۷ ۱

پیاده سازی شد. این شبکه، به عنوان یک نمونه Motorola اولین شبکه ی محلی ب یسیم تجاری توسط از این شبکه ها، هزینه یی بالا و پهنای باندی پایین را تحمیل می کرد که ابداً مقرون به صرفه نبود. از همان شروع شد. پس از IEEE زمان به بعد، در اوایل دهه ی ۹۰ میلادی، پروژ هی استاندارد ۸۰۲,۱۱ در نهایی شده و IEEE ۸۰۲,۱۱ توسط ۸۰۲,۱۱ b و a نزدیک به ۹ سال کار، در سال ۱۹۹۹ استانداردهای ،GHz۵ با استفاده از فرکانس حامل ،a تولید

محصولات بسیاری بر پایه ی این استانداردها آغاز شد. نوع ۲,۴ ، تا GHz با استفاده از فرکانس حامل ۵۴ b را فراهم می کند.

در حالی که نوع Mbps پهنای باندی تا در مقایسه ۱۱ b پهنای باند را پشتیبانی می کند. با این وجود تعداد کانال های قابل استفاده در نوع Mbps بیش تر است. تعداد این کانال ها، با توجه به کشور مورد نظر، تفاوت می کند. در حالت معمول، a، با نوع ۸۰۲,۱۱ است. b استاندارد WLAN مقصود از ۸۰۲,۱۱ شناخته می شود. این g معرفی شده است که به IEEE استاندارد دیگری نیز به تاز ه گی توسط ۲,۴ عمل می کند ولی با استفاده از روش های نوینی م یتواند GHz استاندارد بر اساس فرکانس حامل ۵۴ بالا ببرد. تولید محصولات بر اساس این استاندارد، که مدت Mbps پهنای باند قابل استفاده را تا زیادی از نهایی شدن و معرفی آن نمی گذرد، بیش از یک سال است که آغاز شده و با توجه سازگار ی آن ۸۰۲,۱۱ ، استفاده از آن در شبکه های بی سیم آرام آرام در حال گسترش است. b با استاندارد

۷ ۸ معماری شبکه های محلی بیسیم

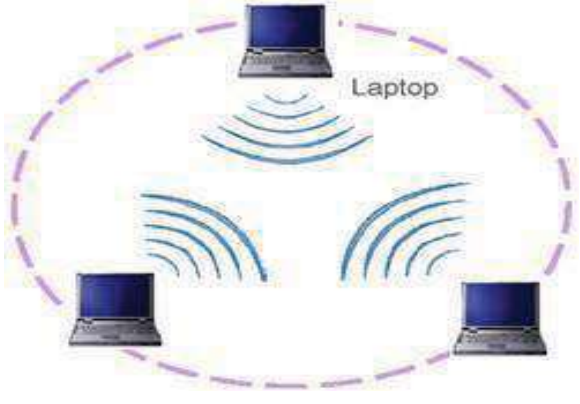
۸۰۲,۱۱ به تجهیزات اجازه م یدهد که به دو روش ارتباط در شبکه برقرار شود. این دو b استاندارد به کار Ad hoc روش عبارت اند از برقراری ارتباط به صورت نقطه به نقطه –همان گونه در شبکه های (AP=Access Point. می رود- و اتصال به شبکه از طریق نقاط تماس یا دسترسی عملاً ،AP است. با نصب یک AP معمار ی معمول در شبکه های محل ی بی سیم بر مبنای استفاده از مرزهای یک سلول مشخص می شود و با روش هایی م یتوان یک سخت افزار مجهز به امکان ارتباط بر پوشش می دهد ۸۰۲,۱۱ AP را میان سلول های مختلف حرکت داد. گستره یی که یک b اساس استاندارد می نامند. مجموعه ی تمامی سلول های یک ساختار کلی شبکه، که (BSS(Basic Service Set راESS می نامند. با استفاده از (ESS(Extended Service Set های شبکه است، را BSS ترکیبی از می توان گستر هی وسیع تری را تحت پوشش شبک هی محل ی بی سیم درآورد. در سمت هریک از سخت افزارها که معمولاً مخدوم هستند، کارت شبکه یی مجهز به یک مودم بی سیم علاوه بر ارتباط با چند کارت شبک هی بی سیم، به بستر AP . ارتباط را برقرار می کند AP قرار دارد که با پرسرعت تر شبک هی 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 میدهد :

شکل ۳ ۷

هما نگونه که گفته شد، اغلب شبک ههای محل ی ب یسیم بر اساس ساختار فوق، که به نوع نیز موسوم است، پیاده سازی می شوند. با این وجود نوع دیگری از شبکه های محلی Ad Infrastructure بی سیم نیز وجود دارند که از همان منطق نقطه به نقطه استفاده می کنند. در این شبکه ها که عموماً نامیده می شوند یک نقط هی مرکز ی برای دسترسی وجود ندارد و سخ تافزارهای همراه – مانند hoc کامپیوترهای کیفی و جیبی یا گوش یهای 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 نیز خواند می شوند. شکل زیر شمایی ساده از IBSS (Independent Basic Service Set) منظور را نشان می دهد :

Ad hoc یک شبکه ی



شکل ۷ ۴

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

۷ ۹ 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 ب یسیم به شبکه ی محلی متصل م یشود. این ایستگاه م یتواند 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 شبک هی محلی استفاده می کنند.

در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به صورت سرخود مجهز هستند و نیازی به اضاف هکردن یک کارت شبک هی بی سیم نیست. است. در صورت نیاز به PCMCIA کارت های شبکه ی بی سیم عموماً برای استفاده در چاک های استفاده از این کارت ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت ها را بر روی نصب می کنند. PCI چا کهای گسترش

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 میگردد.

۷ ۱۰ 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

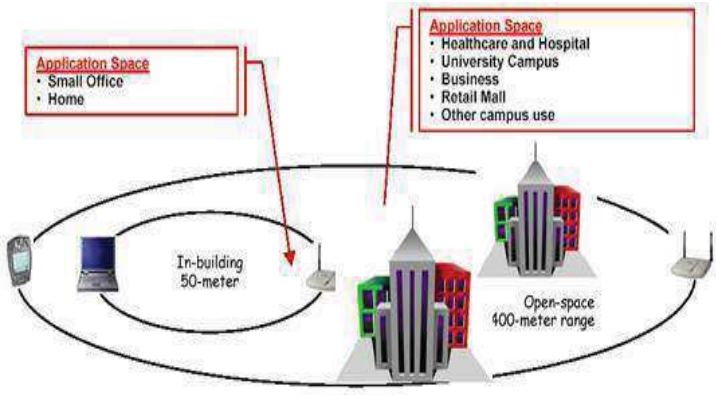
منابع امواج ارسالی و محل قرارگیری فرستنده ها و گیرنده ها

مشخصات فضای قرارگیری و نصب تجهیزات شبک هی بی سیم

قدرت امواج

نوع و مدل آنتن

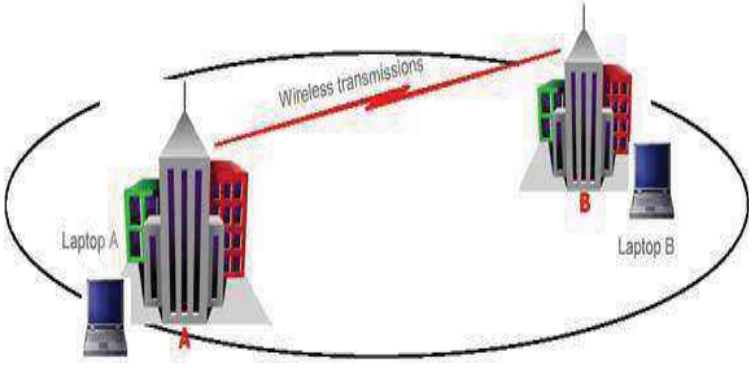
شعاع پوشش از نظر تئوری بین ۲۹ متر (برای فضاهای بسته ی داخلی) و ۴۸۵ متر (برای فضاهای باز) در ۸۰۲,۱۱ متغیر است. با این وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با b استاندارد توجه به گیرنده ها و فرستنده های نسبتاً قدرت مندی که مورد استفاده قرار می گیرند، امکان استفاده از این پروتکل و گیرنده ها و فرستنده های آن، تا چند کیلومتر هم وجود دارد که نمونه های عملی آن فراوا ناند. ۸۰۲,۱۱) ذکر می شود چیزی میان ۵۰ تا b) با این وجود شعاع کلی یی که برای استفاده از این پروتکل ۱۰۰ متر است. این شعاع عمل کرد مقداری ست که برای محل های بسته و ساختمان های چند طبقه نیز معتبر بوده و م یتواند مورد استناد قرار گیرد. شکل زیر مقایسه یی میان بردهای نمونه در کاربردهای مختلف شبکه های بی سیم مبتنی بر پروتکل ۸۰۲,۱۱ را نشان می دهد : b



شکل ۷ ۵

یکی از عملکردهای نقاط دسترسی به عنوان سوییچ های بی سیم، عمل اتصال میان حوزه های بی سیم برای شبکه های Bridge است. ب هعبارت دیگر با استفاده از چند سوییچ بی سیم م یتوان عمل کردی مشابه بی سیم را به دست آورد. اتصال میان نقاط دس ترسی 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 م یکنند 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 ۵۸۰۲,۱۱ b کیلومتر است. البته باید توجه داشت که این فاصله، فاصله یی متوسط بر اساس پروتکل ۸۰۲,۱۱ می توان فواصل بیشتری را نیز ب هدست آورد. a است. برای پروتکل های دیگری چون شکل زیر نمون هیی از ارتباط نقطه به نقطه با استفاده از نقاط دسترسی مناسب را نشان میدهد :



شکل ۷ ۶

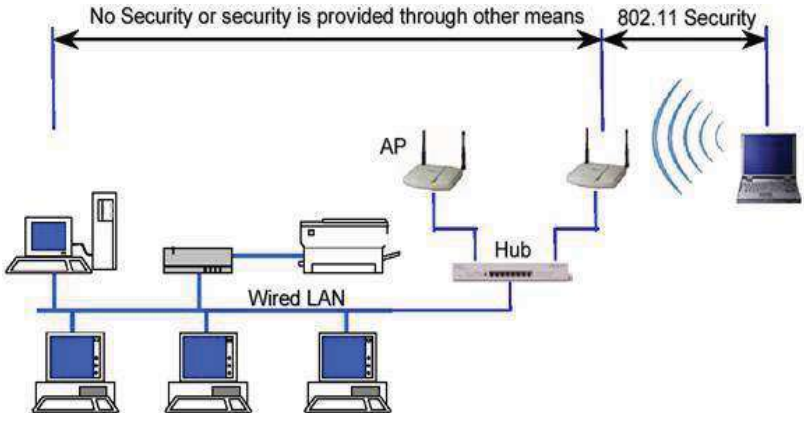
از دیگر استفاده های نقاط دسترسی با برد بالا م یتوان به امکان توسعه ی شعاع پوشش شبکه های بی سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبک هی بی سیم، م یتوان از چند نقطه ی دست رسی بی سیم به صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا م یتوان با

استفاده از یک فرستنده ی دیگر در بالای هریک از ساختمان ها، سطح پوشش شبکه را تا ساختمان های دیگر گسترش داد.

۷ ۱۱ امنیت در شبک ههای 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 تأمین WEP (Wired Equivalent Privacy) می دهد. این سرویس ها اغلب توسط پروتکل 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 در یک شبکه ی بی سیم به معنی استفاده از قابلیت درونی WEP ندارد.

این بدان معنی است که استفاده از 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 ۷ ۷

را نشان می دهد. (WEP شکل بالا محدوده ی عمل کرد استانداردهای امنیتی ۸۰۲,۱۱ (خصوصاً

۷ ۱۲ قابلیتها 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 است. این پروتکل با وجود قابلیت هایی که دارد، نوع استفاده از WEP استاندارد ۸۰۲,۱۱ فراهم می کند 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، در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی WEP ریشه در پیکربندی ناصحیح 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 سخ تافزارهای 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 سیم ی و بی سیم یی ست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

تعریفها:

برای شبکه های محلی بی سیم تعریف میگردد :

- **Authentication توسط سرویس پایه و قابلیت سه IEEE**

ایجاد امکانی برای احراز هویت مخدوم بی سیم است. این عمل که در WEP هدف اصلی اقع 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**

با هدف WEP است. این بعد از سرویس ها و خدمات WEP محرمانه گی هدف دیگرایجاد امنیتی در حدود سطوح شبکه های سیمی طراحی شده است. سیاست این

جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه ی محلی بی سیم WEP بخش از است.

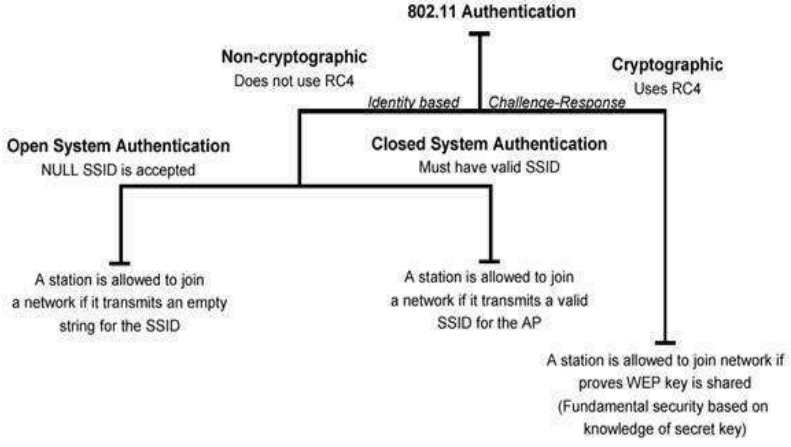
- **Integrity**

طراحی سیاستی است که تضمین کند پیام ها و WEP هدف سوم از سرویس ها و قابلیت های 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. و Auditing وجود دارد نبود سرویس های معمول WEP نکته ی مهمی که در مورد سه سرویس در میان سرویس های ارایه شده توسط این پروتکل است. Authorization

Authentication

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



شکل ۷ ۸

استفاده می کند و روش RC همان گونه که در شکل نیز نشان داده شده است، یک روش از رمزنگاری ۴ دیگر از هیچ تکنیک رمزنگاری یی استفاده نمی کند.

بدون رمزنگاری Authentication

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 پاسخ می دهد.

SSID (Service Set Identifier) حاوی یک خالی نیز برای SSID موسوم است، یک Open System Authentication در روش اول که به 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 نیز NULL Authentication توسط نقطه ی دسترسی نگاه داری م یشود. به همین دلیل به این روش اطلاق می شود.به نقطه ی دسترسی ارسال م یگردد با این تفاوت که اجازه ی SSID در روش دوم از این نوع، بازهم یک ی ارسال شده جزو SSID اتصال به شبکه تنها در صورتی از سوی نقط هی دسترسی صادر م یگردد که Closed System Authentication های

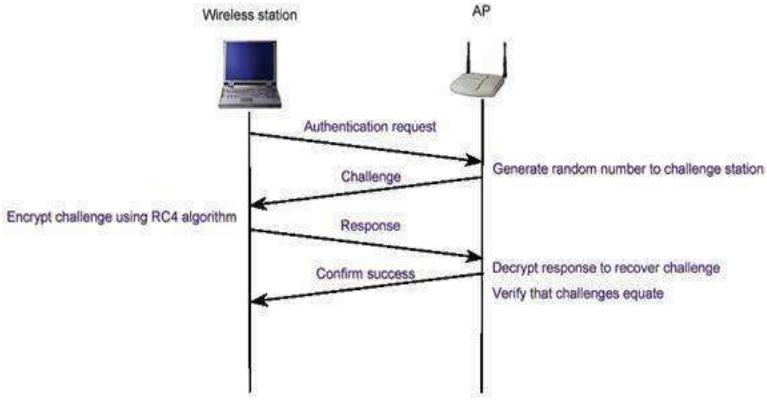
مجاز برای دسترسی به شبکه باشند. این روش به SSID موسوم است.

نکته ای 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 درخواس تکننده هستند.

با این وصف از آن جایی که امنیت در این حالات تضمین شده نیست و معمولاً حملات موفق بسیاری، حتی توسط نفوذگران ک متجربه و مبتدی، به شبکه هایی که بر اساس این روش ها عمل م یکنند، رخ م یدهد، 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!

RC با رمزنگاری ۴ Authentication

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



شکل ۷ ۹

یک رشته تصادفی تولید کرده و آن را به مخدوم می فرستد. (AP) در این روش، نقطه ی دسترسی نیز نامیده می شود) رمز WEP مخدوم این رشته ی تصادفی را با کلیدی از پیش تعیین شده (که کلید می کند و حاصل را برای نقطه ی دسترسی ارسال می کند. نقط هی 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 است.

RC رمزگشایی در این تبادل روش ۴

را روشی کاملاً مطمئن بدانیم، دو خطر در کمین این روش RC در این میان با فرض اینکه رمزنگاری ۴ 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 در خطر هستند. man-in-the-middle یا تبادل اطلاعات حیاتی، قرار دارند با حملاتی تحت عنوان در این دسته از حملات نفوذگر میان دو طرف قرار می گیرد و به گونه یی هریک از دو طرف را گمراه می کند.

Privacy

از آن یاد م یگردد Confidentiality این سرویس که در حوزه های دیگر امنیتی اغلب به عنوان به معنای حفظ امنیت و محرمانه نگا هداشتن اطلاعات کاربر یا گره های در حال تبادل اطلاعات با یکدیگر است. برای رعایت محرمانه گی عموماً از تکنیک های رمزنگاری استفاده م یگردد، 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.

است. RC استفاده م یگردد که برپای هی ۴ WEP ۸۰۲,۱۱ ، از تکنیک های رمزنگاری b در استاندارد یک الگوریتم رمزنگاری متقارن است که در آن یک رشته ی نیمه تصادفی تولید م یگردد و توسط RC۴ آن کل داده رمز می شود.

این رمزنگاری بر روی تمام بست هی اطلاعاتی پیاده می شود. ب هبیان دیگر داده های گرفته تا لایه های بالاتری IP تمامی لایه های بالای اتصال بی سیم نیز توسط این روش رمز می گردند، از از آنجایی

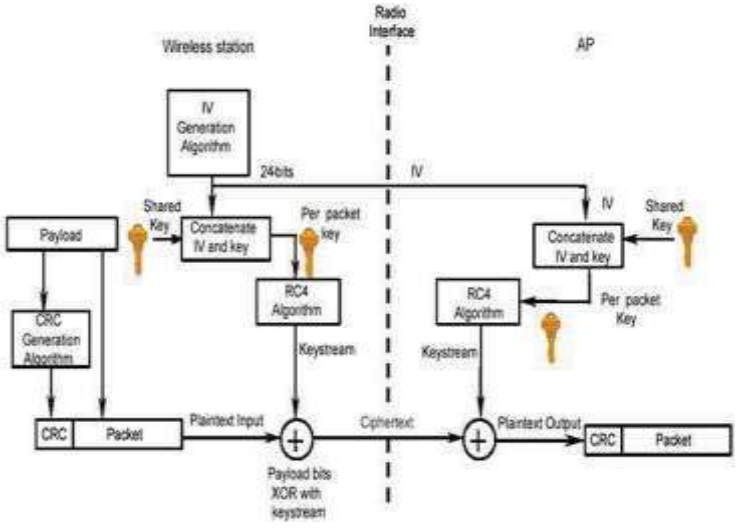
که این روش عملاً اصلی ترین بخش از اعمال سیاست های امنیتی در شبکه های .HTTP مانند ۸۰۲,۱۱ است، معمولاً به کل پروسه ی امن سازی اطلاعات در این b محلی بی سیم مبتنی بر استاندارد گفته می شود. WEP استاندارد ب هاختصار مخفف)IV اندازه هایی از ۴۰ بیت تا ۱۰۴ بیت م یتوانند داشته باشند. این کلیدها با WEP کلیدهای را تشکیل RC یا بردار اولیه) ۲۴ بیتی ترکیب شده و یک کلید ۱۲۸ بیتی ۴ Initialization Vector می دهند.

طبیعتاً هرچه اندازه ی کلید بزرگ تر باشد امنیت اطلاعات بالاتر است. تحقیقات نشان م یدهد که را برای شکستن brute-force استفاده از کلیدهایی با اندازه ی ۸۰ بیت یا بالاتر عملاً استفاده از تکنیک رمز غیرممکن می کند. به عبارت دیگر تعداد کلیدهای ممکن برای اندازه ی ۸۰ بیت (که تعدد آ نها از مرتب هی 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، در مقابل حملات دیگری، غیر از استفاده از روش WEP این ست که

روش تأمین محرمانه گی توسط نیز آسیب پذیر است و این آسیب پذیری ارتباطی به انداز هی کلید استفاده شده ندارد. brute-force، برای تضمین محرمانه گی در شکل زیر نمایش داده شده است:

نمایی از روش استفاده شده توسط WEP



شکل ۷ ۱۰

Integrity

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

۸۰۲,۱۱ نیز سرویس و روشی استفاده می شود که توسط آن امکان تغییر اطلاعات در b در استاندارد حال تبادل میان مخدوم های بی

سیم و نقاط دست رسی کم می شود. روش مورد نظر استفاده از یک کد قبل از رمزشدن بسته CRC- است.

همان طور که در شکل قبل نیز نشان داده شده است، یک ۳۲ CRC داده های رمزگشایی شده مجدداً محاسبه شده CRC، تولید می شود. در سمت گیرنده، پس از رمزگشایی به معنای تغییر CRC نوشته شده در بسته مقایسه م یگردد که هرگونه اختلاف میان دو CRC و با مستقل ،RC محتویات بسته در حین تبادل است.

متأسفانه این روش نیز مانند روش رمزنگاری توسط ۴ از اندازه ی کلید امنیتی مورد استفاده، در مقابل برخی از حملات شناخته شده آسیب پذیر است. ۸۰۲,۱۱ هیچ مکانیزمی برای مدیریت کلیدهای امنیتی ندارد و عملاً تمامی عملیاتی b متأسفانه استاندارد که برای حفظ امنیت کلیدها انجام می گیرد باید توسط کسانی که شبک هی بی سیم را نصب میکنند 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 انجا مشده 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 م یدهد. حتا با فرض تلاش برای جلوگیری از ر خداد چنین سهل انگاری هایی، زمانی که تعداد مخدوم های شبکه از حدی می گذرد عملاً کنترل کردن این تعداد بالا بسیار دشوار شده و گ هگاه خطاهایی در گوشه و کنار این شبک هی نسبتاً بزرگ رخ می دهد که همان باعث رخنه در کل شبکه می شود.

۱۳ ۷ WEP ضعفهای اولیه امنیتی

استوار است. WEP همان گونه که گفته شد، عملاً پایه ی امنیت در استاندارد ۸۰۲,۱۱ بر اساس پروتکل استفاده RC در حالت استاندارد بر اساس کلیدهای ۴۰ بیتی برای رمزنگاری توسط الگوریتم ۴ WEP را با کلیدهایی با تعداد WEP می شود، هرچند که برخی از تولیدکننده گان نگارش های خاصی از بیت های بیش تر پیاده سازی کرد هاند.

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 آ نجاکه 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 انداز هی 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 اولی هی این پروتکل است :

۱ WEP .استفاده از کلیدهای ثابت

یکی از ابتدایی ترین ضعف ها که عموماً در بسیاری از شبک ههای محلی ب یسیم 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 ایستگا ههای کاری عملاً استفاده از تمامی این ایستگاه ها ناامن است. از سوی دیگر با توجه به مشابه بودن کلید، در هر لحظه کانا لهای ارتباطی زیادی توسط یک حمله نفوذپذیر هستند.

۲. Initialization Vector (IV)

این بردار که یک فیلد ۲۴ بیتی است در قسمت قبل معرفی شده است. این بردار به صورت متنی ساده تولید IV فرستاده می شود. از آن جایی که کلیدی که برای رمزنگاری مورد استفاده قرار می گیرد بر اساس عملاً نشان دهنده ی احتمال تکرار آن و در نتیجه احتمال تولید کلیدهای مشابه IV می شود، محدوده ی کوتاه باشد در مدت زمان کمی م یتوان به کلیدهای مشابه IV است. به عبارت دیگر در صورتی که دست یافت.

این ضعف در شبکه های شلوغ به مشکلی حاد مبدل می شود. خصوصاً اگر از کارت شبکه ی استفاده شده های ثابت استفاده می کنند و بسیاری از کارت های IV مطمئن نباشیم. بسیاری از کارت های شبکه از های مشابه دارند. این خطر به همراه ترافیک بالا در یک شبک هی IV شبک هی یک تولید کنند هی واحد در مدت زمانی کوتاه را بالاتر می برد و در نتیجه کافی ست نفوذگر در مدت IV شلوغ احتمال تکرار های بسته های اطلاعاتی را ذخیره کند. با IV زمانی معین به ثبت داده های رمز شده ی شبکه بپردازد و های استفاده شده در یک شبکه ی شلوغ احتمال بالایی برای نفوذ به آن شبکه در مدت IV ایجاد بانکی از زمانی نه چندان طولانی وجود خواهد داشت.

۳. ضعف در الگوریتم

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

عنوان ضعفی برای این پروتکل محسوب میگردد. رمز نشده CRC ۴.استفاده از رمز نمی شود. لذا بسته های تأییدی که از سوی نقاط دست رسی بی سیم CRC کد ،WEP در پروتکل رمزنشده ارسال م یگردد و تنها در صورتی که نقط هی CRC ب هسوی گیرنده ارسال م یشود بر اساس یک دسترسی از صحت بسته اطمینان حاصل کند تأیید آن را می فرستد. این ضعف این امکان را فراهم می کند را نیز به دلیل این که رمز نشده CRC که نفوذگر برای رمزگشایی یک بسته، محتوای آن را تغییر دهد و 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.

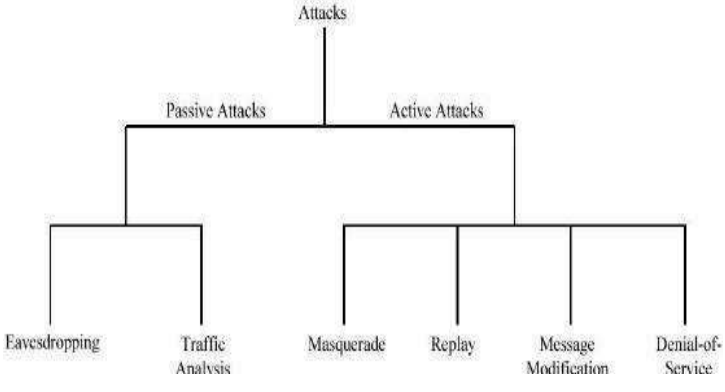
هستند. نکته های WEP ضعف های بیان شده از مهم ترین ضعف های شبکه های بی سیم مبتنی بر پروتکل که در مورد ضعف های فوق باید به آن اشاره کرد این است که در میان این ضعف ها تنها یکی از آن ها (مشکل امنیتی سوم) به ضعف در الگوریتم رمزنگاری باز م یگردد و لذا با تغییر الگوریتم رمزنگاری تنها این ضعف است که برطرف می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

Security Issue / Vulnerability	Remarks
1. Security features in vendor products are frequently not enabled.	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. IVs are short (or static).	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. Cryptographic keys are short.	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
4. Cryptographic keys are shared.	Keys that are shared can compromise a system. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. Cryptographic keys cannot be updated automatically and frequently.	Cryptographic keys should be changed often to prevent brute-force attacks.
6. RC4 has a weak key schedule and is inappropriately used in WEP.	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 keystream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. Packet integrity is poor.	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8. No user authentication occurs.	Only the device is authenticated. A device that is stolen can access the network.
9. Authentication is not enabled; only simple SSID identification occurs.	Identity-based systems are highly vulnerable particularly in a wireless system.
10. Device authentication is simple shared-key challenge-response.	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.

جدول ۲ ۷

۷ ۱۴ 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 می پردازیم. IEEE ۸۰۲,۱۱x موجود در استفاده از شبکه های محلی بی سیم بر اساس استاندارد شکل زیر نمایی از دسته بندی حملات مورد نظر را نشان می دهد :



شکل ۷ ۱۱

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

۷ ۱۴ ۱ 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.

۷ ۱۴ ۲ حملات فعال

در این نوع حملات، برخلاف حملات غیرفعال، نفوذگر اطلاعات مورد نظر را، که از منابع به دست میآید، 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.

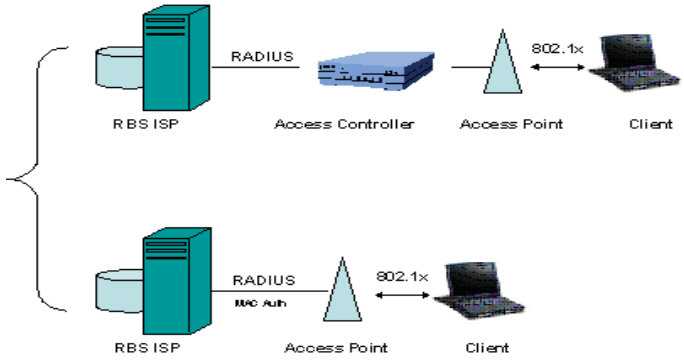
تغییر پیام

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. (Denial-of-Service) DoS حمله های 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 یی ست که مشکلاتی برای نفوذگر برای دسترسی 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. تمامی ریسک هایی که در شبکه های محلی، خصوصاً انواع بی سیم، وجود دارد ناشی از یکی از خطرات فوق است.

۷ ۱۵ شش مشکل امنیتی مهم شبکه های بی سیم ۸۰۲,۱۱

است. همچنانکه ۸۰۲,۱۱ به ترقی خود « اترنت بی سیم » موفقیت حیرت انگیز ۸۰۲,۱۱ به علت توسعه ادامه می دهد، تفاوت هایش با اترنت بیشتر مشخص می شود. بیشتر این تفاوت ها به دلیل نا آشنایی نسبی بسیاری از مدیران شبکه با لایه فیزیکی فرکانس رادیویی است. در حالیکه همه مدیران شبکه باید درک پایه ای از لینک رادیویی داشته باشند، تعدادی از ابزارها برای کمک به آنها به خدمت گرفته می شوند. آنالایزرهای (تحلیل کننده) شبکه های بی سیم برای مدت ها ابزاری لازم برای مهندسان شبکه در اشکال زدایی و تحلیل پروتکل بوده اند. بسیاری از آنالایزرها بعضی کارکردهای امنیتی را نیز اضافه کرده اند که به آنها اجازه کار با عملکردهای بازرسی امنیتی را نیز می دهد. یک آنالایزر از اولین خریدهایی است که یک مدیر شبکه باید انجام دهد. آنالایزرها علاوه بر عملکردهای سنتی تحلیل پروتکل و ابزار تشخیص عیب، می توانند برای تشخیص بسیاری از نگرانی های امنیتی که استفاده از شبکه بی سیم را کند می کنند، استفاده شوند.



شکل ۷ ۱۲

مسأله شماره ۱: دسترسی آسان

های بی سیم به آسانی پیدا می شوند. برای فعال کردن کلاینت ها در هنگام یافتن آنها، شبکه ها LAN با پارامتر های شبکه را ارسال کنند. البته، اطلاعات مورد نیاز برای پیوستن به Beacon باید فریم های توسط Beacon یک شبکه، اطلاعاتی است که برای اقدام به یک حمله روی شبکه نیاز است. فریم های هیچ فانکشن اختصاصی پردازش نمی شوند و این به این معنی است که شبکه ۸۰۲,۱۱ شما و پارامترهایش برای هر شخصی با یک کارت ۸۰۲,۱۱ قابل استفاده است. نفوذگران با آنتن های قوی می توانند شبکه ها را در مسیرها یا ساختمان های نزدیک بیابند و ممکن است اقدام به انجام حملاتی

کنند حتی بدون به امکانات شما دسترسی فیزیکی اینکه داشته باشند.

شکل ۷ ۱۳

مسأله شماره ۲: نقاط دسترسی نامطلوب

بی سیم امری منفک از راه اندازی آسان آن نیست. این دو LAN دسترسی آسان به شبکه های خصوصیت در هنگام ترکیب شدن با یکدیگر می توانند برای مدیران شبکه و مسوولان امنیتی ایجاد دردسر کنند. هر کاربر می تواند به فروشگاه کامپیوتر نزدیک خود برود، یک نقطه دسترسی! بخرد و بدون کسب اجازه ای خاص به کل شبکه متصل شود.

شکل ۷ ۱۴

بسیاری از نقاط دسترسی با اختیارات مدیران بی سیمشان را بدون صدور اجازه از LAN میانی عرضه می شوند و لذا دپارتمان ها ممکن است بتوانند بکارگرفته « نامطلوب » مرکزی در معرض عموم قرار دهند. این دسترسی به اصطلاح IT یک سازمان شده توسط کاربران ، خطرات امنیتی بزرگی را مطرح می کند.

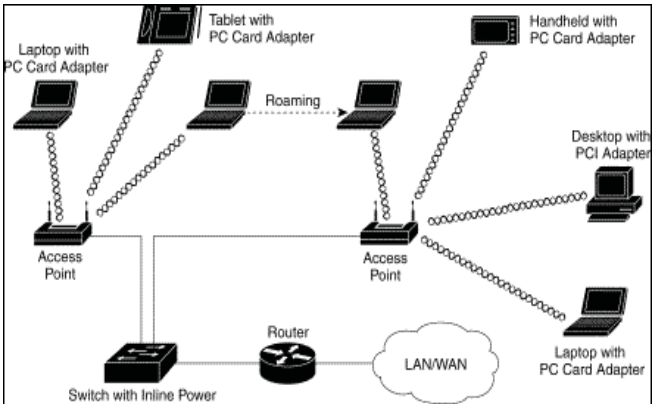
کاربران در زمینه امنیتی خبره نیستند و های بی سیم آگاه نباشند. ثبت بسیاری از ورودها به LAN ممکن است از خطرات ایجاد شده توسط شبکه نشان از آن دارد که ویژگی های امنیتی فعال نیستند و بخش بزرگی از آنها تغییراتی نسبت به پیکربندی پیش فرض نداشته اند و با همان پیکربندی راه اندازی شده اند.

راه حل شماره ۲ : رسیدگی های منظم به سایت

مانند هر تکنولوژی دیگر شبکه، شبکه های بی سیم به مراقبت از سوی مدیران امنیتی نیاز دارند. بسیاری از این تکنولوژی ها به دلیل سهولت استفاده مورد بهره برداری نادرست قرار می گیرند، لذا آموختن نحوه یافتن شبکه های امن نشده از اهمیت بالایی برخوردار است. روش بدیهی یافتن این شبکه ها انجام همان کاری است که نفوذگران انجام می دهند: استفاده از یک آنتنو جستجوی آنها به این منظور که بتوانید قبل از نفوذگران این شبکه ها را پیدا کنید. نظارت های فیزیکی سایت باید به صورت مرتب و در حد امکان انجام گیرد. اگرچه هرچه نظارت ها سریع تر انجام گیرد، امکان کشف استفاده های غیرمجاز بیشتر است، اما زمان زیادی که کارمندان مسوول این امر باید صرفکنند، کشف تمامی استفاده های غیرمجاز را بجز برای محیط های بسیار حساس، غیرقابل توجیه می کند.

یک راهکار برای عدم امکان حضور دائم می تواند انتخاب ابزاری در اندازه دستی باشد. این عمل می تواند استفاده تکنسین ها از اسکنرهای دستی در هنگام انجام امور پشتیبانی کاربران، برای کشف شبکه های غیرمجاز باشد.

۸۰۲,۱۱ به عنوان یک محصول a یکی از بزرگترین تغییرات در بازار ۸۰۲,۱۱ در سال های اخیر ظهور ۸۰۲,۱۱ را بوجود a تجاری قابل دوام بود. این موفقیت نیاز به ارائه ابزارهایی برای مدیران شبکه های پیشینیان خود استفاده می کند، بنابراین بیشتر آنچه MAC ۸۰۲,۱۱ از همان a ، آورد. خوشبختانه مدیران راجع به ۸۰۲,۱۱ و تحلیل کننده ها می دانند، بدرد می خورد. مدیران شبکه باید دنبال محصولی ۸۰۲,۱۱ را بصورت یکجا و ترجیحاً به صورت ۸۰۲,۱۱ b و a سازگار باشند که هر دو استاندارد ۸۰۲,۱۱ و کارت های ساخته شده با آنها به a/b همزمان پشتیبانی کند. چیپ ست های دوباندی آنالایزرها اجازه می دهد که روی هر دو باند بدون تغییرات سخت افزاری کار کنند، و این بدین معنی است که مدیران شبکه نیاز به خرید و آموزش فقط یک چارچوپ پشتیبانی شده برای هر دو استاندارد ۸۰۲,۱۱ ادامه یابد، تا جایی که سازندگان آنالایزرها کارت های g دارند. این روال باید تا ۸۰۲,۱۱ را مورد پذیرش قرار دهند. a/b/g



شکل ۷ ۱۵

بسیاری از ابزارها می توانند برای انجام امور رسیدگی به سایت و ردیابی نقاط دسترسی نامطلوب استفاده شوند، اما مدیران شبکه باید از نیاز به همگامی با آخرین تکنیک های استفاده شده در این بازی موش و گربه! آگاه باشند. نقاط دسترسی می توانند در هر باند فرکانسی تعریف شده در ۸۰۲,۱۱ بکارگرفته شوند، بنابراین مهم است که تمام ابزارهای مورد استفاده در بررسی های سایت بتوانند کل محدوده ۸۰۲,۱۱ را انتخاب کرده اید، آنالایزر استفاده شده b فرکانسی را پویش کنند. حتی اگر شما استفاده از ۸۰۲,۱۱ را نیز پویش کند تا در طول a برای کار نظارت بر سایت، باید بتواند

همزمان نقاط دسترسی یک بررسی کامل نیازی به جایگزین های سخت افزاری و نرم افزاری نباشد.

b۸۰۲,۱۱ بعضی نقاط دسترسی نامطلوب سعی دارند کانالهایی را به صورت غیرقانونی روی کانال هایتنها اجازه استفاده از کانال های FCC به کار بگیرند که برای ارسال استفاده نمی شوند. برای مثال قوانین ۸۰۲,۱۱ را می دهد. کانال های ۱۲ تا ۱۴ جزء مشخصات آن تعریف شده اند اما فقط ۱ b تا ۱۱ از برای استفاده در اروپا و ژاپن کاربرد دارند. به هرحال، بعضی کاربران ممکن است از نقطه دسترسی کانال های اروپایی یا ژاپنی استفاده کنند، به این امید که رسیدگی یک سایت متمرکز روی کانال های مطابق با از کانال های فرکانس بالاتر چشم پوشی کند.

این قضیه مخصوصاً برای ردیابی ابزارهایی اهمیت FCC دارد که بیرون باند فرکانسی مجاز بکارگرفته شده اند تا از اعمال اجرایی اتخاذ شده توسط نمایندگی ابزار ارزشمندی هستند زیرا (Passive Analyzers) های مجاز برحذر باشند. آنالایزرهای غیرفعال استفاده های غیرمجاز را تشخیص می دهند، اما چون توانی ارسال نمی کنند استفاده از آنها قانونی است. مدیران شبکه همواره تحت فشار زمانی

هستند، و به روش آسانی برای یافتن نقاط دسترسی نامطلوب و در عین حال چشم پوشی از نقاط دسترسی مجاز نیاز دارند.

موتورهای جستجوی خبره به مدیران اجازه می دهند که لیستی از نقاط دسترسی مجاز را پیکربندی کنند.

هر نقطه دسترسی غیرمجاز باعث تولید علامت هشدار دهنده ای می شود. در پاسخ به علامت هشدار دهنده، مدیران شبکه می توانند از ابزار دیگری برای پیدا کردن نقطه دسترسی براساس مقیاس های قدرت سیگنال استفاده کنند. اگرچه این ابزارها ممکن است خیلی دقیق نباشند، ولی برای محدود کردن محوطه جستجوی نقطه دسترسی نامطلوب به اندازه کافی مناسب هستند.

مسأله شماره ۳: استفاده غیرمجاز از سرویس

چندین شرکت مرتبط با شبکه های بی سیم نتایجی منتشر کرده اند که نشان می دهد اکثر نقاط دسترسی با تنها تغییرات مختصری

نسبت به پیکربندی اولیه برای سرویس ارائه می گردند. تقریباً تمام نقاط WEP (Wired Equivalent ، دسترسی که با پیکربندی پیش فرض مشغول به ارائه سرویس هستند را فعال نکرده اند یا یک کلید پیش فرض دارند که توسط تمام تولیدکنند گان محصولات (Privacy دسترسی به شبکه به راحتی میسر است. دو مشکل به دلیل این دسترسی WEP استفاده می شوند. بدون باز می تواند بروز کند: کاربران غیرمجاز لزوماً از مفاد ارائه سرویس تبعیت نمی کنند، و نیز ممکن است تان لغو شود. ISP تنها توسط یک اسپم ساز اتصال شما به

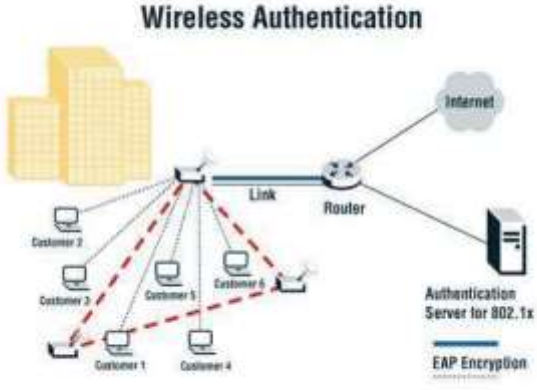
راه حل شماره ۳ : طراحی و نظارت برای تأیید هویت محکم

راه مقابله مشخص با استفاده غیرمجاز، جلوگیری از دسترسی کاربران غیرمجاز به شبکه است. تأیید هویت محکم و محافظت شده توسط رمزنگاری یک پیش شرط برای صدور اجازه است، زیرا امتیازات که برای حفاظت از انتقال در لینک رادیویی VPN دسترسی برپایه هویت کاربر قرار دارند.

روش های به کارگرفته می شوند، تأیید هویت محکمی را ارائه می کنند. تخمین مخاطرات انجام شده توسط سازمان ۸۰۲,۱ باید توسط روش های تأیید هویت برپایه رمزنگاری تضمین x ها نشان می دهد که دسترسی به TTLS، TLS (Layer Security Transport) شود. از جمله این روش ها می توان به اشاره Protected Extensible Authentication Protocol)) PEAP یا (Tunneled TLS) کرد. هنگامی که یک شبکه با موفقیت راه اندازی می شود، تضمین تبعیت از سیاست های تایید هویت و اعطای امتیاز مبتنی بر آن حیاتی است. همانند مسأله نقاط دسترسی نامطلوب، در این راه حل نیز نظارت های منظمی بر تجهیزات شبکه بی سیم باید انجام شود تا استفاده از مکانیسم های تأیید هویت و پیکربندی مناسب ابزارهای شبکه تضمین شود. هر ابزار نظارت جامع باید نقاط دسترسی را در هر دو ۵) تشخیص دهد و (GHz U-NII ۲,۴ a) و ۸۰۲,۱۱ GHz ISM باند) b باند فرکانسی ۸۰۲,۱۱ پارامترهای عملیاتی مرتبط با امنیت را نیز مشخص کند. اگر یک ایستگاه غیرمجاز متصل به شبکه کشف شود، یک رسیور دستی می تواند برای ردیابی موقعیت فیزیکی آن استفاده شود.

آنالایزرها نیز می توانند برای تأیید پیکربندی بسیاری از پارامترهای نقاط دسترسی استفاده گردند و هنگامی که نقاط دسترسی آسیب

پذیری های امنیتی را نمایان می کنند، علائم هشدار دهنده صوتی تولید کنند.



شکل ۷ ۱۶

مسأله شماره ۴ : محدودیت های سرویس و کارایی

۸۰۲,۱۱ سرعت انتقالی برابر با b های بی سیم ظرفیت های ارسال محدودی دارند. شبکه های LAN ۵۴ دارند. ۸۰۲,۱۱ Mbps نرخ

انتقال اطلاعاتی تا ۱۱ a و شبکه های برپایه تکنولوژی جدید Mbps تقریباً تا نیمی از ظرفیت اسمی می رسد.

نقاط ،MAC البته ماحصل مؤثر واقعی، به دلیل بالاسری لایه دسترسی کنونی این ظرفیت محدود را بین تمام کاربران مربوط به یک نقطه دسترسی قسمت می کنند.

تصور اینکه چگونه برنامه های محلی احتمالاً چنین ظرفیت محدودی را اشغال می کنند یا چگونه یک روی این منابع محدود طرح ریزی کند، سخت (DoS) نفوذگر ممکن است یک حمله انکار سرویس نیست. ظرفیت رادیویی می تواند به چندین روش اشغال شود. ممکن است توسط ترافیکی که از سمت شبکه ping باسیم با نرخی بزرگتر از توانایی کانال رادیویی می آید، مواجه شود.

اگر یک حمله کننده یک را از یک بخش اترنت سریع بفرستد، می تواند به راحتی ظرفیت یک نقطه دسترسی را اشغال flood امکان اشغال چندین نقطه دسترسی متصل به هم وجود دارد. broadcast کند. با استفاده از آدرس های حمله کننده همچنین می تواند ترافیک را به شبکه رادیویی بدون اتصال به یک نقطه دسترسی بی سیم

تزریق کند. ۸۰۲,۱۱ طوری طراحی شده است که به چندین شبکه اجازه به اشتراک گذاری یک فضا و کانال رادیویی را می دهد.

حمله کنندگانی که می خواهند شبکه بی سیم را از کار بیاندازند، می توانند ترافیک خود را روی یک کانال رادیویی ارسال کنند و شبکه مقصد ترافیک جدید را با استفاده از تا آنجا که می تواند می پذیرد. مهاجمان بداندیش که فریم های ناسالم می CSMA/CA مکانیسم فرستند نیز ظرفیت محدود را پر می کنند.

همچنین ممکن است مهاجمان تکنیک های تولید پارازیت رادیویی را انتخاب کنند و اقدام به ارسال اطلاعات با نویز بالا به شبکه های بی سیم مقصد کنند. بارهای بزرگ ترافیک الزاماً با نیات بدخواهانه تولید نمی شوند. انتقال فایل های بزرگ یا سیستم ترکیبی ممکن است مقادیر بالایی از دیتا روی شبکه ارسال کنند. اگر تعداد کافی کاربر client/server شروع به گرفتن اندازه های بزرگی از دیتا از طریق یک نقطه دسترسی کنند، شبکه شبیه سازی دسترسی را آغاز می کند dial-up

راه حل شماره ۴ : دیدبانی شبکه

نشان یابی مسائل کارایی با دیدبانی و کشف آنها آغاز می شود. مدیران شبکه بسیاری از کانال ها را برای (SNMP (imple کسب اطلاعات در مورد کارایی در اختیار دارند: از ابزارهای تکنیکی خاص مانند گرفته تا ابزارهای بالقوه قوی غیرفنی مانند گزارش های Network Management Protocol کارایی کاربران. یکی از مسائل عمده بسیاری از ابزارهای تکنیکی، فقدان جزئیات مورد نیاز برای درک بسیاری از شکایت های کاربران در مورد کارایی است.

آنالایزرهای شبکه های بی سیم می توانند با گزارش دهی روی کیفیت سیگنال و سلامت شبکه در مکان کنونی خود، کمک باارزشی برای مدیر شبکه باشند. مقادیر بالای ارسال های سرعت پایین می تواند بیانگر تداخل خارجی یا دور بودن یک ایستگاه از نقطه دسترسی باشد. توانایی نشان دادن سرعت های لحظه ای روی هر کانال، یک تصویر بصری قوی از ظرفیت باقی مانده روی کانال می دهد که به سادگی اشغال کامل یک کانال را نشان می دهد.

ترافیک مفرط روی نقطه دسترسی می تواند با تقسیم ناحیه پوشش نقطه دسترسی به نواحی پوشش کوچک تر یا با اعمال روش شکل

دهی ترافیک در تلاقی شبکه بی سیم با شبکه اصلی تعیین شود. در حالیکه هیچ راه حل فنی برای آسیب پذیری های ناشی از فقدان تأیید هویت فریم های کنترل و مدیریت وجود ندارد، مدیران می توانند برای مواجهه با آنها گام هایی بردارند.

آنالایزرها اغلب نزدیک محل های دردسرساز استفاده می شوند تا به تشخیص عیب کمک کنند و به صورت ایده آل برای کار گذاشته می شوند. مهاجمان می توانند با تغییر دادن فریم های DoS مشاهده بسیاری از حملات ۸۰۲,۱۱ با استفاده از یکی از چندین روش معمول واسط های برنامه نویسی ۸۰۲,۱۱ موجود، از شبکه سوءاستفاده کنند. حتی یک محقق امنیتی ابزاری نوشته است که پیام های قطع اتصال فرستاده شده توسط نقاط دسترسی به کلاینت ها را جعل می کند.

بدون تأیید هویت پیام های قطع اتصال بر اساس رمزنگاری، کلاینت ها به این پیام های جعلی عمل می کنند و اتصال خود را از شبکه قطع می کنند. تا زمانی که تأیید هویت به صورت یک فریم رمزشده استاندارد درنیاید، تنها مقابله علیه حملات جعل پیام، مکان یابی حمله کننده و اعمال عکس العمل مناسب است.

مسأله شماره ۵: حملات سطح بالاتر

هنگامی که یک نفوذگر به یک شبکه دسترسی پیدا می کند، می تواند از آنجا به عنوان نقطه ای برای انجام حملات به سایر سیستم ها استفاده کند. بسیاری از شبکه ها یک پوسته بیرونی سخت دارند که از ابزار امنیت پیرامونی تشکیل شده، به دقت پیکربندی شده و مرتب دیده بانی می شوند. اگرچه درون های بی سیم می توانند به سرعت با اتصال به شبکه LAN . پوسته یک مرکز آسیب پذیر نرم قرار دارد های اصلی آسیب پذیر مورد استفاده قرار گیرند، اما به این ترتیب شبکه در معرض حمله قرار می گیرد. بسته به امنیت پیرامون، ممکن است سایر شبکه ها را نیز در معرض حمله قرار دهد، و می توان شرط بست که اگر از شبکه شما به عنوان نقطه ای برای حمله به سایر شبکه ها استفاده شود، حسن شهرت خود را از دست خواهید داد.

بی سیم محافظت کنید LAN راه حل شماره ۵ : هسته را از به دلیل استعداد شبکه های بی سیم برای حمله، باید به عنوان شبکه های غیرقابل اعتماد مورد استفاده در اتاق های آموزش یا سالن ها ارائه می guest قرار بگیرند. بسیاری از شرکت ها درگاه های دسترسی

کنند. شبکه های بی سیم به دلیل احتمال دسترسی توسط کاربران غیرقابل اعتماد می توانند به عنوان درگا تصور شوند.

شبکه بی سیم را بیرون منطقه پیرامون امنیتی شرکت قرار دهید و از guest ه های دسترسی بی سیم و شبکه مرکزی LAN تکنولوژی کنترل دسترسی قوی و ثابت شده مانند یک فایروال بین تثبیت شده ارائه کنید. VPN استفاده کنید، و سپس دسترسی به شبکه مرکزی را از طریق روش های

مسأله شماره ۶: تحلیل ترافیک و استراق سمع

ترافیک را مشاهده می کنند، (۸۰۲,۱۱ (passive هیچ محافظتی علیه حملاتی که بصورت غیرفعال ارائه نمی کند. خطر اصلی این است که ۸۰۲,۱۱ روشی برای تامین امنیت دیتای در حال انتقال و هستند و برای «in the clear » فریم ها همیشه Header . جلوگیری از استراق سمع فراهم نمی کند هرکس با در اختیار داشتن یک آنالایزر شبکه بی سیم قابل مشاهده هستند. فرض بر این بوده است که ارائه گردد.

بخش WEP (Wired (quivalent Privacy جلوگیری از استراق سمع در مشخصات نوشته شده است که فقط از اتصال ابتدایی بین شبکه و فریم های WEP زیادی در مورد رخنه های رمزنگاری و تصدیق هویت WEP دیتای کاربر محافظت می کند. فریم های مدیریت و کنترل توسط نمی شوند و به این ترتیب آزادی عمل زیادی به یک نفوذگر می دهد تا با ارسال فریم های جعلی و AirSnort مانند crack نسبت به ابزارهای WEP اختلال به وجود آورد. پیاده سازی های اولیه آسیب پذیر هستند، اما آخرین نسخه ها تمام حملات شناخته شده را حذف می کنند.

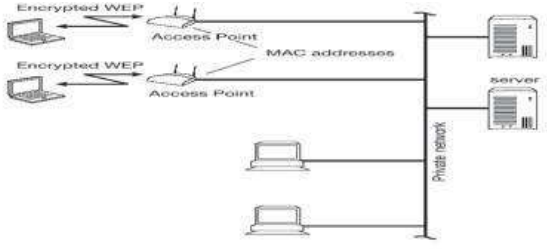
به WEPcrack یک گام فراتر می روند و از پروتکل WEP عنوان یک اقدام احتیاطی فوق العاده، آخرین محصولات در هر پانزده دقیقه استفاده می کنند. حتی مشغول ترین WEP های مدیریت کلید برای تعویض کلید بی سیم آنقدر دیتا تولید نمی کند که بتوان در پانزده دقیقه کلید را بازیافت کرد. LAN

راه حل شماره ۶ : انجام تحلیل خطر

تنها WEP هنگام بحث در مورد خطر استراق سمع، تصمیم کلیدی برقراری توازن بین خطر استفاده از و پیچیدگی بکارگیری راه حل اثبات شده دیگری است. در وضعیت فعلی برای امنیت لایه لینک، استفاده تا حد زیادی مورد کنکاش قرار WEP . با کلیدهای طولانی و تولیدکلید پویا توصیه می شود WEP از گرفته است و پروتکل های امنیتی علیه تمام حملات شناخته شده تقویت شده اند.

یک قسمت بسیار مهم در این تقویت، زمان کم تولید مجدد کلید است که باعث می شود نفوذگر نتواند در مورد قبل از جایگزین شدن، اطلاعات عمده ای کسب کند. ، WEP خصوصیات کلید را انتخاب کنید، باید شبکه بی سیم خود را نظارت کنید تا مطمئن شوید که WEP اگر شما استفاده از نیست. یک موتور آنالیز قوی به طور خودکار تمام ترافیک دریافت شده را AirSnort مستعد حمله بررسی می کند. WEP تحلیل می کند و ضعف های شناخته شده را در فریم های محافظت شده توسط آنها فعال نیست نشان گذاری WEP همچنین ممکن است بتواند نقاط دسترسی و ایستگاه هایی را که کند تا بعداً توسط مدیران شبکه بررسی شوند.

زمان کوتاه تولید مجدد کلید ابزار بسیار مهمی است که در کاهش خطرات مربوط به شبکه های بی سیم استفاده می شود. بعنوان بخشی از نظارت سایت، مدیران شبکه می توانند از آنالایزرهای قوی استفاده کنند تا مطمئن شوند که سیاست های تولید کلید مجدد توسط تجهیزات مربوطه پیاده سازی شده اند. WEP



شکل ۷ ۱۷

برای نیاز WEP بی سیم شما برای انتقال دیتای حساس استفاده می شود، ممکن است LAN اگر از برای انتقال دیتا به صورت IPSec و SSH،SSL شما کافی نباشد.

روش های رمزنگاری قوی مانند امن روی کانال های عمومی طراحی شده اند و برای سال ها مقاومت آنها در برابر حملات ثابت شده است، و یقیناً سطوح بالاتری از امنیت را ارائه می کنند. نمایشگرهای وضعیت نقاط دسترسی می توانند استفاده می کنند، تمایز قائل شوند تا مدیران شبکه VPN ۸۰۲,۱ و WEP،x بین نقاط دسترسی که از بتوانند بررسی کنند که آیا در آنها از سیاست های رمزنگاری قوی تبعیت می شود یا خیر. قوی، ممکن است که تمایل به استفاده از تصدیق هویت قوی VPN علاوه بر استفاده از پروتکل های ۸۰۲,۱ ، نتایج ۸۰۲,۱ x داشته باشید. بعضی جزئیات آنالیز وضعیت تصدیق x کاربر با استفاده از ۸۰۲,۱ ارائه می کند. آنالایزر هنگام انجام نظارت x باارزشی روی قسمت بی سیم تبادل تصدیق هویت بر سایت، نوع تصدیق هویت را مشخص می کند و این بررسی به مدیران شبکه اجازه می دهد که محافظت از کلمات عبور توسط رمزنگاری قوی را تضمین کنند.

امنیت تجهیزات شبکه

۸ ۱ امنیت تجهیزات شبکه

برای تامین امنیت بر روی یک شبکه، یکی از بحرانی ترین و خطیرترین مراحل، تامین امنیت دسترسی و کنترل تجهیزات شبکه است. تجهیزاتی همچون مسیریاب، سوئیچ یا دیوارهای آتش.

اهمیت امنیت تجهیزات به دو علت اهمیت ویژه ای می یابد :

الف – عدم وجود امنیت تجهیزات در شبکه به نفوذگران به شبکه اجازه می دهد ک ه با دستیابی به تجهیزات امکان پیکربندی آنها را به گونه ای که تمایل دارند آن سخت افزارها عمل کنند، داشته باشند. از این طریق هرگونه نفوذ و سرقت اطلاعات و یا هر نوع صدمه دیگری به شبکه، توسط نفوذگر، امکان پذیر خواهد شد.

تأمین امنیت تجهزات بر روی شبکه

DoS (Denial of Service)

ب – برای جلوگیری از خطرهای الزامی است. توسط این حمله ها نفوذگران م یتوانند سرویس هایی را در شبکه از کار بیاندازند که از این فراهم AAA طریق در برخی موارد امکان دسترسی به اطلاعات با دور زدن هر یک از فرایندهای می شود.

در این بخش اصول اولیه امنیت تجهیزات مورد بررسی اجمالی قرار می گیرد. عناوین برخی از این موضوعات به شرح زیر هستند :

- امنیت فیزیکی و تأثیر آن بر امنیت کلی شبکه
- امنیت تجهیزات شبکه در سطوح منطقی
- بالابردن امنیت تجهیزات توسط افزونگی در سرویس ها و سخت افزارها

موضوعات فوق در قالب دو جنبه اصلی امنیت تجهیزات مورد بررسی قرار م یگیرند :

- امنیت فیزیکی
- امنیت منطقی

۸ ۲ امنیت فیزیکی

امنیت فیزیکی بازه وسیعی از تدابیر را در بر می گیرد که استقرار تجهیزات در مکان های امن و به دور از خطر حملات نفوذگران و استفاده از افزونگی در سیستم از آن جمل هاند. با استفاده از افزونگی، اطمینان از صحت عملکرد سیستم در صورت ایجاد و رخداد نقص در یکی از تجهیزات (که توسط عملکرد مشابه سخت افزار و یا سرویس دهنده مشابه جایگزین می شود) بدست می آید.

در بررسی امنیت فیزیکی و اعمال آن ، ابتدا باید به خطر هایی که از این طریق تجهزات شبکه را تهدید میکنند نگاهی داشته باشیم. پس از شناخت نسبتاً کامل این خطرها و حمله ها م یتوان به را هحل ها و ترفند های دفاعی در برار این گونه حملات پرداخت.

۸ ۲ ۱ افزونگی در محل استقرار شبکه

یکی از را هکارها در قالب ایجاد افزونگی در شبکه های کامپیوتری، ایجاد سیستمی کامل، مشابه شبکه ی اولیه ی در حال کار است. در این راستا، شبکه ی ثانویه ی، کاملاً مشابه شبکه ی اولیه، چه از بعد تجهیزات و چه از بعد کارکرد، در محلی که م یتواند از نظر جغرافیایی با شبکه ی اول فاصله ای نه چندان کوتاه نیز داشته باشد برقرار می شود. با استفاده از این دو سیستم مشابه، علاوه بر آنکه در صورت رخداد وقایعی که کارکرد هریک از این دو شبکه را به طور کامل مختل می کند (مانند زلزله) م یتوان از شبکه ی دیگر به طور کاملاً جایگزین استفاده کرد، در استفاده های روزمره نیز در صورت ایجاد ترافیک سنگین بر روی شبکه، حجم ترافیک و پردازش بر روی دو شبکه ی مشابه پخش می شود تا زمان پاسخ به حداقل ممکن برسد.

با وجود آنکه استفاده از این روش در شبکه های معمول که حجم جندانی ندارند، به دلیل هزینه های تحمیلی بالا، امکان پذیر و اقتصادی به نظر نمی رسد، ولی در شبکه های با حجم بالا که قابلیت اطمینان و امنیت در آنها از اصول اولیه به حساب م یآیند از الزامات است.

۸ ۲ ۲ توپولوژی شبکه

طراحی توپولوژیکی شبکه، یکی از عوامل اصلی است که در زمان رخداد حملات فیزیکی م یتواند از خطای کلی شبکه جلوگیری کند.

بررسی سه طراحی که معمول هستند :

الف – طراحی سری : در این طراحی با قطع خط تماس میان دو نقطه در شبکه، کلیه سیستم به دو تکه منفصل تبدیل شده و امکان سرویس دهی از هریک از این دو ناحیه به ناحیه دیگر امکان پذیر نخواهد بود.

ب – طراحی ستاره ای : در این طراحی، در صورت رخداد حمله فیزیکی و قطع اتصال یک نقطه از خادم اصلی، سروی سدهی به دیگر نقاط دچار اختلال نم یگردد. با این وجود از آنجاییکه خادم اصلی در این میان نقش محوری دارد، در صورت اختلال در کارایی این نقطه مرکزی، که م یتواند بر اثر حمله فیزیکی به آن رخ دهد، ارتباط کل شبکه دچار اختلال می شود، هرچند که با درنظر گرفتن افزونگی برای خادم اصلی از احتمال چنین حالتی کاسته می شود.

ج – طراحی مش : در این طراحی که تمامی نقاط ارتباطی با دیگر نقاط در ارتباط هستند، هرگونه اختلال فیزیکی در سطوح دسترسی منجر به اختلال عملکرد شبکه نخواهد شد، با وجود آنکه زمان بندی سروی سدهی را دچار اختلال خواهد کرد. پیاد هسازی چنین روش با وجود امنیت بالا، به دلیل محدودیت های اقتصادی ، تنها در موارد خاص و بحرانی انجام می گیرد.

۸ ۲ ۳ محل های امن برای تجهیزات

در تعیین یک محل امن برای تجهیزات دو نکته مورد توجه قرار می گیرد :

- یافتن مکانی که به اندازه کافی از دیگر نقاط مجموعه متمایز باشد، به گونه ای که هرگونه نفوذ در محل آشکار باشد.

- در نظر داشتن محلی که در داخل ساختمان یا مجموعه ای بزرگتر قرار گرفته است تا تدابیر امنیتی بکارگرفته شده برای امن سازی

مجموعه ی بزرگتر را بتوان برای امن سازی محل اختیار شده نیز به کار گرفت.

با این وجود، در انتخاب محل، میان محلی که کاملاً جدا باشد (که نسبتاً پرهزینه خواهد بود) و مکانی که درون محلی نسبتاً عمومی قرار دارد و از مکان های بلااستفاده سود برده است (که باعث ایجاد خطرهای امنیتی م یگردد) ، م یتوان اعتدالی منطقی را در نظر داشت.

در مجموع می توان اصول زیر را برای تضمین نسبی امنیت فیزیکی تجهیزات در نظر داشت :

- محدود سازی دسترسی به تجهیزات شبکه با استفاده از قفل ها و مکانیزم های دسترسی دیجیتالی به همراه ثبت زما نها، مکان ها و کدهای کاربری دسترسی های انجام شده.

- استفاده از دوربین های پایش در ورودی محل های استقرار تجهیزات شبکه و اتاق های اتصالات و مراکز پایگاه های داده.

- اعمال ترفند هایی برای اطمینان از رعایت اصول امنیتی.

۸ ۲ ۴ انتخاب لایه کانال ارتباطی امن

با وجود آنکه زمان حمله ی فیزیکی به شبکه های کامپیوتری، آنگونه که در قدیم شایع بوده، گذشته است و در حال حاضر تلاش اغلب نفوذگران بر روی به دست گرفتن کنترل یکی از خادم ها و سروی سدهنده های مورد اطمینان شبکه معطوف شده است ، ولی گون های از حمل هی فیزیکی کماکان دارای خطری بحرانی است. و چه در زوج های تابیده، هم اکنون نیز از راه های Coax عمل شنود بر روی سیم های مسی، چه در انواع نفوذ به شمار م یآیند. با استفاده از شنود م یتوان اطلاعات بدست آمده از تلاش های دیگر برای نفوذ در سیستم های کامپیوتری را گسترش داد و به جمع بندی مناسبی برای حمله رسید. هرچند که میتوان سیم ها را نیز به گونه ای مورد

محافظت قرار داد تا کمترین احتمال برای شنود و یا حتی تخریب فیزیکی وجود داشته باشد، ولی در حال حاضر، امن ترین روش ارتباطی در لایه ی فیزیکی، استفاده از فیبرهای نوری است.

در این روش به دلیل نبود سیگنال های الکتریکی، هیچگونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از رو شهای معمول شنود به پایین ترین حد خود نسبت به استفاده از سیم در ارتباطات می شود.

۸ ۲ ۵ منابع تغذیه

از آنجاکه داده های شناور در شبکه به منزله ی خون در رگهای ارتباطی شبکه هستند و جریان آنها بدون وجود منابع تغذیه، که با فعال نگا هداشتن نقاط شبکه موجب برقراری این جریان هستند، غیر ممکن است، لذا چگونگی چینش و نوع منابع تغذیه و قدرت آنها نقش به سزایی در این میان بازی می کنند. در این مقوله توجه به دو نکته زیر از بالاترین اهمیت برخوردار است :

- طراحی صحیح منابع تغذیه در شبکه بر اساس محل استقرار تجهیزات شبکه . این طراحی باید به گونه ای باشد که تمامی تجهیزات فعال شبکه، برق مورد نیاز خود را بدون آنکه به شبک هی تامین فشار بیش اندازه ای (که باعث ایجاد اختلال در عملکرد منابع تغذیه شود) وارد شود، بدست آورند. - وجود منبع یا منابع تغذیه پشتیبان به گونه ای که تعداد و یا نیروی پشتیبانی آنها به نحوی باشد که نه تنها برای تغذیه کل شبکه در مواقع نیاز به منابع تغذیه پشتیبان کفایت کند، بلکه امکان تامین افزونگی مورد نیاز برای تعدادی از تجهیزات بحرانی درون شبکه را به صورت منفرد فراهم کند.

۸ ۲ ۶ عوامل محیطی

یکی از نکات بسیار مهم در امن سازی فیزیکی تجهیزات و منابع شبکه، امنیت در برار عوامل محیطیاست. نفوذگران در برخی از موارد با تاثیرگذاری بر روی این عوامل، باعث ایجاد اختلال در عملکرد شبکه می شوند. از مهمترین عواملی در هنگام بررسی امنیتی یک شبکه رایانه ای باید در نظر گرفت میتوان به دو عامل زیر اشاره کرد :

- احتمال حریق (که عموماً غیر طبیعی است و منشآ انسانی دارد)
- زلزله، طوفان و دیگر بلایای طبیعی

با وجود آنکه احتمال رخداد برخی از این عوامل، مانند حریق، را می توان تا حدود زیادی محدود نمود، ولی تنها راه حل عملی و قطعی برای مقابله با چنین وقایعی، با هدف جلوگیری در اختلال کلی در عملکرد شبکه، وجود یک سیستم کامل پشتیبان برای کل شبکه است. تنها با استفاده از چنین سیستم پشتیبانی است که م یتوان از عدم اختلال در شبکه در صورت بروز چنین وقعایعی اطمینان حاصل کرد.

۸ ۳ امنیت منطقی

امنیت منطقی به معنای استفاده از روش هایی برای پایین آوردن خطرات حملات منطقی و نرم افزاری برضد تجهیزات شبکه است. برای مثال حمله به مسیریاب ها و سوئیچ های شبکه بخش مهمی از این گونه حملات را تشکیل می دهند. در این بخش به عوامل و

مواردی که در اینگونه حملات و ضد حملات مورد نظر قرار م یگیرند می پردازیم.

۸ ۳ ۱ امنیت مسیریا بها

حملات ضد امنیتی منطقی برای مسیریاب ها و دیگر تجهیزات فعال شبکه، مانند سوئیچ ها، را م یتوان به سه دسته ی اصلی تقسیم نمود:

- حمله برای غیرفعال سازی کامل
- حمله به قصد دستیابی به سطح کنترل
- حمله برای ایجاد نقص در سرویس دهی

طبیعی است که راه ها و نکاتی که در این زمینه ذکر می شوند مستقیماً به امنیت این عناصر به تنهایی مربوط بوده و از امنیت دیگر مسیرهای ولو مرتبط با این تجهیزات منفک هستند. لذا تأمین امنیت تجهیزات فعال شبکه به معنای تآمین قطعی امنیت کلی شبکه نیست، هرچند که عملاً مهمترین جنب هی آنرا تشکیل می دهد.

۸ ۳ ۲ مدیریت پیکربندی

یکی از مهمترین نکات در امینت تجهیزات، نگاهداری نسخ پشتیبان از پرونده ها مختص پیکربندی است. از این پرونده ها که در حافظه های گوناگون این تجهیزات نگاهداری می شوند ، م یتوان در فواصل زمانی مرتب یا تصادفی، و یا زمانی که پیکربندی تجهیزات تغییر می یابند، نسخه پشتیبان تهیه کرد. با وجود نسخ پشتیبان، منطبق با آخرین تغییرات اعمال شده در تجهیزات، در هنگام رخداد اختلال در کارایی تجهزات، که م یتواند منجر به ایجاد اختلال در کل شبکه شود، در کوتاه ترین زمان ممکن م یتوان با جایگزینی آخرین پیکربندی، وضعیت فعال شبکه را به آخرین حالت بی نقص پیش از اختلال بازگرداند. طبیعی است که در صورت بروز حملات علیه بیش از یک سخت افزار، باید پیکربندی تمامی تجهیزات تغییریافته را بازیابی نمود.

نرم افزارهای خاصی برای هر دسته از تجهیزات مورد استفاده وجود دارند که قابلیت تهیه نسخ پشتیبان را فاصل ههای زمانی متغیر دارا می باشند. با استفاده از این نر م افزارها احتمال حملاتی که به سبب تآخیر در ایجاد پشتیبان بر اثر تعلل عوامل انسانی پدید م یآید به کمترین حد ممکن می رسد.

۸ ۳ ۳ کنترل دسترسی به تجهیزات

دو راه اصلی برای کنترل تجهزات فعال وجود دارد :

- کنترل از راه دور
- کنترل از طریق درگاه کنسول

در روش اول م یتوان با اعمال محدودیت در امکان پیکربندی و دسترسی به تجهیزات از آدرس هایی خاص یا استاندارها و پروتکل های خاص، احتمال حملات را پایین آورد. در مورد روش دوم، با وجود آنکه به نظر می رسد استفاده از چنین درگاهی نیاز به دسترسی فیزکی مستقیم به تجهیزات دارد، ولی دو روش معمول برای دسترسی به تجهیزات فعال بدون داشتن دسترسی مستقیم وجود دارد. لذا در صورت عدم کنترل این نوع دسترسی، ایجاد محدودیت ها در روش اول عملاً امنیت تجهیزات را تآمین نمی کند. برای ایجاد امنیت در روش دوم باید از عدم اتصال مجازی درگاه

کنسول به هریک از تجهیزات داخلی مسیریاب، که امکان دسترسی از راه دور دارند، اطمینان حاصل نمود.

۸ ۳ ۴ ایمن سازی دسترسی

یکی دیگر از روش های معمول ،Authentication علاوه بر پیکربندی تجهیزات برای استفاده از امن سازی دسترسی، استفاده از کانال رمز شده در حین ارتباط است. یکی از ابزار معمول در این روش ارتباطات فعال را رمز کرده و احتمال شنود و تغییر در ارتباط که از SSH . است SSH(Secur Shell) معمول ترین روش های حمله هستند را به حداقل می رساند.

این روش IPsec مبتنی بر VPN از دیگر روش های معمول م یتوان به استفاده از کانال های اشاره نمود. روشی با قابلیت اطمینان بالاتر است، به گونه ای که اغلب تولیدکنندگان SSH نسبت به روش استفاده از تجهیزات فعال شبکه، خصوصاً تولید کنندگان مسیریاب ها ، این روش را مرجح می دانند.

۸ ۳ ۵ مدیریت رمزهای عبور

است. هرچند که در Authentication مناسب ترین محل برای ذخیره رمزهای عبور بر روی خادم بسیاری از موارد لازم است که بسیاری از این رموز بر روی خود سخ تافزار نگاه داری شوند. در این صورت مهم ترین نکته به یاد داشتن فعال کردن سیستم رمزنگاری رموز بر روی مسیریاب یا دیگر سخت افزارهای مشابه است.

۸ ۴ ملزومات و مشکلات امنیتی ارائه دهندگان خدمات

زمانی که سخن از ارائه دهندگان خدمات و ملزومات امنیتی آنها به میان می آید، مقصود شبکه های بزرگی است که خود به شبکه های رایانه ای کوچکتر خدماتی ارائه م یدهند. به عبارت دیگر این شبکه های بزرگ هستند که با پیوستن به یکدیگر، عملاً شبکه ی جهانی

اینترنت کنونی را شکل می دهند. با وجود آنکه غالب اصول امنیتی در شبک ههای کوچکتر رعایت می شود، ولی با توجه به حساسیت انتقال داده در این اندازه، ملزومات امنیتی خاصی برای این قبیل شبکه ها مطرح هستند.

۸ ۴ ۱ قابلیتهای امنیتی

ملزومات مذکور را می توان، تنها با ذکر عناوین، به شرح زیر فهرست نمود :

۱ –قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع حملات

۲ –وجود امکان بررسی ترافیک شبکه، با هدف تشخیص بسته هایی که به قصد حمله بر روی شبکه ارسال می شوند. از آنجاییکه شبکه های بزرگتر نقطه تلاقی مسیرهای متعدد ترافیک بر روی شبکه هستند، بر روی آنها، م یتوان به بالاترین بخت برای تشخیص حملات دست IDS با استفاده از سیستمهای یافت.

۳ – قابلیت تشخیص منبع حملات. با وجود آنکه راه هایی از قبیل سرقت آدرس و استفاده از سیستم های دیگر از راه دور، برای حمله کننده و نفوذگر، وجود دارند که تشخیص منبع اصلی حمله را دشوار م ینمایند، ولی استفاده از سیستم های ردیابی، کمک شایانی برای دست یافتن و یا محدود ساختن بازه ی DoS مشکوک به وجود منبع اصلی م ینماید. بیشترین تآثیر این مکانیزم زمانی است که حملاتی از نوع از سوی نفوذگران انجام م یگردد.

۸ ۴ ۲ مشکلات اعمال ملزومات امنیتی

با وجود لزوم وجود قابلیت هایی که بطور اجمالی مورد اشاره قرار گرفتند، پیاده سازی و اعمال آنها همواره آسان نیست. است. خطر یا ترافیکی که برای یک دسته از کاربران به IDS یکی از معمول ترین مشکلات، پیاد هسازی عنوان حمله تعبیر می شود، برای دسته ای دیگر به عنوان جریان عادی داده است. لذا تشخیص این دو افزوده و در اولین گام از کارایی و سرعت پردازش ترافیک و IDS جریان از یکدیگر بر پیچیدگی بسته های اطلاعاتی خواهد کاست. برای جبران

این کاهش سرعت تنها می توان متوسل به تجهیزات گران تر و اعمال سیاست های امنیتی پیچیده تر شد.

با این وجود ، با هرچه بیشتر حساس شدن ترافیک و جریان های داده و افزایش کاربران، و مهاجرت کاربردهای متداول بر روی شبک ههای کوچکی که خود به شبکه های بزرگتر ارائه دهنده خدمات متصل هستند، تضمین امنیت، از اولین انتظاراتی است که از اینگونه شبکه ها م یتوان داشت.

۹ ۱ مروری بر استانداردهای شبکه های محلی بدون سیم

استفاده از شبکه های محلی بدون سیم در نتیجه پیشرفت مخابرات دیجیتال و کامپیوترهای قابل حمل ونیز اینترنت، سرعت بسیار زیادی گرفته است. اولین کاربردهایی که برای این سیستم در نظر گرفته شد در مکانهایی بود که حرکت زیادی نیاز نداشت مانند استفاده در انبارها یا ترمینالهای فروش اجناس در مغازه ها. سپس این روش برای

کاربردهایی که در آن حرکت با سرعت کم وجود داشت پیشنهاد شد مانند دانشگاهها و بیمارستانها.

واضح است که استفاده از شبکه با سیم و کابل به مراتب گرانتر از شبکه است. از طرف دیگر از شبکه بدون سیم م یتوان به عنوان گسترش شبکه با سیم و یا به عنوان WLAN در کاربرهایی که امنیت شبکه مهم است استفاده کرد. (back up) پشتیبان آن با توجه به این کاربردها و نیاز به وجود یک استاندارد یکسان در محصولات، در حال حاضر دو گروه گروه ۸۰۲ ، استاندارد IEEE مشغول به فعالیت هستند. در WLAN متفاوت روی استانداردهای HiperLAN استاندارد دیگری را بنا م ، ETSI اختصاص داده اند و نیز ۸۰۲,۱۱ WLAN را به درنظر گرفته است . WLAN برای سه باند فرکانسی برای آن مورد استفاده قرار گرفته است که شامل ، WLAN از شروع به ساخت ۹۰۰ هیچ استاندارد مشترکی وجود ۲,۴ MHz است. در باند ۹۰۰MHz ,۵GHz ,GHz باندهای آن، باند b ندارد و هر شرکتی محصول خود را ارائه کرده است.

ولی استاندارد ۸۰۲,۱۱و ضمیمه دارای ۵ IEEE, ETSI نیز هر دو گروه ۲,۴ GHz را مورد توجه قرار داده است. در باند GHz استاندارد هستند. نکته مهم در این باند این است که این باند در

آمریکا و اروپا یکسان نیست و بنابراین با اینکه این دو استاندارد شباهت زیادی دارند، تفاوتهایی بخصوص در باند فرکانسی دارند. در این گزارش ابتدا مروری کوتاه بر استانداردهای این دو گروه خواهیم داشت. در بخش سوم مدولاسیون لایه فیزیکی استانداردها مورد توجه قرار گرفته و در بخش چهارم نیز لایه دسترسی چندگانه استانداردها مورد بررسی قرار می گیرد.

گروه IEEE ۸۰۲,۱۱ ۳ ۹ استاندارد :

تنها به دو لایه فیزیکی و دسترسی چندگانه پرداخته است . در اولین WLAN استاندارد ۸۰۲,۱۱ برای نسخه این استاندارد که در سال ۹۷ داده شد ، سه روش مختلف برای لایه فیزیکی ارائه شده است .

وپرش (DS) این سه روش شامل ، دو روش رادیوئی طیف گسترده ، که به روش دنباله مستقیم است .

در هر Diffused Infrared تقسیم می شود و همچنین روش نوری بصورت (FH) فرکانسی ۱،۲ باید قابل ارسال باشند . لازم به

ذکر است که دو روش Mbit/Sec سه روش، داده ها با نرخ ۲,۴ انجام می شود. GHz در فرکانس مرکزی ISMi ارسال در باند فرکانس FH و DS رادیوئی در سال ۹۹ ، دو ضمیمه به این استاندارد اضافه شد که در آنها دو پیشنهاد جدید برای لایه فیزیکی ارائه در ۸۰۲,۱۱ OFDMii روش مدولاسیون a شده بود تا به نرخهای داده بالاتری دست یابد . در ضمیمه است، ارائه شده است .

با این روش مدولاسیون نرخ ۵ UNIIiii که مطابق قوانین GHz باند فرکانسی ۸۰۲,۱۱) در ۵۴ (b قابل تغییر است. در ضمیمه دوم ۶ Mbit/Sec تا Mbit/Sec ارسال داده از استفاده می کند و فقط با بکارگیری کد های ۲,۴ DS از همان روش طیف گسترده GHZ باند توانسته است که تعداد بیت بیشتری در هر دنباله طیف گسترده بفرستد و قابلیت Complementary دارد . ۱۱ DS را نیز با روش ۵,۵ Mbit/Sec و Mbit/Sec ارسال بطور خلاصه مدولاسیون، نرخ داده و باند فرکانسی استاندارد ۸۰۲,۱۱ در جدول ۱ توضیح داده شده است .

IEEE جدول ۹ ۱ مقایسه استانداردهای

Standard	Modulation	Frequency Band	Bit Rate(Mbps)
802.11	DS FH Infrared	2-4 GHz 2-4 GHz Baseband	1-2
802.11 a	OFDM	5 GHz**	6-54
802.11 b	DS (CCK)*	2.4 GHz	1-2-5.5-11

* CCK : Complememtry Code Keying

: (GHz ۵,۱۵ (۵,۸۲۵-۵,۷۲۵

و - باند ۵,۳۵ ** UNII

در مورد لایه دسترسی چندگانه، همه روش های بالا دارای یک استاندارد هستند که در دو ساختار کار می کنند و قابلیت ارسال داده را بصورت غیر همزمان به روش Ad hoc و Infrastructure دارند

CSMA/CAiv .

HiperLAN : گروه ۴ ۹ ETSI استاندارد

را برای شبکه های محلی HiperLAN استاندارد ، ETSI گروه استاندارد اروپایی IEEE همزمان با بدون سیم پیشنهاد کرده اند که خود این استانداردها نیز شامل دو لایه فیزیکی و دسترسی چندگانه است.

تا بحال چهار نوع از این استاندارد ارائه شده است.

۵ است و فقط نوع ۱ و ۲ مربوط به استاندارد شبکه محلی GHz در ۳ استاندارد اول فرکانس کاردر است و استاندارد Wireless Local Loop بدون سیم است در حالیکه استاندارد سوم مربوط به چهارم نیز ارتباط نقطه به نقطه را مد نظر قرار داده است. لایه دسترسی چندگانه این استانداردها تنها در نوع اول شبیه ۸۰۲,۱۱ است ولی در استاندارد دوم و دوپلکس TDMA را نیزپشتیبانی می کند و بصورت ATM های مختلفی ارائه شده که QoSv زمانی است. در مورد لایه فیزیکی وضعیت به عکس است و لایه فیزیکی استاندارد دوم بسیار

مشابه و اکوالایزرهای پیچیده استفاده می کند. بطور GMSK ۸۰۲,۱۱ است و استاندارد اول از روش a را خلاصه کرد . خلاصه در شکل زیر می توان انواع مختلف استانداردهایHiperLAN

	HIPERLAN Type 1	HIPERLAN Type 2	HIPERAccess	HIPERLink
Application	Wireless Ethernet (LAN)	Wireless ATM	Wireless Local Loop	Wireless Point-to-Point
Frequency Range	5 GHz	5 GHz	5 GHz	17 GHz
Data Rate	23.5 Mbps	~20 Mbps	~20 Mbps	~155 Mbps
Status	Completed and ratified 1996	Under development	Under development	No current activity

HiperLAN شکل ۹ ۱ انواع مختلف استاندارد های

۹ ۵ WLAN مشخصات لایه فیزیکی استانداردهای

را مورد بحث قرار WLAN در این قسمت مشخصات لایه فیزیکی تمام استاندارد های مربوط به میدهیم . ابتدا به روش ارسال نوری بطور مختصر اشاره کرده و سپس به روشهای طیف گسترده که در را

OFDM ۲,۴ پیشنهاد شده می پردازیم. در آخر نیز روش GHz استاندارد ۸۰۲,۱۱ و در باند بصورت کامل مورد مطالعه قرار می دهیم.

۹ ۵ ۱ روش ارسال نوری :استاندارد ۸۰۲,۱۱

همانطور که گفته شد در استاندارد ۸۰۲,۱۱ یک روش مدولاسیون نوری نیز مطرح گردیده است. مطابق استفاده کرد و PPMvii ویا استفاده از روش OOKvi با این استاندارد می توان از مدولاسیونهای ساده از تکنیکهای دستیابی چندگانه در حوزه زمان یا در حوزه کد برای استفاده همزمان کاربران از کانال استفاده کرد .

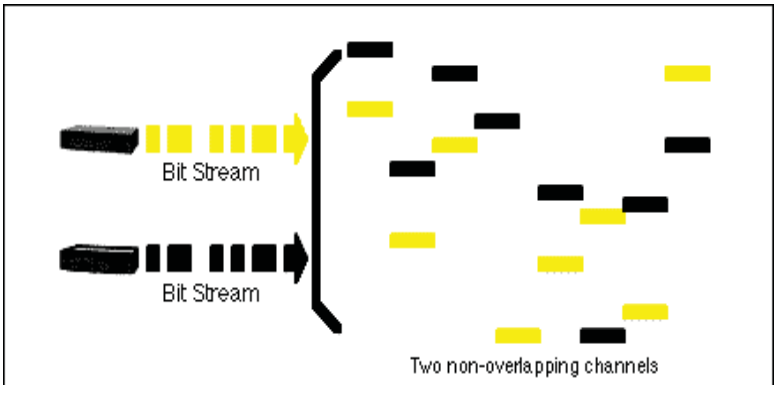
در روشهای نوری با استفاده از خاصیت پراکنده ساز بودن سطوح می توان از موانع هم سیگنال را عبور ۵۰ در شعاع حدود ۳ متر دست یافته اند همچنین موسسه Mbps داده که در این حالت به نرخهای داده روش ارسال داده بصورت نقطه به نقطه که Infrared Data Association (IrDa) استاندارد نوری ۱۶ ۴ Mbps تا Mbps نیاز به دید مستقیم دارد را ارائه کرده که در فاصله کمتر از ۱۰ متر با نرخ است که نرخ ارسال Bluetooth قابلیت ارسال دارد را ساخته

است . روش رادیویی مقابل آن تکنیک پایین تری دارد ولی قابلیت عبور از دیوار و موانع را داراست و شعاع بیشتری را تحت پوشش قرار می دهد .

۹ ۵ ۲ روش ارسال طیف گسترده پرش فرکانسی استاندارد ۸۰۲,۱۱:

۲,۴ پیشنهاد شده است. این باند GHz این روش طیف گسترده در استاندارد ۸۰۲,۱۱ در باند فرکانسی ۱ تقسیم کرده و با استفاده از ۷۹ MHz پهنا دارد را به ۷۹ کانال با عرض MHz فرکانسی که ۲ را دارد. Mbps و نیز شکل پرش فرکانسی بین ۷۹ کانال، قابلیت ارسال داده تا GFSK مدولاسیون لازم به ذکر است که پرش کردن بین فرکانس ها از روی یک کد مشخصی است که به زوج فرستنده و گیرنده اختصاص داده شده است و برای بقیه کاربران قابل درک نخواهد بود نکته قابل توجه دیگر این است که این روش از لحاظ پیاده سازی از بقیه روشها ارزانتر بوده ولی دارای دو اشکال مهم است: بین هر پرش فرکانسی مقداری اتلاف زمان در سوئیچ کردن بین فرکانسها داریم و نیز با این روش نرخ داده قابل افزایش بیشتر نخواهد

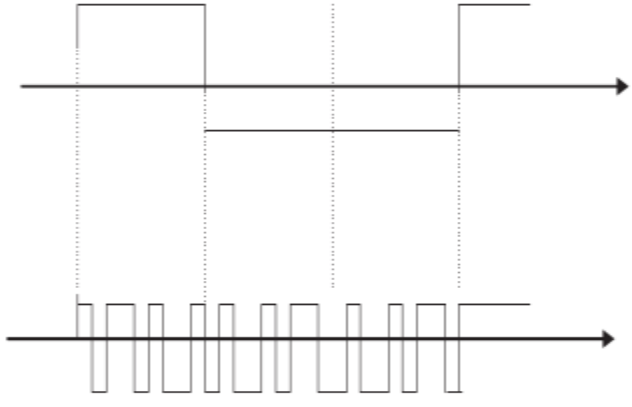
بود. در شکل زیر نحوه ارسال همزمان دو کاربر با کدهای مختلف نشان داده شده است.



شکل ۹ ۲ روش مدولاسیون طیف گسترده پرش فرکانسی

استاندارد ۸۰۲,۱۱ : ۳ ۵ ۹ DSviii

روش مدولاسیون طیف گسترده این روش نوعی دیگر از تکنیک طیف گسترده است که در آن هر بیت داده را در ۱۱ بیت که کد بارکر QPSK یا ۱۱ BPSK به روش Mbps برابر با Chip Rate است ضرب می کنیم و سپس آنرا با مدوله می کنیم و می فرستیم. کد بارکر دارای بهترین و تیزترین تابع همبستگی است. بطور مثال کد بارکر طول ۱۱ برابر است با: (۱ ،۱-،۱-،۱،۱-،۱،۱،۱،۱-،۱-،۱-).



شکل ۹ ۳روش مدولاسیون طیف گسترده دنباله مستقیم (DS)

۲۲ داریم که واضح است همپوشانی بین این کانالها خواهیم داشت که MHz در واقع ۵ کانال با پهنای بدلیل طیف گسترده بودن

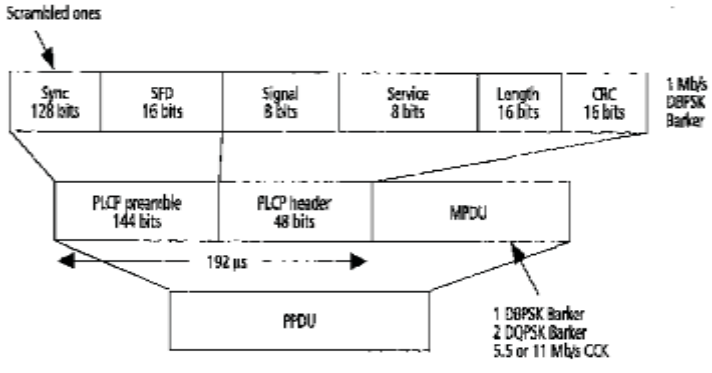
اشکالی در کارایی سیستم بوجود نمی آورد. همچنین فاصله مرکز کانالها از است ولی به ۱۵ FH است. بدلیل نرخ ارسال چیپ بالا این روش گرانتر از روش MHz همدیگر نرخهای داده بالاتر نیز می توان رسید که در قسمت بعد به آن اشاره خواهد شد. در شکل زیر نحوه ارسال داده با ضرب کردن در دنباله مستقیم نشان داده شده است.

b۸۰۲,۱۱ استاندارد : ۴ ۵ ۹ DS روش ارسال طیف گسترده

استفاده می کنیم ولی کد ۲,۴ DS و بصورت GHz در این روش دوباره از تکنیک طیف گسترده در باند گسترده کننده طیف آنرا تغییر می دهیم و بجای اینکه با هر کد ارسالی یک بیت داده بفرستیم در آن ۸ ۸ میکرو ثانیه است و کدهای استفاده / بیت را کد می کنیم و می فرستیم.

بنابراین عرض ارسال چیپ ۱۱ هستند. به این مدولاسیون Complementary Code بنام Golay شده از زیر مجموعه کد ها گفته می شود CCKix

۲,۴ است .برای GHz موضوع دیگر نحوه سازگاری روشهای ارائه شده در استاندارد ۸۰۲,۱۱ در باند که ۲ جزء Preamble, Header, Data : ارسالی از ۳ جزء تشکیل شده است x این سازگاری هربسته تشخیص سیگنال و سنکرون سازی است در Preamble ۱ ارسال می شود. وظیفه Mbps اول با نرخ اطلاعات مربوط به نرخ داده وطول هر بسته است. ساختار بسته در شکل زیر Header حالیکه در توضیح داده شده است.



شکل ۹ ۴ ساختار ارسالی هر بسته در ۸۰۲,۱۱

a۸۰۲,۱۱ استاندارد :

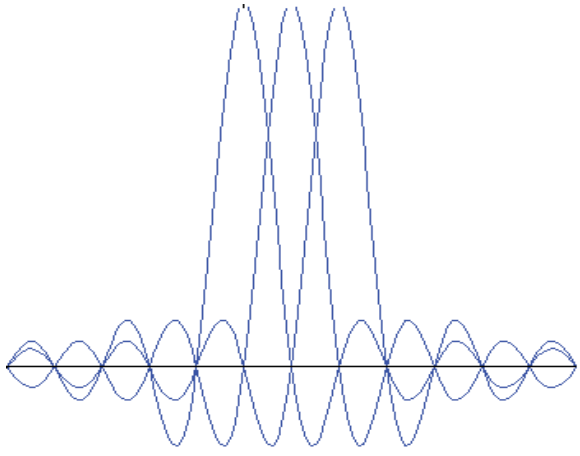
۵ ۵ ۹ OFDMxi روش مدولاسیون

پیشنهاد شده است .HiperLAN/ ۸۰۲,۱۱ و نیز ۲ a برای لایه فیزیکی استاندارد OFDM مدولاسیون ۵ هستند. ایده اصلی این روش در این است که با افزایش نرخ داده وکوتاه شدن GHz که هر دودر باند سیگنال در زمان، حساسیت سیگنال به تاخیر در کانال زیادتر می شود و با وجود فیدینگ متغیر با فرکانس شدیدا کارایی سیستم تحت تاثیر قرار می گیرد. روش مقابله با این اثر، افزایش طول سیگنال در زمان و استفاده از گارد زمانی است. بنابراین باید داده ها را بصورت موازی در فرکانس و در زمان طولانی تری بفرستیم . برای این کار دو روش موجود است :

۱) ر وش مالتیپلکس فرکانسی

در این روش سیگنالها را در فرکانس بطور مجزا کنار هم قرار میدهیم. این سیگنالها در فرکانس با هم همپوشانی ندارند، بنابر این به باند محافظ فرکانسی و نیز تعداد زیادی فیلتر جداکننده نیاز است. پس اولا پیاده سازی آن مشکل است، ثانیا بازده استفاده از فرکانس آن پایین است .

OFDM ۲) ر وش ملتیپلکس متعامد فرکانسی یا در این روش سیگنالها در فرکانس با یکدیگر همپوشانی دارند ولی چون در زمان مدوله شده روی پایه های عمود بر هم هستند قابل بازسازی هستند . بطور مثال هارمونیکهای مختلف یک سینوسی در یک پریود بر هم عمود هستند و در صورت مدوله شدن بصورت مستقل، دارای طیفی می شوند که در شکل زیر نمایش داده شده است. واضح است که طیف ساب کاریرها در فرکانس تداخل زیادی با یکدیگر دارند.



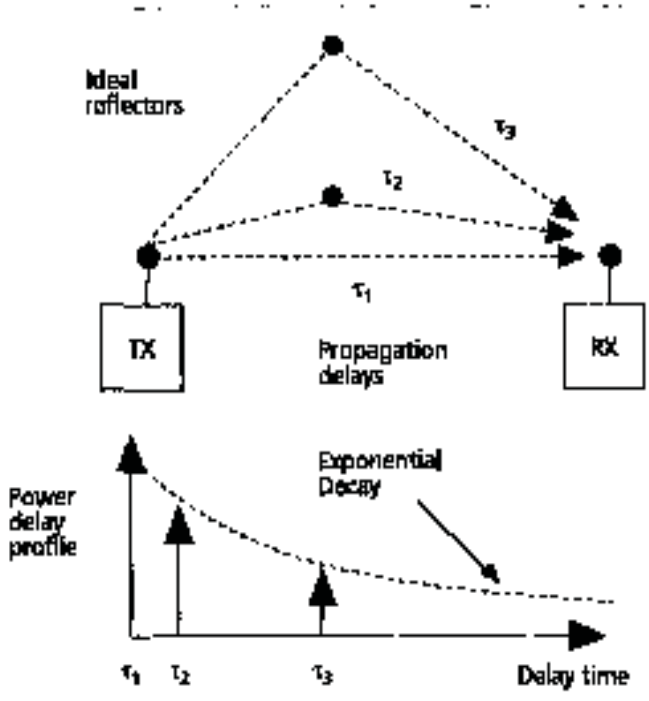
شکل ۹ ۵ طیف ارسالی سیگنال OFDM

همچنین لازم به ذکر است که اگر سیگنالها سنکرون نباشند تعامد پایه ها بهم خورده و در نتیجه سنکرون سازی یکی از مهمترین نکات این مدولاسیون است و در غیر این صورت کارآیی سیستم بشدت پایین می آید.

اثر فیدینگ چند مسیره است که این اثر بصورت آماری و متغیر از دیگر مسائل قابل مطرح در تصادفی رایلی در محیط OFDM داخل ساختمان مدل می شود.این اثر در شکل زیر نمایش داده شده است و بطور نمونه همچنین مقدار موثر تاخیر در محیطهای Indoor بشرح زیر است

جدول ۲ ۹ مقادیر نمونه ای تاخیر در کانال Indoor

Small Office	20-50 nsec
Large Office	50-100 nsec
Factory	100-200 nsec

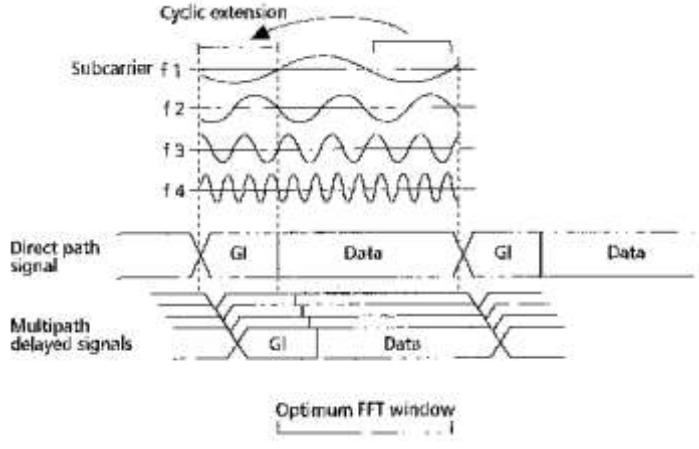


شکل ۹ ۶کانال فیدینگ چند مسیره

برای مقابله با این اثر از گارد زمانی در هر سمبول استفاده می کنیم که از اثر OFDM در مدولاسیون تداخل سمبولها بدلیل متغیر بودن تاخیر جلوگیری می کند. این تاخیر متغیر می تواند باعث از بین رفتن مقداری از اول سیگنال را به ICI، می گویند. برای از بین بردن ICIxii تعامد پایه ها نیز بشود که به آن می گویند.

در این صورت با وجود اثر Cyclic Extension انتهای آن اضافه می کنیم که به آن فیدینگ چند مسیره می توان یک پنجره بهینه ای پیدا کرد و داده ها را از آن استخراج کرد.

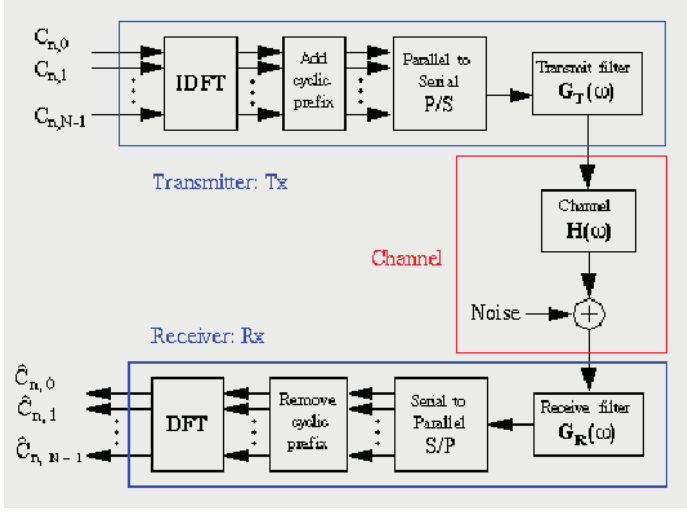
با این روش اثر کانال مانند ضرائب ثابتی در هر ساب کاریر ضرب می شود و واضح است که این اثر با تخمین کانال و نرمالیزاسیون قابل رفع است. این روش در شکل زیر نمایش داده شده است.



برای مقابله با فیدینگ چند مسیره Cyclic Prefix شکل ۹ ۷ نحوه بکارگیری

نکته مهم دیگری که مطرح می شود استفاده از پنجره مناسب در حوزه زمان است که این باعث می شود که مولفه های فرکانسی خارج باند کاهش یابد و سیگنال هموارتر شود.

این کار همچنین تداخل و باید از گارد زمانی بجای ISI و ICI حساسیت به فرکانس را کاهش می دهد.بنابراین برای جلوگیری از اکوالایزر استفاده کرد.



OFDM شکل ۹ ۸ دیاگرام بلوکی گیرنده و فرستنده

در واقع وظایف گیرنده در ۵ مرحله خلاصه می شود :
تخمین بزند. برای اینکار در استاندارد ۸۰۲,۱۱ Preamble آفست فرکانس وضرائب کانال را با کمک ۲۰ تغییرات فرکانس پیش بینی شده است. ppm (part per million) برای هر کاربر گرفتن.

FFT دمدوله کردن بوسیله نرمالیزه کردن به ضرائب کانال و حذف اثر کانال. شیفت فاز را که حاصل از کمی تخمین غلط فرکانس است ، تصحیح کند. بدست آورد. Constellation داد ها را از روی نوع در شکل زیر نمایش بلوکی این سیستم نشان داده شده است.

۸۰۲,۱۱ نشان داده شده است a در ضمیمه OFDM در شکل زیر نیز مشخصات اصلی استاندارد

۹ مشخصات اصلی مدولاسیون استفاده می کنیم و Puncturing لازم به تذکر است که برای داشتن نرخ داده های مختلف در سیستم از با نرخ کدینگ متفاوت به نرخهای داده متفاوت خواهیم رسید.

۸۰۲,۱۱ چیزی گفته نشد. ولی این a بدلیل شباهت زیاد با HiperLAN/ تا بحال در مورد استاندارد ۲ دو در سه مورد جزئی تفاوت دارند

Data rate	6, 9, 12, 18, 24, 36, 48, 54 Mbit/s
Modulation	BPSK, QPSK, 16-QAM, 64-QAM
Coding rate	1/2, 2/3, ¾
Number of subcarriers	52
Number of pilots	4
OFDM symbol duration	4 µs
Guard interval	800 ns
Subcarrier spacing	312.5 kHz
-3 dB Bandwidth	16.56 MHz
Channel spacing	20 MHz

شکل ۹ OFDM در a۸۰۲,۱۱

های اضافی برای رسیدن به نرخهای متفاوت استفاده شده است . Puncturing از HiperLAN/ در ۲

۸۰۲,۱۱ متفاوت است . ۲۴ a با Mbps نرخ کد کانولوشن در نرخ HiperLAN/ در ۲

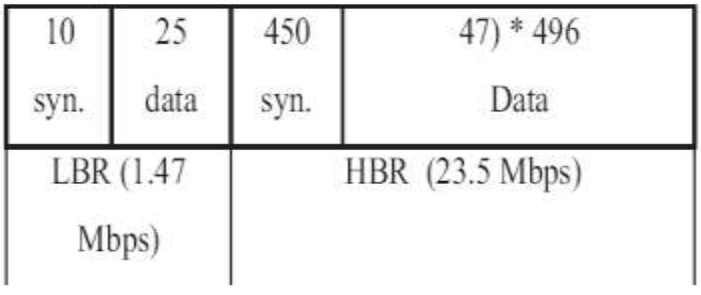
برای سنکرون کردن متفاوت است. training دنباله های اشاره کرد که داشتن تغییرات زیاد دامنه OFDM در انتها لازم است به یک مشکل اساسی سیگنالهای سیگنال در زمان است که نیاز به تقویت کننده های بسیار خطی را ایجاب می کند. برای مقابله با این اثر روشهای زیادی مانند استفاده از کدینگ یا برش دامنه سیگنال، ارائه شده است

HiperLAN/ استاندارد ۲ :۶ ۵ ۹ GFSK روش مدولاسیون این استاندارد بدلیل پیچیدگی پیاده سازی و به صرفه نبودن اقتصادی آن، تابحال در بازار ارائه نشده به همراه اکوالایزر استفاده شده است . در جدول زیر GFSK است. در این استاندارد از مدولاسیون مشخصات اصلی این استاندارد ارائه شده است.

TX frequency/power	5150 - 5300 MHz@10mW..1W
frequency accuracy	10ppm
RX-sensitivity	-50, -60, -70 dBm
Channels	5 (FDMA)
Bandwidth/channel	23.5294 MHz
Max. velocity	1.4 m/s (5 km/h)
Protocol features	•OSI Medium Access Control SAP Interface •instantaneous ACK; CRC •connectionless, peer-to-peer structure •variable packet length •support of Time Bounded Services •efficient sleep and doze mode •Forwarders
Modulation	•HBR: GMSK with BT=0.3 •LBR: FSK
Data rate	•HBR: 23.5294 Mbps@10ppm •LBR: 1.47060 Mbps@10ppm
Max. burst duration	•1 ms
Error correction (FEC)	•BCH-code (31,26,3)
Error detection	•32 bits CRC

شکل ۹ ۱۰ مشخصات اصلی مدولاسیون GFSK در استاندارد HiperLAN

در این استاندارد هر بسته ارسالی به دو قسمت نرخ داده بالا و پایین بصورت زیرتقسیم می شود. در قسمت کم سرعت، اطلاعات مربوط به سنکرون سازی و طول بسته موجود است در حالیکه قسمت دیگر برای ارسال داده های استفاده می شود



شکل ۹ ۱۱ بسته ارسالی در استاندارد ۱

علت پیچیدگی پیاده سازی این مدولاسیون اثر فیدینگ چند مسیره است که نیاز به اکوالایزر با فیدبک و مقدار عملیات بسیار زیاد دارد. بطور مثال عنوان شده که نیاز به یک گیگا عملیات در ثانیه دارد که بسیار بالا است و از نظر اقتصادی بسیار گران خواهد بود.

۹ ۶ WLAN مشخصات لایه دسترسی چندگانه تمام استانداردهای

همانطور که می دانیم دسترسی چندگانه در مخابرات را به ۲ طریق کلی می توان انجام داد:

و در هر یک قسمتی از زمان یا TDMA, FDMA, CDMA روشهای تخصیص ثابت که عبارتند از فرکانس و یا کد خاصی به هر کاربر اختصاص می یابد.

, ALOHA, CSMA/CA, روشهای تخصیص تصادفی که بطور مثال می توان از روشهای نام برد.در این روش هر کاربر که مترصد ارسال داده در کانال CSMA/CD و Slotted ALOHA, است، سعی می کند با رقابت با بقیه کاربران و با استفاده از پروتوکل مشخصی به کانل دسترسی پیدا کند.

از روش تخصیص تصادفی استفاده HiperLAN/ بجز ۲ WLAN بر این اساس در استانداردهای بدلیل داشتن گارانتی برای انواع سرویسها از تخصیص ثابت HiperLAN/ شده است .

در استاندارد ۲ و دوپلکس زمانی استفاده شده است. البته این استاندارد هنوز نهایی نشده TDMA زمانی بصورت است و در این گزارش به همین میزان بسنده می کنیم. همانطور که گفته شد تمام استانداردهای ۸۰۲,۱۱ دارای یک استاندارد برای لایه دسترسی چندگانه ا مورد مطالعه قرار HiperLAN استاندارد ۸۰۲,۱۱ و MAC هستند. بنابر این در ادامه به ترتیب لایه می دهیم.

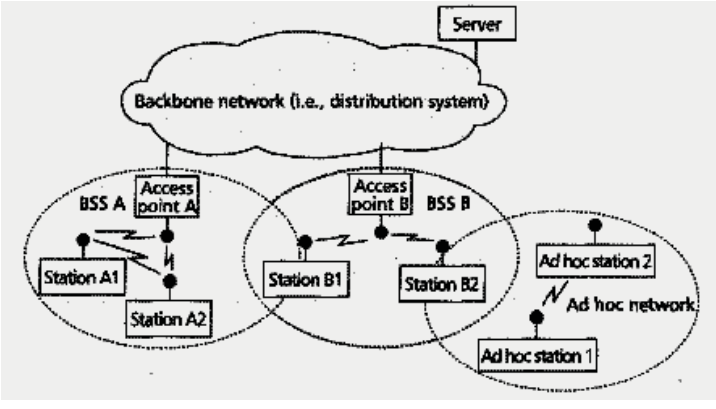
۹ ۶ ۱ پروتکل لایه دسترسی چندگانه در استاندارد ۸۰۲,۱۱

در استاندارد ۸۰۲,۱۱ ، دو ساختار برای شبکه پیشنهاد شده است Back bone در این ساختار که روش انتقال داده بصورت نفر به نفر

است نیازی به : Ad hoc ساختار برای شبکه نیست و فقط قابلیت ارسال آسنکرون را دارد .

برای شبکه است و قابلیت ارسال Back bone در این روش نیاز به یک :Infrastuscture ساختار سنکرون و آنسکرون را داراست .

در شکل زیر این دو مود کاری نمایش داده شده است.در قسمت راست شکل دو کاربر در شبکه با Back bone با هم ارتباط دارند در حالیکه بقیه کاربران از طریق شبکه (Ad hoc) بصورت مستقل پوشش خیلی بیشتری خواهیم Infrastructure یکدیگر مرتبط هستند. واضح است که در ساختار داشت



شکل ۹ ۱۲ توپولوژی و ساختار شبکه های محلی بدون سیم

در ارسال سنکرون داده با تاخیر محدود و بدون گارانتی مقدار خاصی برای تاخیر ارسال می شود . این انجام می شود که در آن آنتن مرکزی هر سلول مسئول برقرار کردن PCFxiii ارسال در مودکاری ارتباط هر کاربر با بقیه کاربران در سلول و نیز خارج سلول از طریق شبکه ثابت است.

انجام می شود. در این مود، ارتباط هر دو کاربر بدون DCFxiv ارسال آسنکرون بوسیله مودکاری و با استفاده از پنجره های تاخیر زمانی برقرار می شود . ارجحیت ارسال AP دخالت بقیه کاربران و نیز هر بسته نسبت به بسته های دیگر در موقع ارسال به کانال، بوسیله فاصله های خالی زمانی تعیین می بشرح زیر است : IFS می گویند .

انواع IFSxv شود که به این فاصله ها

کوتاهترین فاصله زمانی یا در واقع حداکثر ارجحیت در برقراری ارتباط است. :Short IFS(SIFS)

مورد استفاده قرار می گیرد. .PCF فاصله زمانی که در مود : PCF IFS(PIFS)

مورد استفاده قرار می گیرد. DCF فاصله زمانی که در مود : DCF IFS(DIFS)

DIFS>PIFS>SIFS بصورت IFS برای تعیین اولویت بین مود های کاری و نیز بسته ها، اندازه هر نیز از روی محدودیت در پیاده سازی این فاصله زمانی بدست (SIFS) است. کوتاهترین فاصله زمانی می آید. با توجه به زمان لازم برای تغییر وضعیت کاربر از فرستنده به گیرنده، مقدار های نمونه ای آن بشرح زیر است :

جدول ۹ ۳ : مقایسه کمترین زمان سوئیچ کردن بین وضعیت گیرنده و فرستنده

	FH (802.11)	DS (802.11)	Irda (802.11)
Min. Time	19 usec	10 usec	Negligible

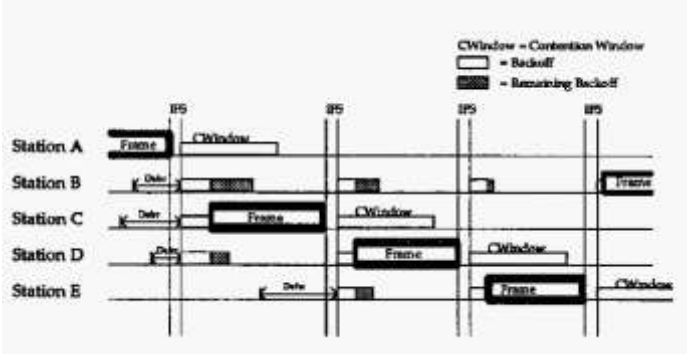
در ادامه به بررسی دقیقتر دو مود کاری:

۱ ۱ ۶ ۹ DCF دسترسی در مود می. PCF, DCF پردازیم.

همانطور که گفته شد ارسال داده ها بصورت آسنکرون است . برای اینکار از روش DCF در روش استفاده شده است که دلیل استفاده از آن این است که فرستنده CSMA/CAxvi تخصیص تصادفی نمی توان از Ethernet نمی تواند در حین فرستادن داده به کانال گوش کند بنابراین مانند استاندارد استفاده کرد CSMA/CDxvii .

روش کار در این مود بدین صورت است که ابتدا هر کاربر کانال را حس می کند اگر خالی بود به مدت می back off time صبر می کند سپس اگر دوباره خالی بود به مقدار زمان تصادفی که به آن DIFS گویند صبر می کند در آخر اگر خالی بود داده را می فرستد و اگر خالی نبود دوباره صبر می کند تا صبر می کند و سپس به اندازه بقیه آن زمان DIFS بعدی را در کانال ببیند و دوباره به اندازه

Ack صبر می کند . این فرایند در شکل زیر که ۵ کاربر در انتظار دسترسی به کانال هستند، back off توضیح داده شده است .

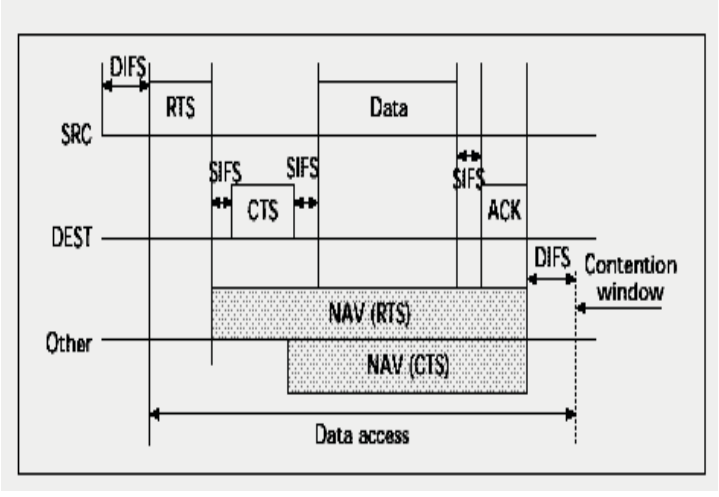


شکل ۹ ۱۳ مراحل کاری در پروتکل DCF

دریافت نمی شود، بنابراین اگر کاربر Ack رخ دهد Collision نکته قابل توجه در این است که اگر را بزرگتر انتخاب می کند و دوباره مراحل اجراء back off دریافت نکرد زمان Ack فرستنده می شود.نکته دیگر وقتی است که داده ها بزرگ باشد و این باعث اشغال بیش از حد کانال می شود. برای حل این مشکل اگر داده ما بزرگتر از مقدار آستانه ای بود آنرا خرد می کنیم و سپس ارسال می کنیم گویند. Fragmentation .به این کار بحث قابل ملاحظه دیگر وقتی است که ۲ کاربر می خواهند با کاربر خاصی ارتباط برقرار کنند در حالیکه این دو همدیگر را نمی بینند و پیغام های ارسالی در کانال

یکدیگر را حس نمی کنند پس مطمئنا گویند. راه حل این مشکل استفاده Hidden Node Terminal رخ می دهد به این مشکل collision است که پیغام های کوتاهی هستند که کاربر فرستنده و گیرنده می CTSxviii, RTSxix از سیگنالینگ NAV را ببیند دیگر داده ها را در زمان ثابتی بنام RTS, CTS فرستند در این حالت هر کاربری که ارسال نمی کند بنابراین دامنه بزرگتری را پوشش می دهد. نحوه کار در شکل زیر نمایش داده شده است.

است که زمان های کوچکی هستند و RTC, CTS هم رخ دهد در زمان ارسال collision اگر احیانا خیلی کارایی سیستم را خراب نمی کند. البته اگر داده ها کوچک باشند اینکار به صرفه نخواهد بود و طول بسته ارسالی هم فرستاده RTS, CTS را در سیستم زیاد می کند. در حین ارسال Header را بدست می آورد و بعد از اتمام این زمان شروع به NAV می شود که بقیه کاربرها با استفاده از آن می کنند. Ack آشکارکردن

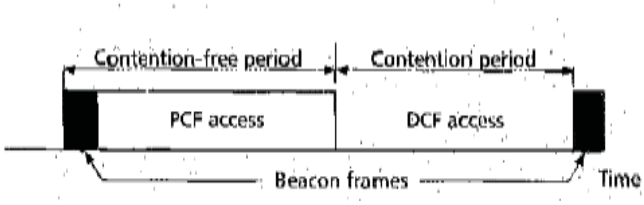


شکل ۹ ۱۴ نحوه ارسال با استفاده از CTS, RTS

۲ ۱ ۶ ۹ PCF دسترسی در مود است و هر سلول Infrastructure حتما سیستم دارای ساختار PCF همانطور که گفته شد در مود است. در استاندارد ۸۰۲,۱۱ داده هایی که حساس به تاخیرهستند را AP دارای یک آنتن مرکزی بنام با AP وارسال سنکرون استفاده کرد. ابتدا PCF هم می توان ارسال کرد. برای اینکار فقط باید از مود تمام کاربران حاضر در سلول خود را لیست می کندتا اگر داده Beacon Frame شروع یک فریم بنام ارسال

کنند و بعد از اتمام این قسمت که به SIFS ای دارند ، بدون اجازه از بقیه با یک فاصله زمانی آغاز می شود. این در شکل زیر نمایش DCF می گویند قسمت ارسال در مود Contention Free آن داده شده است

Beacon



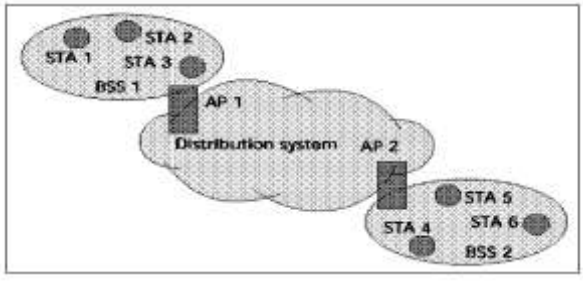
شکل ۹ ۱۵ فریم زمانی شروع شده با نیز چیز ثابتی نیست و قابل تنظیم با Beacon Frame

مدت زمان دو قسمت با تاخیر و بدون آن در معرفی می کند. این کار AP تقاضا است. حال این سوال مطرح می شود که چگونه یک کاربر خود را به به ۲ روش انجام می شود:

شود، ۱- Beacon منتظر دریافت فریم بفرستد.این به عهده سازنده سیستم است که کدام روش را انتخاب ۲- AP خود کاربر یک فریم برای کند.

حال سوال کلی تری پیش می آید که کلا وظایف شبکه ثابت چیست؟

همانطور که گفته شد هدف از ها انجام می شود.از AP افزایش سطح پوشش شبکه است که این کار بوسیله Infrastructure قراردادن می توان شبکه محلی را به شبکه های دیگر متصل ساخت. شکل زیر Bridge طرف دیگر با استفاده از این سیستم گسترده را نشان می دهد



شکل ۹ ۱۶ ساختار شبکه و قرار گرفتن DS

واضح است که شبیه هر سیستم سلولی دیگری، برقراری ارتباط بین کاربران در DS حال وظایف سلولهای متفاوت و نیز امکان حرکت هر

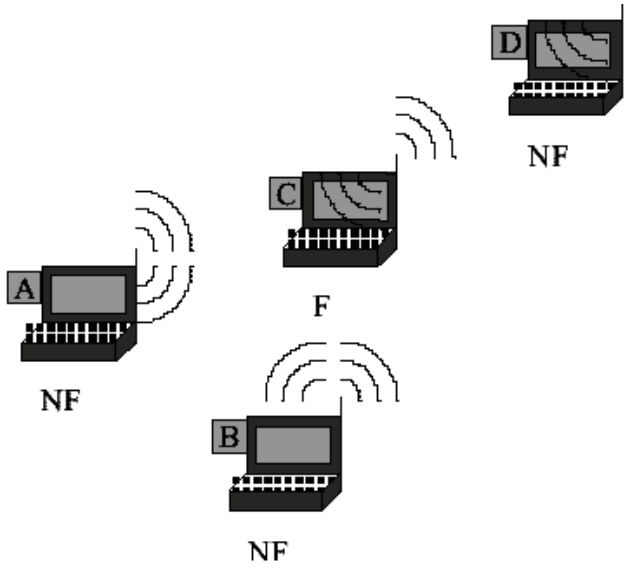
کاربر از یک سلول به سلول دیگر است پس باید قابلیت در استاندارد ۸۰۲,۱۱ مشخص Routing بین سلولها وجود داشته باشد. البته الگوریتم های Routing نشده است و بعهده سازنده سیستم است .

با این حال برای انجام این وظایف بیت های خاصی در هر بسته پیش بینی شده است. HiperLAN/ ۹ ۶ ۲ Header پروتکل لایه دسترسی چندگانه در استاندارد ۱ لایه دسترسی چندگانه این استاندارد مانند استاندارد ۸۰۲,۱۱ قابلیت ارسال سنکرون و آنسکرون را دارد کار می کند و در این مود Ad hoc البته بدون گارانتی برای میزان تاخیر. این استاندارد فقط در ساختار بودن شبکه، برای Ad hoc برخلاف ۸۰۲,۱۱ قابلیت ارسال سنکرون را نیز داراست .

بنابراین با فرض ارسال داده از یک کاربر به کاربر دیگری که مستقیما در دسترس نیست، نیاز به روشی بنام است که در آن یک کاربر واسط داده را برای کاربر مورد نظر می فرستد و بعنوان پل Forwarding این در شکل Forwarder عمل می کند. بنابراین تمام نودها به دو دسته تقسیم می شوند :کاربر ساده یا زیر نشان داده شده است

واضح است با توجه به حرکت کاربران توپولوژی شبکه دائما تغییر می کند و تمام کاربران باید این تغییرات را بدانند.

Forwarding



شکل ۹ ۱۷ نحوه دسترسی به کاربر دور با استفاده از Forwarder

بنابر این تمام کاربران برای ارسال به کاربرهای دور یا غیر قابل دسترس باید به نودهای بسپارند. بنابراین همه نودها باید از ناحیه تحت پوشش خود خبر داشته باشند .

این کار بوسیله بسته ۳۰ آنرا می فرستد. لایه های قسمت دسترسی msec انجام می شود که هر کاربر هر Hello ارسالی چندگانه این استاندارد شامل ۲ قسمت است کردن را به عهده دارد و Routing این قسمت وظیفه رساندن بسته ها به کاربر دلخواه یا : MACxx و جمع آوری اطلاعات از بقیه کاربرها را دارد. Forwarding نیزوظیفه این قسمت وظیفه اختصاص کانال به بسته و کاربر با اولویت بالاتر را دارد. همانطور که :CACxxi گفته شد این استاندارد قابلیت ارسال سنکرون و آنسکرون را داراست .

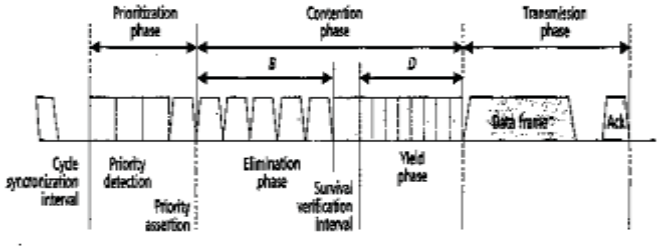
این کار بوسیله نسبت دادن ارجحیتهای مختلف به هر بسته انجام می شود همچنین هر بسته یک طول عمر دارد که با نزدیک شدن ها نیز ارجحیت بسته بالاتر می رود. Hop به صفر ، ارجحیت آن بیشتر می شود . البته با توجه به تعداد در این استاندارد نحوه ارجحیت دادن بین بسته ها بسیار پیچیده تر از استاندارد ۸۰۲,۱۱ است و شامل ۳ قسمت متوالی است:

Priority Resolution
Elimination
Yield Phase

بازه p+ که بین صفر تا چهار است تا ۱ (p) ابتدا هر نود بعد از اتمام ارسال با توجه به ارجحیت خود می فرستد بعد از این priority assertation زمانی می ایستد اگر کانال خالی بود یک بسته بنام بازه w انتخاب می کنند و در w قسمت، تمام بسته های هم ارجحیت یک عدد تصادفی بین صفر و زمانی آنرا به کانال ارسال می کند.

هر کدام از کاربران که بعد از اتمام ارسال به کانال گوش داد و خالی می رود در این مرحله دوباره عدد تصادفی انتخاب می شود و هر کدام که تاآن Yeild بود به مرحله هر بسته که Yeild عدد صبر کردند و کانال خالی بود شروع به فرستادن می کنند. در واقع در قسمت است.

در شکل زیر مراحل Elimination تاخیر کوچکتری دارد موفقتر است و این بر عکس مرحله این کار توضیح داده شده است



شکل ۹ ۱۸ مراحل ارجحیت یابی برای دسترسی به کانال

نتیجه‌گیری

شبکه‌های ادهاک موبایل در واقع آینده شبکه‌های بی سیم می‌باشند به دلیل اینکه آنها ارزان، ساده، انعطاف‌پذیر و استفاده آسانی دارند. ما در جهانی زندگی می‌کنیم که شبکه‌ها در آن پیوسته تغییر می‌کنند

و توپولوژی خودشان را برای اتصال نودهای جدید تغییر می‌دهند به همین دلیل ما به سمت این شبکه‌ها می‌رویم.

علی‌رغم مشکلات امنیتی که دارند کاربردهای زیادی دارند در واقع روز به روز بر کارآیی آنها افزوده شده و از قیمتشان کاسته می‌شود به همین دلیل در بازار طرفداران زیادی دارند.

پایان

.... مهندس رضا خواجوند خزایی در سال ۱۳۵۲ در یکی از مناطق روستائی در شهرستان نوشهر (شهر زیبای بندری و دارای جاذبه ها فراوان گردشگری واقع در استان مازندران است) بدنیا آمد. او در شرایط سخت محیطی و کارگری رشد کرد و در سالهائی که هنوز یک نوجوان به حساب می آمد، از خانواده پدری جدا، و در پائین ترین سطح مالی، وارد بازار کار شد و پس از چند سال کارگری و دستفروشی، از سال ۱۳۶۹ به استخدام ارتش جمهوری اسلامی ایرن درآمد. در زمان خدمتش در ارتش، با اکثر قریب به اتفاق اقوام ایرانی و برخی اقوام همسایه، از نزدیک آشنا شد و در طول سالها، درد و رنج مردم ایران زمین را با تمام وجود لمس نمود و با آنها زندگی کرد. او در سالهای خدمتش، و در حین انجام ماموریتهای محوله، چندین بار دچار سانحه شد و نهایتاً بدلیل همان جراحات، ادامه خدمت در ارتش برایش مقدور نبود و بهمین دلیل در سال ۱۳۹۱ از ارتش بازنشسته شد و به محض رهائی از خدمت وارد دانشگاه گردید و پس از تحصیل در رشته برنامه نویسی کامپیوتر، با درجه مهندسی، از دانشگاه فنی مازندران فارغ التحصیل گردید. مهندس خزایی همزمان با خدمت در ارتش و همچنین در زمان دانشجوئی و پس از آن دست به گردآوری و نگارش مطالبی مرتبط با رشته تحصیلی و تخصصش، و همچنین مطالب مورد علاقه و داستان نویسی زد و بنا به دلایل شخصی تا سال ۱۳۹۸ از انتشار عمومی نوشته هایش خودداری کرد. اما در سال ۱۳۹۸ شروع به انتشار عمومی دستنوشته ها و مطالب گردآوری شده نمود که این کتاب یکی از اولین کتب منتشرشده او بصورت عمومی است.

بهاء ۴۵۰۰۰۰ ریال