آموزشگده فنی و حرفه‌ای شهید بهشتی کرج

عنوان:

مسیریابی پیازی در شبکه‌های تور

پژوهش‌گر:

مهدی بیات ترک

استاد راهنما:

آقای میلاد رحمانی نوده

بهار۹۴

تقدیم به:

همه افرادی که ما را در تهیه این پایان نامه یاری کرداند و این پایان نامه رو به مادر و پدر گلم و تمام دوستانم که با همه سختی ها ما را یاری کرده‌اند و به استادم جناب آقای میلاد رحمانی که من را در جمع آوری و پی‌ریزی این پایان نامه کمک کردند.

چکیده

اینترنت امروزی بی‌شک بزرگترین سیتم مهندسی ساخته شده توسط انسان تا به امروز است که شامل صدها میلیون کامپیوتر متصل به هم،پیوندهای ارتباطی و سوئیچ‌ها می‌باشد.صدها میلیون کاربر به صورت متناوب از طریق تلفن های همراه، *PDA* و تلفن های هوشمند به این شبکه متصل می‌شوند و تجهیزاتی مثل حسگرها، دوربین‌های مخصوص وب، کنسول های بازی،قاب‌های عکس و حتی ماشین‌های لباسشویی به اینترنت متصل شده‌اند. و برای برقراری ارتباط بین این شبکه‌ها نیازمند به یک ستون فقرات می باشیم، این شبکه زیر بنایی که از تعداد زیادی مسیریاب تشکیل شده است وظیفه انتقال اطلاعات را دارد.بر روی این مسیریاب ها باید الگوریتم‌های اجرا شوند تا بتوانند بهترین مسیر را برای انتقال اطلاعات در این دهکده را انتخاب کنند. بنده سعی دارم در این پایان نامه به شکلی مسیریاب‌ها را مورد برسی قرار دهم و در فصل اول کلیاتی درباره شبکه‌های کامپیوتری و اینترنت ارائه می‌دهم. در این فصل هدف من ترسیم تصویر گسترده‌ای است تا با شناخت اجزای شبکه، کل شبکه را بتوان درک کرد.در این فصل ما اجزای گوناگون یک شبکه کامپیوتری را مورد برسی قرار می‌دهیم این فصل زیربنای برای فصل های بعد است، بعد از بیان کلیات درباره شبکه ما به توصیف تحلیل مسیریاب‌ها می‌پرازیم و در فصل آخر به تحلیل و تجزیه مسیریابی پیازی می‌پردازیم و الگوریتم مسیریابی پیازی رو مورد برسی قرار می‌دهیم.

کلمات کلیدی: مسیر یابی ها،شبکه،پرتوکل،شبکه های تور،مسیریابی پیازی، اینترنت

فهرست مطالب

مقدمه

فصل ۱ مفاهیم کلی شبکه‌های اینترنت *6*

*1-*۱ مقدمه *6*

۱-۲ تعریف شبکه کامپیوتری *7*

۱-۳ انواع شبکه کامپیوتری *7*

۱-۳-۱ انواع شبکه کامپیوتری از نظر اندازه *7*

۱-۳-۲ انواع شبکه کامپیوتری از نظر تکنولوژی سیم کشی *8*

-۳-۳ انواع شبکه کامپیوتری از نظر تکنولوژی بی‌سیم *9*

۱- ۴ پروتکل *9*

۱-۴-۱ تعریف پروتکل *10*

۱-۴-۲ انواع پروتکل *10*

فصل ۲ لایه شبکه ۱۲

۲-۱ مقدمه لایه شبکه *12*

۲-۱-۱ روانه‌سازی و مسیریابی *13*

۲-۲ مسیریاب‌ها *14*

۲-۲-۱ در درون یک مسیر یاب چه چیز های وجود دارد؟ *14*

۲-۳ سوئیچینگ *15*

۲-۴ الگوریتم‌های مسیریابی *16*

۲-۴-۱ انواع الگوریتم های مسیریاب *16*

فصل ۳ مسیر یابی پیازی *23*

۳-۱ سامانه *tor* *23*

۳-۲ مسیریابی پیازی *23*

۳-۴ طرز کار مسیریابی پیازی 25
۳-۲ الگوریتم مسیریابی پیازی در TOR 26
۳-۷ حملات Tor و ازبین رفتن گمنامی کاربران 31
۳-۸ نتیجه‌گیری 34
۳-۹ منابع 35

فهرست اشکال

شکل۱-۱ طرز کار 10

شکل۲-۱ مسیریاب 13

شکل ۲-۲ مسیریاب *AS* 18

شکل۲-۳ *IGP* 19

شکل۳-۱ روش‌کار۱ 24

شکل۳-۲ روش‌کار۲ 24

شکل۳-۳ *CODING*۱ 25

شکل۳-۴ *CODING*۲ 25

شکل۳-۵ *PROXY* 26

شکل۳-۶ پیدا کردن نود 26

شکل۳-۷ انتخاب مسیر 27

شکل۳-۸ انتخاب متفاوت 27

شکل۳-۸ *DB-PACK*۱ 28

شکل۳-۸ *DB-PACK*۲ 28

شکل۳-۸ *DB-PACK*۳ 29

شکل۳-۸ *DB-PACK*۴ 29

شکل۳-۸ *DB-PACK*۵ 30

شکل۳-۸ اطلاعات *TOR* 30

شکل۳-۸ روند ایجاد جریان 30

شکل۳-۸ *CELL* 31

شکل۳-۸ طرح حمله 32

مقدمه

این پایان‌نامه برای دانشجویانی که به زمینه‌های شبکه کامپیوتر علاقه دارند نوشته شده است.شبکه‌های کامپیوتری بحثی بسیار پیچیده است و شامل مفاهیم، پروتکل‌ها و فناوری‌هایی است که به نحوی پیچیده با یکدیگر در ارتباط هستند.

و سعی دارم در این پایان نامه به شکلی مسیریاب‌ها را مورد برسی قرار دهم و در فصل اول کلیاتی درباره شبکه‌های کامپیوتری و اینترنت ارائه می‌دهم. در این فصل هدف من ترسیم تصویر گسترده‌ای است تا با شناخت اجزای شبکه، کل شبکه را بتوان درک کرد.در این فصل ما اجزای گوناگون یک شبکه کامپیوتری را مورد برسی قرار می‌دهیم این فصل زیربنای برای فصل های بعد است، بعد از بیان کلیات درباره شبکه ما به توصیف تحلیل مسیریاب‌ها می‌پرازیم و در این فصل مفاهیم پیچیده لایه شبکه مثل مسیریاب‌ها و سوئیچ‌ها و تحلیل الگوریتم‌ها می‌پردازیم و در فصل آخر به تحلیل و تجزیه مسیریابی پیازی می‌پردازیم و الگوریتم مسیریابی پیازی رو مورد برسی قرار می‌دهیم.

فصل اول

مفاهیم کلی شبکه‌های اینترنت

اینترنت یک شبکه کامپیوتری است که میلیون‌ها وسیله محاسباتی در سراسر جهان را به هم متصل می‌کند. این تجهیزات محاسباتی تا سال‌های نه چندان دور شامل کامپیوترهای رومیزی، ایستگاه‌های کاری با سیستم عامل *Linux* و سرویس دهنده‌ها دخیره و انتقال اطلاعات از قبیل صفحات وب و پیام‌های الکترونیکی بودند. رفته رفته تجهیزات دیگری مانند سیستم‌های انتهایی جدید اینترنتی مانند *PDA* (همکار دیجیتال شخصی)،تلویزیون‌ها، کامپیوترهای قابل حمل،تلفن‌های همراه، دوربین‌های وب، اتومبیل‌ها،حسگرهای محیط، قالب‌های عکس و سیستم‌های امنیتی و الکتریکی خانگی در حال اتصال به اینترنت هستند. در واقع عبارت شبکه کامپیوتری با روی کارآمدن تجهیزات غیرمتعارف متصل به اینترنت، کمی قدیمی شده است. در فرهنگ اصطلاحات اینترنت، کلیه این تجهیزات، میزبان‌ها یا سیستم‌های انتهایی نامیده می‌شوند. سیتم‌های انتهایی از طریق شبکه‌ای از پیوندهای ارتباطی و سوئیچ‌های بسته‌ای به یک دیگر متصل می‌شوند.پیوندهای ارتباطی متفاوت،داده‌ها را با نرخ‌های متفاوتی انتقال می‌دهند که این نرخ انتقال با واحد بیت برثانیه اندازه‌گیری می‌شود.

یک سوئیچ بسته، بسته رسیده به یکی از پیوندهای ارتباطی ورودی خود را دریافت کرده و آنرا روی یکی از پیوندهای ارتباطی خورجی خود هدایت می‌کند.سوئیچ‌های بسته‌ای، در شکل‌ها و انواع مختلفی وجود دارند، ولی دو نمونه ازپرکاربردترین آنها در اینترنت کنونی، مسیریاب‌ها و سوئیچ‌های لایه پیوند هستند. سوئیچ های لایه پیوند معمولا در شبکه‌های دسترسی استفاده می‌شوند، در صورتی که مسیریاب‌ها معمولا در هسته شبکه استفاده می‌شوند

۱-۱ مقدمه

در یک کاربرد شبکه سیستم‌های انتهایی بسته‌ها را بین یکدیگر تبادل می کنند. پیام‌ها حاوی تمام آنچه طراح کاربرد می‌خواهد می‌باشند. پیام‌ها می‌توانند حاوی بسته‌های کنترلی و یا حاوی بسته‌های داده همچون نامه الکترونیکی،تصویر و یا یک فایل صوتی باشند. ما در این فصل به توضیح کامل شبکه و مفاهیم ان می‌پردازییم تا به به حال با طرز کل کار آشنا شدیم.

۱-۲ تعریف شبکه کامپیوتری

به عبارتی شبکه‌های کامپیوتری مجموعه‌ای از کامپیوترهای مستقل متصل به یکدیگرند که با یکدیگر ارتباط داشته و تبادل داده می‌کنند. مستقل بودن کامپیوترها بدین معناست که هر کدام دارای واحدهای کنترلی و پردازشی مجزا بوده و بود و نبود یکی بر دیگری تاثیرگذار نیست.

متصل بودن کامپیوترها یعنی از طریق یک رسانه فیزیکی مانند کابل، فیبر نوری، ماهواره‌ها و... به هم وصل می‌باشند. دو شرط فوق شروط لازم برای ایجاد یک شبکه کامپیوتری می‌باشند اما شرط کافی برای تشکیل یک شبکه کامپیوتری داشتن ارتباط و تبادل داده بین کامپیوترهاست. این موضوع در بین متخصصین قلمرو شبکه مورد بحث است که آیا دو رایانه که با استفاده از نوعی از رسانه ارتباطی به یکدیگر متصل شده‌اند تشکیل یک شبکه می‌دهند. در این باره بعضی مطالعات می‌گویند که یک شبکه نیازمند دست کم ۳ رایانه متصل به هم است. یکی از این منابع با عنوان «ارتباطات راه دور: واژه‌نامه اصطلاحات ارتباطات راه دور»، یک شبکه رایانه‌ای را این طور تعریف می‌کند: «شبکه‌ای از گره‌های پردازشگر دیتا که جهت ارتباطات دیتا به یکدیگر متصل شده‌اند». در همین سند عبارت «شبکه» این طور تعریف شده‌است: «اتصال سه با چند نهاد ارتباطی» رایانه‌ای که به وسیله‌ای غیر رایانه‌ای متصل شده‌است (به عنوان نمونه از طریق ارتباط اترنت به یک پرینتر متصل شده‌است) ممکن است که یک شبکه رایانه‌ای به حساب آید، اگرچه این نوشتار به این نوع پیکربندی نمی‌پردازد.

۱-۳ انواع شبکه کامپیوتری

انواع شبکه های کامپیوتری را می‌توان به بخش های زیر تقسیم کرد: بر اساس نوع اتصال، بر اساس تکنولوژی سیم کشی،بر اساس تکنولوژی بی سیم، بر اساس اندازه، بر اساس لایه شبکه، بر اساس معماری کاربری، بر اساس همبندی و بر اساس قرارداد، که ما به توضیح بخشی مهم از آن‌ها در این پایان نامه می‌پردازیم.

۱-۳-۱ انواع شبکه کامپیوتری از نظر اندازه

۱-شبکه شخصی (*PAN*): «شبکه شخصی» (*Personal Area Network*) یک «شبکه رایانه‌ای» است که برای ارتباطات میان وسایل رایانه‌ای که اطراف یک فرد می‌باشند بکار می‌رود. این که این وسایل ممکن است متعلق به آن فرد باشند یا خیر جای بحث خود را دارد. برد یک شبکه شخصی عموماً چند متر بیشتر نیست. **۲- شبکه محلی (*LAN*)**: «شبکه محلی» (*Local Area Network*) یک «شبکه رایانه‌ای» است که محدوده جغرافیایی کوچکی مانند یک خانه، یک دفتر کار یا گروهی از ساختمان‌ها را پوشش می‌دهد. **۳- شبکه کلان‌شهری (*MAN*)**: «شبکه کلان‌شهری» (*Metropolitan Area Network*) یک «شبکه رایانه‌ای» بزرگ است که معمولاً در سطح یک شهر گسترده می‌شود. **۴-**

شبکه گسترده (*WAN*): «شبکه گسترده» (*Wide Area Network*) یک «شبکه رایانه‌ای» است که نسبتاً ناحیه جغرافیایی وسیعی را پوشش می‌دهد (برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قاره‌ای دیگر). این شبکه‌ها معمولاً از امکانات انتقال خدمات دهندگان عمومی مانند شرکت‌های مخابرات استفاده می‌کند. به عبارت کمتر رسمی این شبکه‌ها از مسیر یاب ها و لینک‌های ارتباطی عمومی استفاده می‌کنند.

۱-۳-۲ انواع شبکه کامپیوتری از نظر تکنولوژی سیم کشی

زوج به هم تابید: زوج به‌هم‌تابیده یکی از بهترین رسانه‌های مورد استفاده برای ارتباطات راه دور می‌باشد. سیم‌های زوج به‌هم‌تابیده، سیم تلفن معمولی هستند که از دو سیم مسی عایق که دو به دو به هم پیچ خورده‌اند درست شده‌اند. از زوج به‌هم‌تابیده برای انتقال صدا و داده‌ها استفاده می‌شود. استفاده از دو سیم به‌هم‌تابیده به کاهش تداخل و القای الکترومغناطیسی کمک می‌کند. سرعت انتقال داده، دامنه‌ای از ۲ میلیون بیت درهر ثانیه تا ۱۰۰ میلیون بیت در هر ثانیه، دارد.

کابل هم محور: کابل هم‌محور به طور گسترده‌ای در سیستم‌های تلویزیون کابلی، ساختمان‌های اداری، و دیگر سایت‌های کاری برای شبکه‌های محلی، استفاده می‌شود .کابل‌ها یک رسانای داخلی دارند که توسط یک عایق منعطف محصور شده‌اند، که روی این لایه منعطف نیز توسط یک رسانای نازک برای انعطاف کابل، به هم بافته شده‌است .همه این اجزا، در داخل عایق دیگری جاسازی شده‌اند. لایه عایق به حداقل رساندن تداخل و اعوجاج کمک می‌کند. سرعت انتقال داده، دامنه‌ای از ۲۰۰ میلیون تا بیش از ۵۰۰ میلیون بیت در هر ثانیه دارد.

فیبر نوری: کابل فیبر نوری شامل یک یا چند رشته از الیاف شیشه‌ای پیچیده شده در لایه‌های محافظ می‌باشد. این کابل می‌تواند نور را تا مسافت‌های طولانی انتقال دهد. کابل‌های فیبر نوری تحت تاثیر تابش‌های الکترومغناطیسی قرار نمی‌گیرند. سرعت انتقال ممکن است به چند تریلیون بیت در ثانیه برسد.

۱-۳-۳ انواع شبکه کامپیوتری از نظر تکنولوژی بی‌سیم

ریزموج زمینی: ریزموج‌های زمینی از گیرنده‌ها و فرستنده‌های زمینی استفاده می‌کنند. تجهیزات این تکنولوژی شبیه به دیش‌های ماهواره‌است. مایکروویو زمینی از دامنه‌های کوتاه گیگاهرتز استفاده می‌کند، که این سبب می‌شود تمام ارتباطات به صورت دید خطی محدود باشد. فاصله بین

ایستگاه‌های رله (تقویت سیگنال) حدود ۳۰ مایل است. آنتن‌های ریزموج معمولاً در بالای ساختمان‌ها، برج‌ها، تپه‌ها و قله کوه نصب می‌شوند.

ماهواره های ارتباطی: ماهواره‌ها از ریزموج‌های رادیویی که توسط جو زمین منحرف نمی‌شوند، به عنوان رسانه مخابراتی خود استفاده می‌کنند.

ماهواره‌ها در فضا مستقر هستند؛ به طور معمول ۲۲۰۰۰ مایل برای ماهواره‌های *(geosynchronous)* بالاتر از خط استوا. این سیستم‌های در حال چرخش به دور زمین، قادر به دریافت و رله صدا، داده‌ها و سیگنال‌های تلویزیونی هستند.

تلفن همراه و سیستم‌های پی سی اس: تلفن همراه و سیستم‌های پی سی اس از چندین فناوری ارتباطات رادیویی استفاده می‌کنند. این سیستم‌ها به مناطق مختلف جغرافیایی تقسیم شده‌اند. هر منطقه دارای فرستنده‌های کم قدرت و یا دستگاه‌های رله رادیویی آنتن برای تقویت تماس‌ها از یک منطقه به منطقه بعدی است.

شبکه‌های محلی بی سیم: شبکه محلی بی سیم از یک تکنولوژی رادیویی فرکانس بالا (مشابه سلول دیجیتالی) و یک تکنولوژی رادیویی فرکانس پایین استفاده می‌کند. شبکه‌های محلی بی سیم از تکنولوژِی طیف گسترده، برای برقراری ارتباط میان دستگاه‌های متعدد در یک منطقه محدود، استفاده می‌کنند. نمونه‌ای از استاندارد تکنولوژی بی سیم موج رادیویی، *IEEE*است.

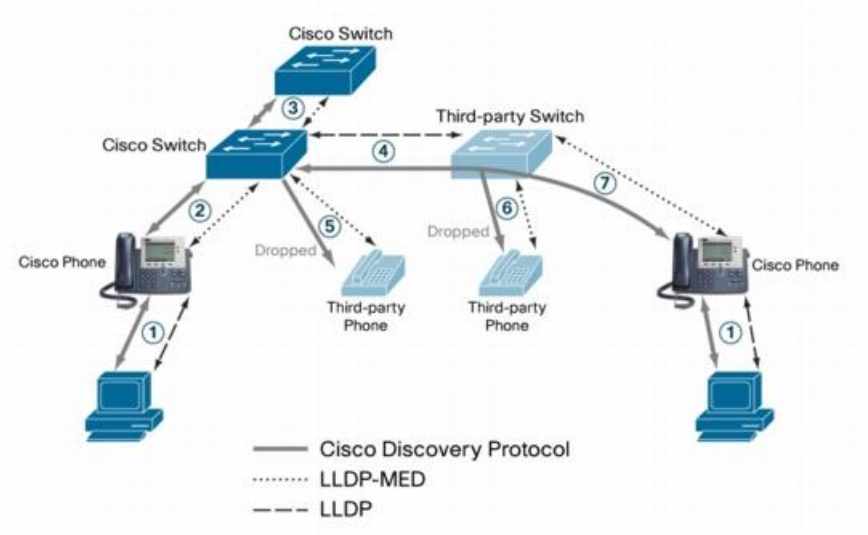
۱- ۴ پروتکل

یک پروتکل شبکه مشابه پروتکلی از نوع انسانی است. با این تفاوت که موجودیت‌های مبادله کننده پیام و عمل کننده، اجزای نرم‌افزاری یا سخت‌افزاری برخی از تجهیزات (مانند کامپیوتر، *PDA*، تلفن همراه، مسیریاب یا وسایل دیگری با قابلیت شبکه شدن) هستند. کلیه فعالیت‌های که در اینترنت توسط دو یا تعدادی بیشتری موجودیت ارتباطی دور از هم انجام می‌گیرند با استفاده و تحت کنترل یک پروتکل انجام می‌شود. مثلا پروتکل های که به صورت سخت‌افزاری در کارت‌های شبکه دو کامپیوتر پیاده‌سازی شده‌اند که این دو کامپیوتر به صورت فیزیکی به هم متصل‌اند، جریان بیتی درون سیم‌های واقع در بین آن دو کارت شبکه را تحت کنترل دارند. پروتکل ها کنترل ازدحام واقع در سیستم انتهایی، نرخ ارسال بسته‌ها میان فرستنده و گیرنده را کنترل می‌کنند.پروتکل‌های درون مسیریاب‌ها، مسیر بسته از مبداتا مقصد را مشخص می‌کنند.

۱-۴-۱ تعریف پروتکل

یک **پروتکل،** قالب وترتیب پیام‌های مبادله شونده بین دو یا تعدادی بیشتر از موجودیت‌های ارتباطی و اعمالی که بایستی در هنگام انتقال یا دریافت پیام یا رویدادهای دیگر انجام گیرند را تعریف می کند.

به عبارتی مجموعه قوانین لازم به منظور مبادله اطلاعات بین کامپیوترهای موجود در یک شبکه را مشخص می‌نماید. اکثر شبکه‌ها از "اترنت" استفاده می نمایند.اینترنت و بطورکلی شبکه‌های کامپیوتری استفاده گسترده‌ای از پروتکل‌ها می‌کنند. پروتکل‌های مختلفی برای انجام ارتباطات مختلفی استفاده می‌گردند.



(شکل ۱-۱)طرز کار

۱-۴-۲ انواع پروتکل

پروتکل های مختلفی برای انجام کارهای مختلفی وجود دارد که معروف‌ترین آنها عبارت‌اند از *TCP* و *UDP* و *DNS* و*IP*

TCP: این پروتکل انتقال مطمئن داده ها را فراهم می‌کند. *UDP* یک پروتکل انتقال سبک ودارای کیفیت معمولی است که سرویس حداقلی را ارئه می‌دهد.*DNS* یک پروتکل در شبکه است که وظیفه تبدیل نام به *IP* و بلعکس را دارد. و*IP* پروتکل اینترنت است

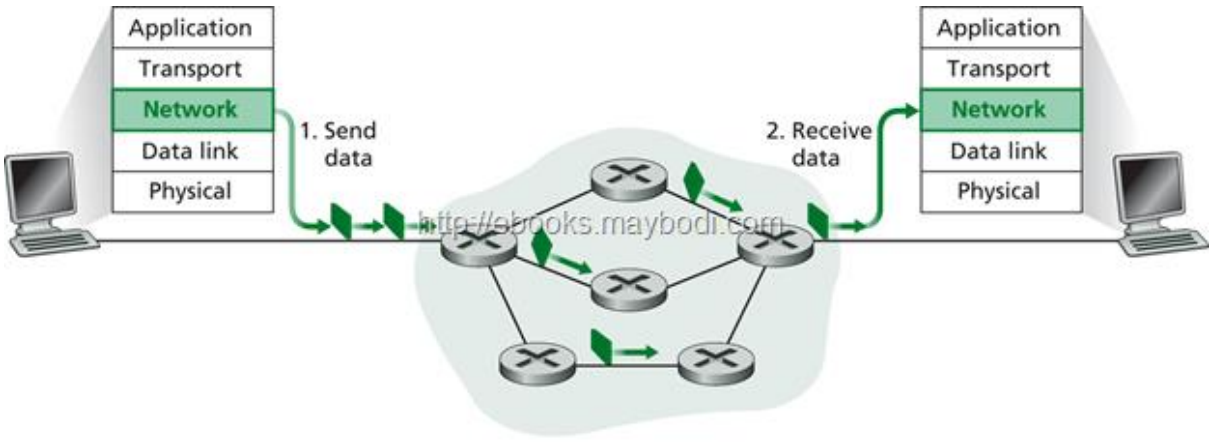
فصل دوم

۲-لایه شبکه

در این فصل یک تمایز مهم بین کارکردهای روانه‌سازی(*Forwarding*) و مسیریابی(*Routing*) در لایه شبکه قائل خواهیم شد. روانه سازی، شامل انتقال یک بسته از یک پیوند ورودی به یک پیوند خورجی در یک مسیریاب واحد می‌باشد. مسیریابی شامل تمام مسیریاب‌های یک شبکه می‌باشد که تعامل دسته جمعی آنها از طریق پروتکل‌های مسیریابی،مسیری را که بسته‌ها از مبدا تا گره مقصد طی می‌کنند تعیین می‌کند. این یک تمایز مهم است که درطول این فصل باید به خاطر داشته باشید. خواهیم دید که کار یک الگوریتم مسیریابی این است که مسیرهای مناسب را از فرستنده‌ها به گیرنده‌ها را تعیین کند

۲-۱ مقدمه

شکل ۲-۱ یک شبکه ساده با دو میزبان و تعدادی مسیریاب است که مسیرهای بین دو میزبان را مشخص می‌کند. لایه شبکه در میزبان اول قطعات را از لایه انتقال در میزبان اول گرفته، هر قطعه را در یک دیتاگرام کپسوله‌سازی کرده وسپس دیتاگرام‌ها را به مسیریاب نزدیک خودش است ارسال می‌کند. در میزبان گیرنده(۲) لایه شبکه دیتاگرام‌ها را از مسیریاب که نزدیک خودش است دریافت کرده، قطعات لایه انتقال را استخراج کرده و قطعات را به لایه انتقال میزبان گیرند(۲) تحویل می‌دهد. نقش اصلی مسیریاب این است که دیتاگرام را از پیوندهای ورودی به پیوندهای خورجی روانه کنند.



(شکل ۲-۱)مسیریاب

۲-۱-۱ روانه‌سازی و مسیریابی

بنابراین نقش لایه شبکه این است که به نحو گول‌زننده‌ای ساده باشد تا بسته‌ها را از یک میزبان فرستنده به یک میزبان گیرنده منتقل کند. برای انجام این کار، می‌توان دو کارکرد مهم لایه شبکه را شناسایی کرد:

- روانه سازی،وقتی بسته‌ای به پیوند ورودی یک مسیریاب می‌رسد، مسیریاب باید بسته را به پیوند خورجی مناسب منتقل کند. به عنوان مثال، بسته‌ای که از میزبان فرستنده(اول) به مسیریاب نزدیک خودش می‌رسد باید در طی مسیر به گیرنده(میزبان ۲) به مسیریاب بعدی ارسال شود
- مسیریابی، لایه شبکه باید مسیری را که بسته‌ها از فرستنده به گیرنده طی می‌کنند تعیین کند. الگوریتم هایی که‌این مسیرها را محاسبه می‌کنند، الگوریتم‌های مسیریابی می‌باشند.

واژه‌های روانه سازی و مسیریابی اغلب توسط مسیریاب‌های که لایه شبکه را برسی می‌کنند به جای یکدیگر به کار می‌روند. روانه‌سازی،به اقدام محلی مسیریاب در مورد ارسال بسته از یک واسط پیوند ورودی به واسط پیوند خروجی مناسب اشاره دارد.مسیر یابی، به فرایند شبکه گسترده اشاره دارد که مسیرهای *end-to-end* را که بسته‌ها از مبدا به مقصد اختیار می‌کنند تعیین می‌کند.

هر مسیریاب دارای یک جدول روانه‌سازی است. یک مسیریاب، با بررسی مقدار یک فیلد درسرآیند بسته ورودی، یک بسته را روانه‌سازی می‌کند.

۲-۲ مسیریاب‌ها

مقدمه: برای برقراری ارتباط بین یک مبدائ و مقصد،به مکانیزمی نیاز است تا اهداف اساسی هر پروتکل مسیریابی محقق گردد.این اهداف عبارتند از: ۱: بیشینه ساختن کارایی شبکه۲: کمینه کردن هزینه شبکه با توجه به ظرفیت آن

سیکل مسیریابی به شرح زیر میباشد:

تولید مسیر: مسیرها را مطابق با اطلاعات جمع آوری و توزیع شده از وضعیت شبکه تولید میکند. انتخاب مسیر: مسیرهای مناسب را بر اساس اطلاعات وضعیت شبکه انتخاب می کند. ارسال داده به جلو: ترافیک کاربر را در امتداد مسیر انتخاب شده به جلو ارسال می کند. نگهداری مسیر: که مسئول نگهداری مسیر انتخاب شده می باشد

تعریف مسیر یابی: مکانیزمی است که به وسیله آن ترافیک کاربر به صورت مستقیم یا با واسطه از مبدا به مقصد هدایت شود و مسیریابها تجهیزاتی هستند که این عمل را انجام میدهند.

پارامترهای مسیر یابی: تعداد گام، تاخیر، توان عملیاتی، نرخ ریزش، استحکام و هزینه و...

۲-۲-۱ در درون یک مسیر یاب چه چیز های وجود دارد؟

- پورت‌های ورودی.یک پورت ورودی،کارکردهای کلیدی مختلفی را اجرا می‌کند. کارکرد لایه فیزیکی، دریافت بیت‌های داده از یک پیوند فیزیکی ورودی به یک مسیریاب، درپورت ورودی اجرا می‌شود
- فابریک سوئیچینگ. فابریک سوئیچینگ، پورت‌های ورودی مسیریاب را به پورت‌های ورودی مسیریاب را به پورت‌های خورجی آن وصل می‌کند. این فابریک سوئیچینگ به طور کامل درون مسیریاب قرار دارد.
- پورت خورجی. یک پورت خورجی،بسته‌های دریافتی از فابریک سوئیچینگ را ذخیره کرده و این بسته‌ها را با انجام عملیات مورد نیاز مربوط به لایه پیوند داده و لایه فیزیکی، به پیوند خروجی ارسال می‌کند
- پردازنده مسیریابی. پردازنده مسیریابی، پروتکل های مسیریابی را اجرا می‌کند،جداول مسیریابی و اطلاعات وضعیت پیوند را نگه می‌دارد و جدول روانه‌سازی مسیریاب را محاسبه می‌کند.

۲-۳ سوئیچینگ

فابریک سوئیچینگ در قلب یک مسیریاب قرار دارد و بسته‌ها در واقع از طریق این فابریک از یک پورت ورودی به یک پورت خورجی سوئیچ می‌شوند سوئیچینگ را می‌توان با چند روش انجام داد:

- سوئیچینگ از طریق حافظه. ساده ترین و ابتدایی‌ترین مسیریاب‌ها، کامپیوترهای قدیمی بودند که در آنها سوئیچینگ بین پورت‌های ورودی و خروجی در یک سیتم عامل رایج به عنوان دستگاه‌های I/O رایج عمل می‌کردند. وقتی یک بسته به یک پورت ورودی وارد می شود، پورت ورودی ابتدا از طریق یک وقفه به پردازنده مسیریابی علامت می دهد. سپس بسته از پودر ورودی به حافظه پردازنده کپی می شود. پردازنده مسیر یابی آدرس مقصد را از سرآیند استخراج کرده، پورت خروجی مناسب را در جدول روانه سازی جستجو کرده و بسته را به بافرهای پورت خروجی کپی می‌کند.
- سوئیچینگ از طریق یک گذرگاه. در این روش، یک پورت ورودی بدون دخالت پردازنده مسیریابی، یک بسته را مستقیما" به پورت خروجی روی یک گذرگاه اشتراکی ارسال می‌کند. این کار معمولا با زدن یک برجسب بر روی بسته(سرآیند) توسط پورت ورودی(سرآیند)، تا پورت خورجی را که این

بسته به آن ارسال شده است را تعیین کند، و ارسال بسته روی گذرگاه انجام می‌شود. بسته توسط تمام پورت‌های خورجی دریافت می‌شود، ولی فقط پورتی که با برچسب انطباق دارد بسته را نگه خواهد داشت. سپس خروجی دریافت می‌شود، ولی فقط پورتی را که با برچسب انطباق دارد بسته را نگه خواهد داشت.

- سوئیچینگ از طریق یک شبکه میان‌ارتباطی. یک روش برای غلبه بر محدودیت پهنای باند یک گذرگاه واحد و اشترکی، استفاده از یک شبکه بسیار پیچیده میان‌ارتباطی می‌باشد، مانند شبکه‌های که در گذشته برای اتصال داخلی پردازنده‌ها در یک معماری کامپیوتری چندپردازنده به کار رفته است.

۲-۴ الگوریتم‌های مسیریابی

وظیفه اصلی لایه شبکه،مسیریابی و هدایت بسته های داده از ماشین مبدا به ماشین مقصد است. در اکثر زیر شبکه‌ها، بسته‌ها برای طی مسیر خود باید چندین گام (*Hop*) راه بپیمایند.الگوریتمی که این مسیرها را انتخاب میکند و همچنین ساختمان داده مورد استفاده،یکی از زمینه های مهم در طراحی لایه شبکه محسوب میشود.

الگوریتم‌های مسیریابی آن بخش از نرم افزار شبکه هستند که مسئولیت دارند در خصوص خط خروجی یک بسته ورودی که باید بر روی آن ارسال شود تصمیم‌گیری کنند. اگر در داخل یک زیر شبکه از روش دیتاگرام استفاده شده باشد این تصمیم‌گیری باید به ازای هر بسته دریافتی از نو تکرار شود. چرا که در هر لحظه ممکن است بهترین مسیر تغییر کند.اگر زیر شبکه از روش مدار مجازی استفاده کند،تصمیم‌گیری در خصوص مسیرها فقط یکبار آنهم در هنگام تنظیم و ایجاد هر مدار مجازی جدید صورت میگیرد.

ویژگیهای یک الگوریتم مسیریابی: ۱: صحت عملکرد (*correctness*) ۲: سادگی (*simplicity*) ۳: قابلیت تحمل (*Robustness*) ۴: پایداری (*stability*) ۵: مساوات (*Fairness*) ۶: بهینگی (*Optimality*)

۲-۴-۱ انواع الگوریتم های مسیریاب

الگوریتمهای مسیر یابی به دو رده کلی تقسیم بندی میشوند:

۱ ***static routing:*** در این روش یک مسیر از قبل بصورت آفلاین محاسبه شده و در هنگام راه اندازی شبکه درون مسیریابها بارگذاری میشود. به این روال اغلب مسیریابی ایستا گفته میشود

۲ ***dynamic routing:*** در این روش، تصمیم گیری در خصوص مسیریابی بر اساس تغییرات توپولوژی و عموما ترافیک لحظه ای بصورت هوشمند انجام میگیرد.

الگوریتم سیل آسا (*flooding*)

یکی از الگوریتمهای ایستا میباشد. بر اساس آن هر بسته ورودی به یک مسیریاب،بر روی تمام خطوط خروجی (به استثنای خطی که بسته از طریق آن دریافت شده) ارسال میشود این فرایند بوضوح منجر به تولید تعداد بسیار زیادی بسته های تکراری (و در حقیقت بینهایت بسته) خواهد شد مگر آنکه برای خاتمه آن سنجشی صورت گیرد. یکی از معیارهای سنجش قراردادن *Hop Counter* میباشد که در هر گام یک واحد از آن کم میشود

مزایا: در چنین حالتی این تضمین وجود دارد که اولاً هر بسته ی اطلاعاتی به تمام مسیرهای زیر شبکه خواهد رسید، دوما سریعترین الگوریتم مسیر یابی است.

معایب: اگر قاعده بر این باشد که همه ی مسیریابها یک بسته ی نوع فراگیر تمام خروجی های خود ارسال کند ممکن است پس از چند لحظه خودشان آن بسته را دریافت کرده وچون مجددا آنرا روی خروجی های خود ارسال می کنند این عمل تا بینهایت ادامه خواهد یافت.

الگوریتم بردار فاصله (*Distance Vector Routing*)

شبکه های کامپیوتری مدرن، عموما بجای استفاده از روشهای ایستا از روشهای پویا (*Dynamic*) بهره میگیرند.زیرا الگوریتمهای ایستا بار فعلی شبکه را در محاسبات مربوط به بهترین مسیرها دخالت نمیدهند.یکی از دو الگوریتم پویا که از رایجترین روشهای موجود هستند *الگوریتم مسیریابی بردار فاصله* یا (*DVR*) میباشد در این روش هر مسیریاب جدولی را در خود نگه میدارد(به عبارتی یک بردار را) که در ان بهترین فاصله تا هر مسیریاب مقصد (یا بعبارتی کمترین هزینه رسیدن به هر مسیریاب در زیر شبکه) و خطی که برای رسیدن به آن مقصد باید مورد استفاده قرار گیرد درج شده است این جدول با مبادله اطلاعات بین مسیریابهای همسایه، بهنگام سازی میشود

مزایا: مزیت این روش در حجم پردازش کم آن می باشد.

معایب: عیب آن کند بودن انتشار اطلاعات یا به عبارت دیگر عدم همگرایی سریع جداول مسیریابی در هنگام خرابی یک کانال ارتباطی می باشد.، پروتکل‌های *RIP*، *IGRP*،*IIGRP* و *BGP* از *DV* استفاده می‌کنند.

الگوریتم مسیریابی حالت لینک (*Link State Routing*)

دو مشکل اساسی منجر به زوال *DVR* شد:

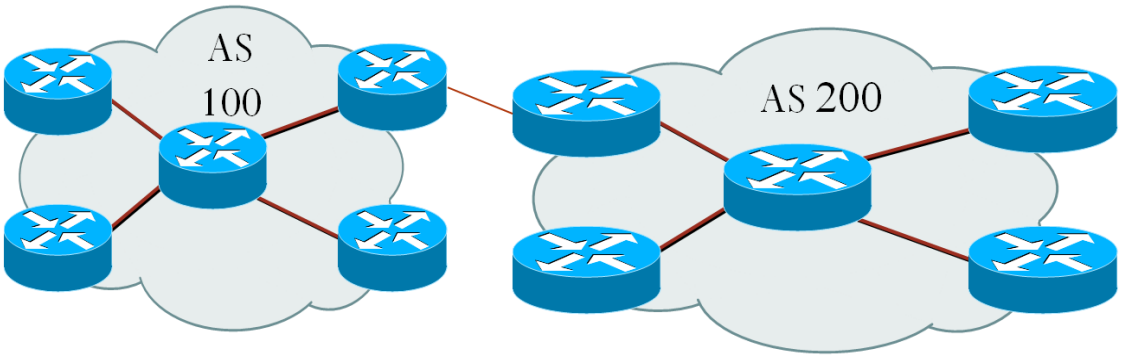
۱: همگرایی بسیار زمانبر ۲: در نظر نگرفتن معیار پهنای باند در محاسبات انتخاب مسیر

بهمین دلایل با الگوریتم جدیدی بنام مسیریابی حالت لینک (*LS*) جایگزین شد ایده اصلی *LS* را میتوان در پنج بند بیان کرد:

۱: همسایه های خود را شناسایی کرده و ادرسهای شبکه آنها را بدست میاورد **۲**: تاخیر یا هزینه هریک از همسایه های خود را اندازه گیری میکند **۳**: بسته ای میسازد و اطلاعاتی که از همسایه ها کسب کرده را در آن جاسازی میکند **۴**: این بسته را برای تمام مسیریابهای دیگر میفرستد **۵**: کوتاهترین مسیر رسیدن به دیگر مسیریابها را محاسبه مینماید بدین ترتیب توپولوژی کامل زیرشبکه و تمام تاخیرها اندازه گیری شده و بین تمام مسیریابها توزیع میشود. پروتکل‌های *IS-IS*،*OSPF* از الگوریتم های *LS* استفاده می کنند.

مسیریابی مختلط (*Hybrid*) این دسته از پرتکلها خصوصیاتی دارند که هم مشابه با پرتکلهای (بردار فاصله) وهم مشابه با پرتوکلهای (حالت لینک) عمل می‌کنند.

شبکه‌های خودمختار(*AS*) یک *AS* شامل گروهی از دستگاه‌هاست که به طور واحد مدیریت می‌شود. این گروه می‌تواند شامل دستگاه‌های موجود در یک کمپانی و یا چند کمپانی باشد. *ISP*ها خود نیز یک *AS* هستند.



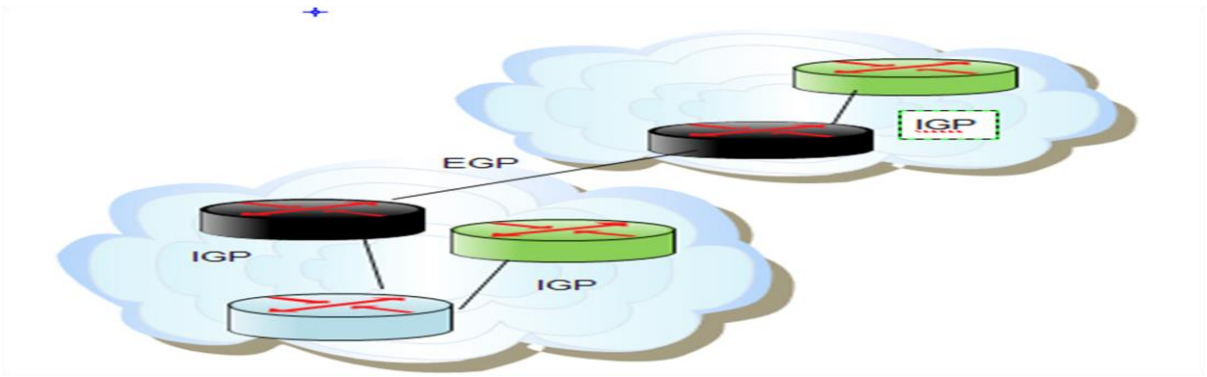
(شکل ۲-۲)مسیریاب *AS*

یک *AS* دارای سیاست‌ها و خط مشی مربوط به خود در مسیریابی است که می تواند با دیگر *AS*ها متفاوت باشد. این *AS* می تواند دارای یک شبکه باشد یا اینکه چندین شبکه که همه این شبکه ها دارای یک مدیر مشترک هستند.

مسیریابی درونی و بیرونی

به مسیریابی روترها در داخل یک *AS*، مسیریابی درونی(*Interior Gateway Protocol*)یا *IGP* گفته می‌شود. برای مسیریابی درونی می توان از پروتکل‌های زیر استفاده کرد*RIP*، *OSPF*، *IS_IS*، *IGRP* ، *EIGRP*

به مسیریابی بین روترهای مرزی *AS*ها که باعث می‌شود اطلاعات بین *AS* ها ردوبدل شود مسیریابی برونی(*EGP*)گویند*BGP* . یک پروتکل مسیریابی برونی است.



شکل(۲-۳)*IGP*

در حال حاضر برای مسیریابی بین *AS* ها در اینترنت یا از *default route* که نوعی مسیریابی ایستا است، استفاده می‌کنیم یا از *BGP*.

پروتکل مسیریابی درونی *RIP*

RIP (برگرفته شده از *Routing Information Protocol*) به معنی واقعی یک پروتکل *distance-vector* است.پروتکل فوق در هر ۳۰ ثانیه تمام اطلاعات موجود در جدول روتینگ را برای تمامی اینترفیسهای فعال ارسال میکند. *RIP* صرفا از تعداد *hop* برای تعیین بهترین مسیر استفاده به شبکه راه دور استفاده میکند حداکثر تعداد *hop* ها میتوتند عدد ۱۵ را داشته باشد و نسبت دهی عددی بالاتر از ۱۵ به منزله غیرقابل دسترس بودن شبکه است *RIP* در شبکه های کوچک به خوبی کار میکند ولی برای شبکه های بزرگ که دارای لینک ارتباطی *WAN* و تعداد بسیار زیادی روتر هستند کند و نامناسب میباشد. در

نسخه شماره یک *RIP*صرفا" از روتینگ *classful* استفاده می گردد. این بدان معنی است که تمامی دستگاه های موجود در شبکه می بایست از *subnet mask*مشابهی استفاده نمایند. محدودیت فوق به دلیل ماهیت ارسال اطلاعات بهنگام می باشد. در نسخه شماره یک *RIP*، اطلاعات بهنگام ارسال شامل اطلاعات *subnet mask*نمی باشند در *RIP* نسخه دو، ویژگی جدیدی به نام روتینگ *Prefix*ارائه شده است که به کمک آن امکان ارسال اطلاعات *subnet mask* به همراه مسیرهای بهنگام شده فراهم می گردد. به این نوع روتینگ، اصطلاحا" روتینگ *classless*گفته می شود.

پروتکل مسیریابی درونی *OSPF*

OSPF مخفف *OPEN SHORTEST FIRST PROTOCOL* می باشد: -دارای سرعت همگرایی بالایی هست. -از ۶ مسیر با هزینه یکسان پشتیبانی می کند. -این پروتکل فقط برای کار با *IP* طراحی شده است-از دسته پروتکل های *LINK STATE* می باشد. -متریک *OSPF* بر اساس پهنای باند می باشد. - پروتکل *OSPF* برای شبکه های بزرگ بوجود آمد لذا این پروتکل شبکه را به قسمت های مختلفی می شکند در واقع این پروتکل برای ساختارهای سلسله مراتبی طراحی شده است. -*OSPF* از *MULTICAST* برای اعلام تغییرات استفاده می کند

پروتکل بیرونی *BGP (exterior)*

پروتکل *BGP* مسئول انتقال اطلاعات و انتخاب بهترین مسیرهای منتهی به مقاصد مختلف در محیط اینترنت می باشند. زمانی که دو *AS* اقدام به برقراری ارتباط با یکدیگر می کنند به طور معمول از *BGP* برای تبادل اطلاعات *routing* استفاده می کنند. در حال حاضر جدیدترین نسخه این پروتکل *BGP*۴ است که این نسخه از ادرس‌دهی *classless* پشتیبانی می کند. این پروتکل برای ردوبدل کردن پیام‌های خود بین روترها از یک اتصال قابل اعتماد استفاده می‌کند برای این کار از پروتکل *TCP* و پورت ۱۷۹ استفاده می‌کند. پروتکل *BGP* یک پروتکل مسیریابی (*path vector protocol*) است بدین معنی که هر روتر اطلاعات کامل مسیر،تا یک مقصد خاص را به روتر همسایه‌ی خود می‌فرستد *BGP* از دو پروتکل مکمل *EBGP* و *IBGP* تشکیل شده است.

BGP*پروتکل مکمل (*IBGP (Interior Border Gateway Protocol

ارسال اطلاعات به سمت اینترنت در شرایطی که تنها یک روتر در مرز بین سازمان و اینترنت قرار دارد کاری بسیار اسان است. در این شرایط کافی است که روتر مرزی یک *default route* را از طریق پروتکل

مسیریابی درونی(*IGP*) برای دیگر دستگاه‌های داخلی ارسال کند تا آن‌ها تمامی پیام‌های مقصد خارجی را برای روتر مرزی بفرستند. اما در صورت استفاده از چندین روتر مختلف برای برقراری ارتباط با اینترنت مسائل مختلفی را باید مد نظر قرار داد. به‌منظور برطرف کردن مشکل احتمالی و همچنین بهره‌گیری از امکانات بیشتر می توان از *IBGP*در بین روترهای مرزی استفاده کرد.

در واقع (*IBGP*) برای این است که مسیریابها مرزی درون یک *AS* بتوانند اطلاعات خود را رد و بدل کنند و به این ترتیب همه مسیریابها از تمام راه های مرزی مطلع هستند و میتوانند بهترین مسیر خروجی را پیدا کنند.

EBGP (Exterior Border Gateway Protocol) پروتکل مکمل BGP

زمانیکه روترهای همسایه در *AS*های جداگانه باشند برای برقراری ارتباط و ردو بدل کردن اطلاعات مسیریابی، از (*EBGP*) استفاده میشود. هریک از *router*های *BGP* از سه جدول برای نگهداری اطلاعات پروتکل *BGP*استفاده می‌کند که این جدول ها به شرح زیر می‌باشند:*Routing table* : شامل اطلاعاتی است که باید طی پیام *Update* مبادله شود. *Neighbor table*: همسایه‌های روتر در این جدول نگهداری می‌شوند. *BGP table*: اطلاعات دریافتی از بقیه مسیریاب‌ها و نیز دیگر *path attribute*ها در این جدول ذخیره می‌شوند.

مسیریابی در شبکه های ویژه(*Routing Ad Hoc Networks*)

تاکنون روشهای مسیریابی در محیطهایی را که ماشینهای میزبان متحرکند ولی مسیریاب‌ها ثابتند را بررسی کرده ایم. یک حالت استثنایی آن است که مسیریابها نیز خودشان متحرک باشند.از چنین محیطهایی میتوان به موارد زیر اشاره کرد: ۱: وسائل نقلیه نظامی در صحنه نبرد بدون دسترسی به هیچگونه زیرساخت ارتباطی ۲: ناوگان دریایی بر روی دریاها ۳: نیروی امداد در شرایط اظطراری مثل سیل زلزله و... که کلیه زیرساختها نابود شده است ۴: گردهمایی افراد با کامپیوترهای کیفی در ناحیه ای بدون شبکه بیسیم ۸۰۲,۱۱

در تمام این موارد هرگره شامل یک مسیریاب و یک ماشین میزبان میباشد که اغلب هردوی آنهابرروی یک ماشین قرار میگیرند.شبکه ای از این گره ها که در کنار هم قرار میگیرند(*MANET*)یا شبکه ویژه نامیده میشوند.

آنچه شبکه های ویژه را از شبکه های سیمی متمایز میسازد آنست که تمام قوائد طبیعی در خصوص توپولوژی ثابت،همسایه های شناخته شده ثابت،تناظر دائم بین موقعیت فیزیکی ماشینها و مواردی از این قبیل در خصوص شبکه ویژه صادق نیست. مسیریابها در رفت وآمد هستند و ممکن است در هر لحظه از محل جدید سر در بیاورند. در یک شبکه سیمی هرگاه یک مسیریاب، مسیری معتبر به برخی نقاط مقصد در شبکه داشته باشد آن مسیر تا ابد معتبر خواهد بود(مگر اینکه در جایی از سیستم خرابی بوجود آید) ولی در یک شبکه ویژه توپولوژی شبکه بطور دائم در حال تغییر است.لذا اعتبار مسیرها و بهینگی آنها،به ناگاه و بی هیچ هشدار قبلی تغییر میکند. آشکار است با چنین وضعیتی،مسیریابی در شبکه های ویژه کاملا متفاوت از شبکه های ثابت میباشد.

الگوریتم *ADOV*برای شبکه های *MANET*

گونه متعددی از الگوریتمهای مسیریابی برای شبکه های ویژه پیشنهاد شده است.از جالبترین آنها،الگوریتم مسیریابی *ADOV* است.(*Ad Hoc On-demand distance Vector*)

این الگوریتم گونه ای از الگوریتمهای بردار فاصله است که برای کار در محیطهای متحرک تطبیق داده شده ودر آن پهنای باند محدود و عمر کم باطری ماشینها در نظر گرفته شده است. یکی دیگر ار ویژگیهای این روش آنست که الگوریتم بر حسب تقاضا (*on-demand*)عمل میکند بدین معنی که مسیر رسیدن به برخی از نقاط مقصد فقط وقتی تعیین میشود که کسی بخواهدبسته ای را بدان مقصد بفرستد

از دیگر پروتکل های شبکه های *MANET* میتوان به*DSR* و*DSDV* و*OLSR* اشاره کرد.

کشف مسیر در الگوریتم *AODV*

در پروسه کشف مسیر، اگر دو ماشین بتوانند از طریق سیستم رادیویی خود مستقیما با یکدیگر ارتباط برقرار کنند میگوییم این دو گره بهم متصلند. از انجاییکه امکان دارد یکی از این دو ماشین فرستنده قدرتمندتری نسبت به دیگری داشته باشد لذا این امکان وجود دارد که ارتباط از A به B برقرار باشد ولی باعکس میسر نباشد.

همچنین باید به این نقطه اشاره کرد که هرگاه دو گره در برد رادیویی یکدیگر باشند،تضمینی وجود ندارد که ارتباط آنها برقرار باشد ممکن است بین آنها ساختمان تپه.. وجود داشته یاشد که مانع ارتباط شود.

جهت مسیریابی، گره مبدا یک بسته خام بنام *Route Request* این ساخته و آن را منتشر میکند. این بسته شامل آدرس مبدا و آدرس مقصد است و مشخص میکند چه کسی در جستجوی چه کسی است.(عموماًاز ادرسهای *IP*استفاده میشود).

این بسته همچنین حاوی *Request ID* است این شناسه در حقیقت یک شمارنده محلی است که در هرگره وجود دارد و هرگاه یک بسته *Route Request* منتشر گردید یک واحد به آن اضافه میشود. ترکیب آدرس مبدا و فیلد *Request ID* هویت *Route Request* را بصورت منحصر بفرد تععین کرده و بدین ترتیب گره ها قادرند بسته های که احتمالا بصورت تکراری دریافت میشوند را تشخیص داده و حذف کنند.

فصل سوم

مسیر یابی پیازی

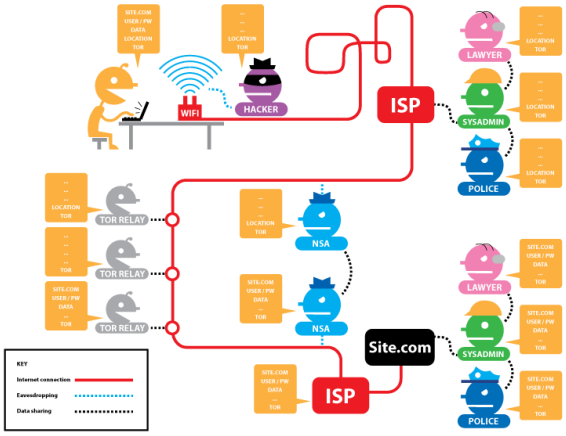
ما در این فصل به توضیح کاملی درباره مسیر یابی پیازی و چگونه ناشناس ماندن در شبکه های اینترنی و به توضیح جامع ای درباره شبکه های تور یا سامانه تور می پردازیم.
در دنیای نفوذ وامنیت گمنامی بحث بسیار مهمی می باشد که تکنیک ها و روش های مختلفی ارائه شده اند. یکی از روش گمنامی شبکه های *Tor* می باشد که امروزه بحثی جالب است. باتوجه به شبکه *Tor* و امکاناتی که می توان در استفاده از این شبکه داشت بدافزارها ترغیب شده اند تا برای گمنامی خود بدافزارهایشان را برپایه این شبکه ایجاد نمایند.

۳-۱ سامانه *TOR*

Tor: (***The Onion Router***) یک نرم افزار و یک شبکه باز است که کاربر را از آنالیزور های ترافیک محافظت می کند. پروژه *Tor* که در سال ۲۰۰۶ پدید آمد و در واقع نسل دوم از پروژه مسیریابی پیازی از آزمایشگاه تحقیقات نیروی دریایی ایالات متحده محسوب می گردد. هدف اصلی در ابتدا محافظت از ارتباطات دولتی بوده است که امروزه برای اهداف مختلفی توسط افراد مختلفی مورد استفاده قرار می گیرد. همانطور که گفته شد *Tor* از مسیریابی پیازی استفاده می کند و مبتنی بر لایه های چندگانه امنیتی است، دقیقا همانند پوست پیاز که لایه به لایه است و این لایه های امنیتی یک به یک از پیام های رد وبدل شده در شبکه *Tor* حذف می گردند.

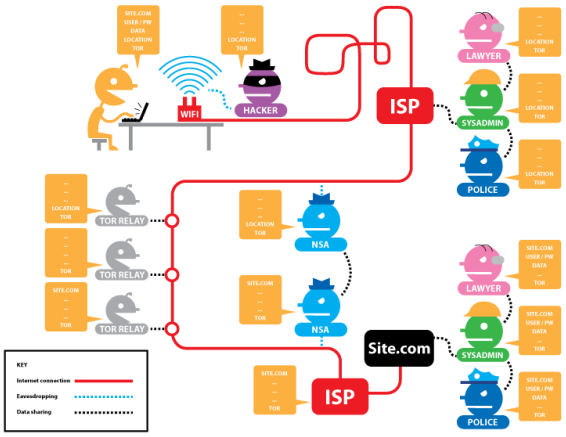
گام اول در سامانه *TOR*

اما *Tor* نسبت به بلوکه شدن آسیب پذیر است. بیشتر نودهای *Tor* در یک دایرکتوری عمومی لیست می‌شوند، بنابراین برای گردانندگان شبکه‌ها ساده است که به لیست دسترسی یافته و آدرسهای *IP* نودها را به فیلتر خود اضافه کنند. یک راه برای خلاصی از این نوع بلوکه کردن استفاده از یکی از چندین پل *Tor* است که نودهای *Tor* هستند، که برای اجتناب از بلوکه کردن، بصورت عمومی لیست نمی‌شوند.
گاها بعضی از برنامه‌هایی که از *Tor* استفاده می‌کنند امکان دارد گمنام ماندن شما را خدشه دار کنند، همچنین اگر از رمزنگاری اضافه برای حفاظت از ارتباطهای خود استفاده نمی‌کنید، داده‌های شما هنگام رسیدن به آخرین گره *Tor* در زنجیره (گره خروج) داده‌های شما بصورت بالقوه برای صاحب آخرین گره *Tor* و *ISP* بین آن گره و سایت وب مقصد شما آشکار خواهد شد.
در تصویر زیر تنها توسط شبکه *TOR* به اینترنت متصل شده ایم و نحوه ارتباط و داده های رد و بدل شده را می توان مشاهده نمود:



شکل(۳-۱)روش‌کار۱

ولی اگر علاوه بر *TOR* از *HTTPS* نیز استفاده نماییم (تصویر زیر) تنها سایت مقصد می تواند داده های مارا مشاهده کند که تفاوت آن را با تصویر قبلی می توانید مشاهده کنید:



شکل(۳-۲) روش‌کار۲

- در واقع این دو تصویر تاثیر شبکه های *TOR* را بر جاسوسی و جمع آوری اطلاعات توسط *NSA* را نشان می دهند که براحتی با مقایسه هر دو می توان فهمید که چه اتفاقاتی می افتد. برای استفاده برنامه ها از این شبکه براحتی یک رابط پراکسی *SOKCS* وجود خواهد داشت و هر برنامه ای که *SOCKS* (نسخه‌های ۴، ۴*A* و ۵) را پشتیبانی کند می‌تواند توسط *Tor*، گمنامی خود را حفظ نماید.
- رله های پلی (یا بطور خلاصه پل ها) رله هایی از شبکه *TOR* هستند که در دایرکتوری اصلی (و عمومی) معرفی نشده اند. حتی اگر *ISP* تمامی ارتباطات با رله های شناخته شده *TOR* را فیلتر کند، احتمالاً قادر نخواهد بود که مانع دسترسی به تمامی پل ها شود.
- یک گره *TOR* به دو صورت ایجاد می شود: یا به صورت گروه خروجی یا به شکل گره واسطه (برخی اوقات به آن گره غیر خروجی نیز می گویند). گره واسطه، ترافیک رمزنگاری شده داده ها را فقط به گره بعدی پاس می دهد، بنابراین به کاربران ناشناس اجازه نمی دهد تا مستقیماً با وب سایت های خارج شبکه *TOR* ارتباط برقرار کنند

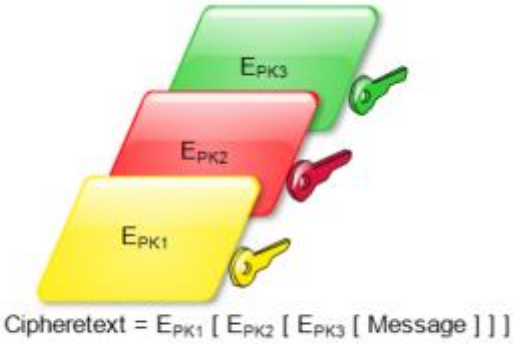
.

۳-۴ طرز کار مسیریابی پیازی

- در شبکه های امروزی که پکت ها ردوبدل می شوند در هدر آن *IP* فرستنده نیز مشخص می شود که براحتی می توان فرستنده اطلاعات ردیابی نمود. برای بهبود گمنامیابتدا به دو روش مهم می پردازیم:
  ۱. *Digital Mixing*
  ۲. *Anonymizing Proxies*

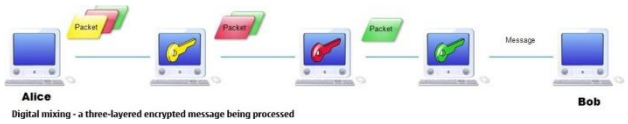
Digital Mixing

- در اوایل دهه هشتاد *David Chaum* اصل *Digital Mixes* را بوجود آورد (گاها شبکه های ترکیبی – *Mixed network* – نامیده می شود) که طرح نمودن آن برای سطح بالاتری از گمنامی از ارتباطات شخصی است. *Digital mixing* همانند روندمسیریابی است ولی لایه های دیگر بین فرستنده و گیرنده به آن اضافه می کند شکل زیر نشان می دهد که چگونه با استفاده از رمزنگاری کلید عمومی این عمل انجام می شود.



شکل(۳-۳)*CODING*۱

- در شکل زیر می بینیم که *Alice* می خواهد پیامی به *Bob* ارسال کند بدون آنکه شخص سومی بتواند تشخیص دهد مبدا ارسال اطلاعات کجا بوده است. ابتدا پیام ۳بار توسط رمزنگاری کلید عمومی رمز می شود. بعداز ارسال اطلاعات به اولین سرور پروکسی اولین لایه حذف می شود و اطلاعات به دومین سرور پروکسی ارسال خواهد شد

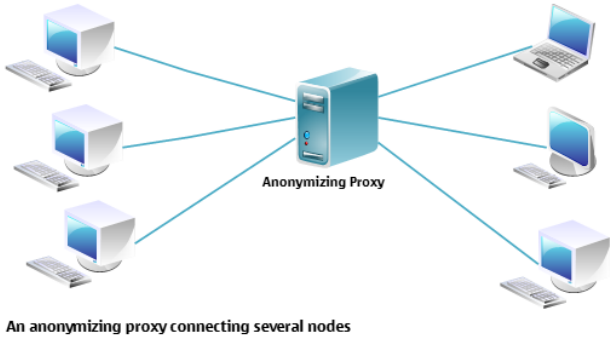


شکل(۳-۴)*CODING*۲

- بطور خلاصه می توان گفت این عمل مانند این است یک نامه در چند پاکت احاطه گردد و برروی هر پاکت چنین متنی نوشته شود: "پاکت را پاره کنید و بسته را دوباره ارسال کنید".

Anonymizing Proxies

- یک سرور پروکسی در بین ارسال کننده اطلاعات و دریافت کننده قرار می گیرد که این پراکسی سرور تنها نقش یک نود را ایفا می کند.

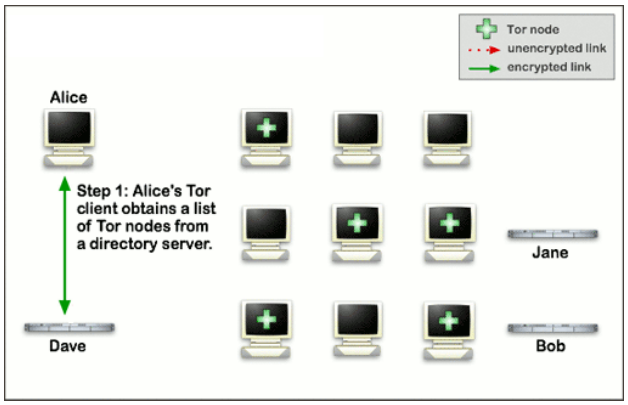


شکل(۳-۵)*PROXY*

- این روش خوبی هایی که دارد می تواند بصورت دوطرفه مورد استفاده قرار گیرد مانند *Web Browsing* و همچنین از تکنیک ها و روش ها گرانی مانند رمزنگاری براساس کلید عمومی نیست که البته جنبه های منفی دارد که ممکن است پراکسی سرور از مجرمان باشد و داده ها را مشاهده کنند.

۳-۵ الگوریتم مسیریابی پیازی در *TOR*

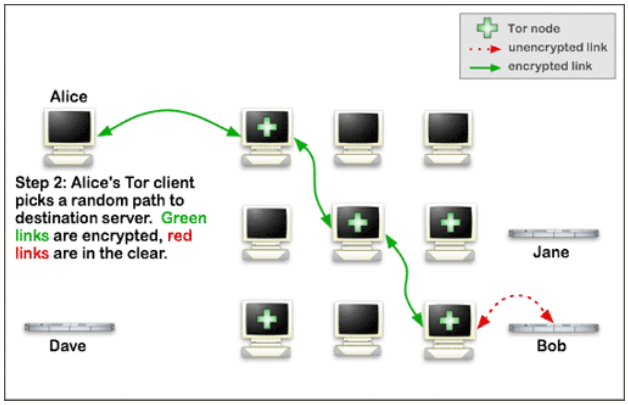
*TOR*بجای استفاده از یک روش خاص، از ترکیبی از روش های فوق استفاده می کند. در تصویر زیر *Alice* می خواهد با *Bob* ازطریق شبکه *Tor* ارتباط برقرار کند ابتدا می بایست ارتباط با سرور مرکزی که شامل آدرس نودهای *Tor* است داشته باشد. بعدازاینکه آدرس ها بدست آمدند برنامه کلاینت *Tor* براساس آن به یک نود بطور تصادفی (نود ورودی) ازطریق ارتباط رمزنگاری شده متصل می شود.



شکل(۳-۶)پیدا کردن نود

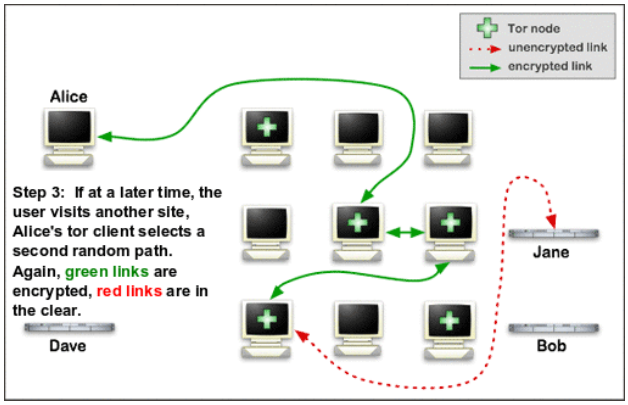
نود ورودی نیز یک ارتباط رمزنگاری شده با نود دوم که آن هم بصورت رندوم انتخاب می شود برقرار نموده و نود دوم نیز همین کار را برای اتصال به نود سوم انجام می دهد. نود سوم بایستی نزدیکترین به مقصد یعنی *Bob* باشد که به نود سوم، گره خروجی نیز می گوییم. هرگره *Tor* بطور تصادفی از لیست انتخاب می شوند، بااین حال یک نود نمی تواند دوبار در یک ارتباط مورد استفاده قرار گیرد و بسته به تراکم داده ها بعضی گره ها نیز مورد استفاده قرار نمی گیرد. لیست نودها توسط مشتری و هچنین خود نودها دریافت می شود که بدین صورت باعث افزایش یک سطح بیشتر برای

گمنامی و هرچه بیشتر باعث گمنامی خواهد شد. *Tor* با *TCP* کار می کند و هربرنامه ای که از *SOCKS*پشتیبانی کند می تواند از آن استفاده نماید.



شکل(۳-۷)انتخاب مسیر

بخاطر اینکه همیشه یک مسیر نداشته باشیم هر ده دقیقه نود ورودی تغییر می کند که درغیراینصورت در برابر ردیابی آسیب پذیر خواهیم بود.

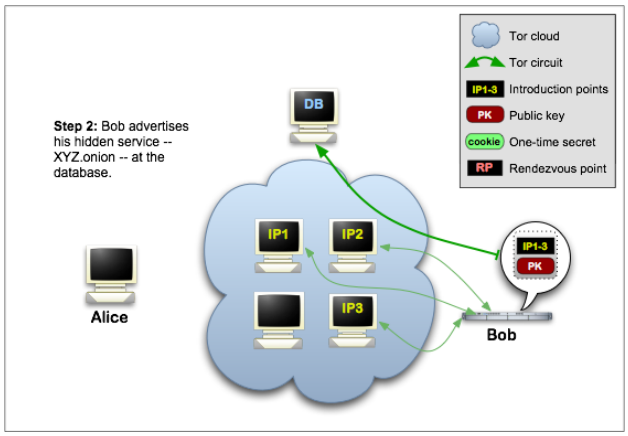


شکل (۳-۸)انتخاب متفاوت

- افزایش گمنامی با ایفا کردن نقش یک نود در شبکه *Tor* بیشتر خواهد شد. همانطور که گفته شد نودهای *Tor* عمومی هستند پس اگر *Alice* بخواهد یک نود باشد در گمنامی اش تاثیری ندارد، اما این مفهموم نیز نمی تواند درست باشد. *Tor* این امکان را می دهد تا کاربران مکان خود را پنهان کنند درحالی که خدماتی را در *Tor* ارائه می دهند می توانند یک سایت راه اندازی کنند بدون آنکه نگران محدودیت ها باشند.
- برخی از سرویس های مخفی بایستی خود را به شبکه معرفی کنند تا دیگر یوزر ها بتوانند به آن متصل گردند. بنابراین این سرویس ها ابتدا برخی از رله ها را بصورت تصادفی انتخاب و جریان اطلاعاتی را با آنها برقرار می کنند و از آنها درخواست می کند تا بعنوان نقاط ورودی (*Introduction Points*) جهت برقراری ارتباط با وی عمل نمایند. *Introduction Points* با سرویس مخفی از طریق *Public Key* ارتباط دارند.

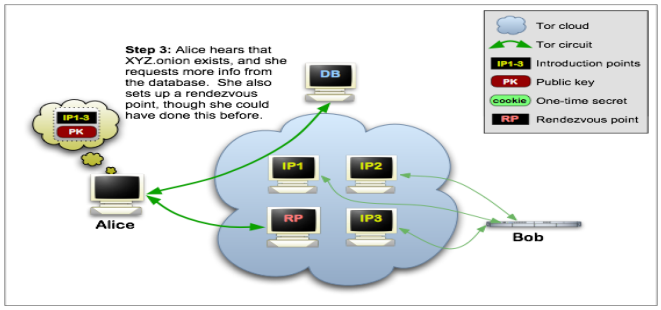
در **مرحله دوم** یک بسته که باعث توصیف و معرفی او می باشد ایجاد نموده که شامل *Introduction Points* و *Public Key* است و توسط *Private Key* خود آن را *sign* نموده است سپس آن را به دیتابیس ارسال می کند. برقراری ارتباط با سرویس پنهان توسط کاربران می تواند با درخواست بصورت

XYZ.onion که *XYZ* یک متن ۱۶ کارکتری است و از کلید عمومی سرویس پنهان بدست می آید صورت پذیرد. بعد از این مرحله دیگر سرویس پنهان شروع به کار می کند. اگر چه ممکن است استفاده از یک نام بصورت اتوماتیک ایجاد شده غیرعملی بنظر برسد. در برخی بدافزار ها مخصوصا کیلاگر ها مشاهده می کنیم که لاگ خود را به سایتی به صورت *XYZ.onion* ارسال می کنند.



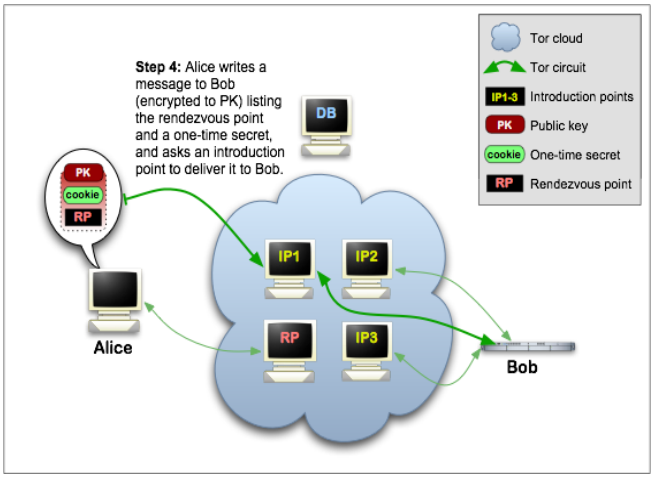
شکل(۳-۹) *DB-PACK*۱

گام سوم: کلاینت ها می خواهند با سرویس های پنهان ارتباط برقرار کنند .ابتدا می بایست آدرس های *onion* را یاد بگیرند، بعد از آن با ایجاد یک ارتباط می تواند جدول توضیحات را دانلود نماید. اگر برای سرویس پنهان شده توضیحاتی وجود داشته باشد می تواند از *Introduction Points* و کلید عمومی برای ارتباط با آن استفاده نمود. این سرویس می تواند آنلاین باشد و یا خیلی وقت شبکه را ترک نموده و یا حتی در آدرس آن اشکال تایپی رخ داده باشد. در این زمان کلاینت می بایست یک جریان اطلاعاتی با یک رله رندوم ایجاد نماید و از آن درخواست کند تا بعنوان یک میعادگاه یا همان *Rendezvous Point* (نود ارتباطی بین کاربر و سرویس پنهان) عمل نماید.



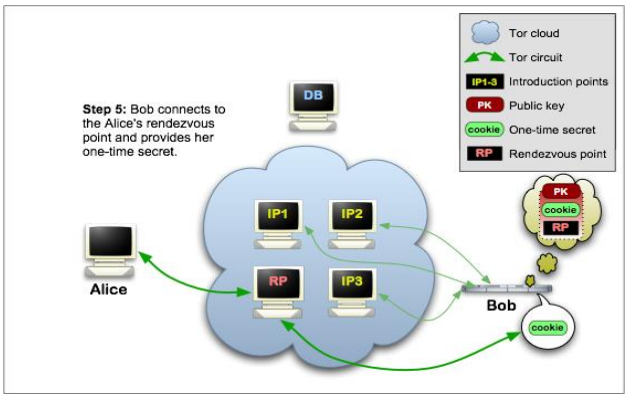
شکل(۳-۱۰) *DB-PACK*۲

گام چهارم *Rendezvous Point*: در جدول توصیف مشخص شده است، حال کلاینت یک پیام ابتدایی جهت برقرار ارتباط ایجاد نموده و با کلید عمومی سرویس پنهان رمزنگاری می کند که شامل *RP* *(Rendezvous Point)*و یک کوکی می باشد. کوکی تنها جنبه *Authenticate*را دارد که *RP* مطمئن شود در آنطرف ارتباط *Bob* واقعی وجود دارد. سپس پیام ابتدایی ایجاد شده را به *Introduction Points* ارسال می کند و یک جریان اطلاعاتی *Tor* برقرار می گردد و کسی نمی تواند پیام ابتدایی را برای سرویس پنهان ارسال کند که بازهم سرویس پنهان باقی مانده است.



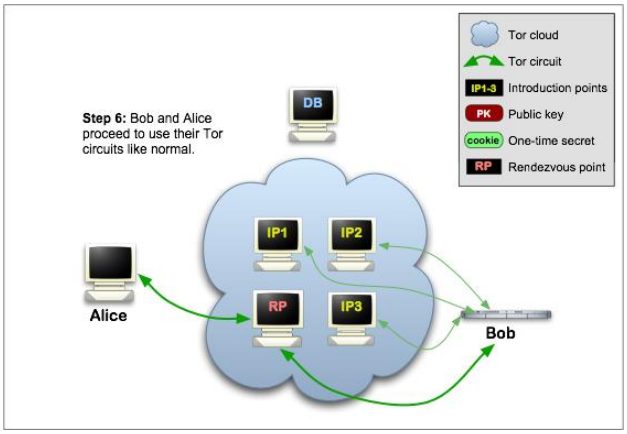
شکل(۳-۱۱)*DB-PACK*۳

گام پنجم سرویس پنهان پیام ابتدایی را توسط کلید خصوصی رمزگشایی می نماید و *RP* را بدست می آورد، کوکی را به آن ارسال خواهد نمود و جریان ارتباطی *Tor*ایجاد می کند. نکته مهم اینجاست که سرویس پنهان با رله های ارتباطی که نگهبان او هستند در ارتباط خواهد بود در غیر اینصورت نفوذگر می تواند با ایجاد رله خود در شبکه و سرویس پنهان را مجبور ساز تا چندین جریان ارتباطی *Tor* را داشته باشد و به این امید که نود تحت کنترل نفوذگر بعنوان گره ورودی انتخاب شود و با استفاده از *Timing Analysis*سرویس پنهان را کشف و *IP* آن را بدست آورد، این حمله توسط *overlier and Syverson* در مقاله خود به نام *Locating Hidden Servers* ارائه نموده اند



شکل(۳-۱۲)*DB-PACK*۴

و در آخر هردوتوسط *RP* بعنوان یک رله ساده به تبادل اطلاعات می پردازند. تنها دلیلی که از *Introduction*ها استفاده نشده به این خاطر است که رله های مسئول یک سرویس مخفی مشخص نگردند و هیچگاه *RP* از سرویس پنهان متوجه نخواهد شد که درواقع ارتباط بین کلاینت و سرویس پنهان شامل ۶ تا رله است که ۳ تا توسط کلاینت انتخاب میگردد که سومین *RP* است و ۳تای دیگر توسط سرویس پنهان، در انتها ارتباطی بدین صورت خواهند داشت



شکل(۳-۱۳)*DB-PACK*۵

Tor ارتباط های *relay-to-relay* را رمزنگاری می کند اما *Proxy Chain* ارتباط را بین چندین پراکسی وب رد و بدل می کند و ارتباط بین آنها رمزنگاری نمی شود.

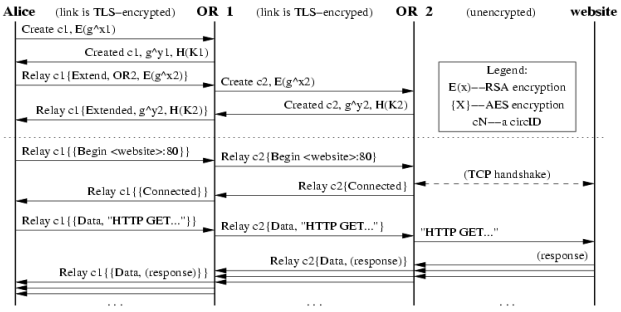
۳-۶ هر نود از *TOR* چه اطلاعاتی را در اختیار دارد؟

گاها نگرانی پیش می آید که هر نود از *TOR* چه اطلاعاتی را می داند که در جدول بطور خلاصه سه نود مورد استفاده در *TOR* را مقایسه نموده ایم.

	user	bridge node or entry guard	middle node	exit node
Tor user's IP/location	yes	yes	no	**no**
IP of bridge node or entry guard	yes	yes	yes	**no**
message for bridge node or entry guard	yes	yes	no	**no**
IP of middle node	yes	yes	yes	**yes**
message for middle node	yes	no	yes	**no**
IP of exit node	yes	no	yes	**yes**
message for exit node	yes	no	no	**yes**
IP of destination server	yes	no	no	**yes**
message for destination server	yes	no	no	**yes**

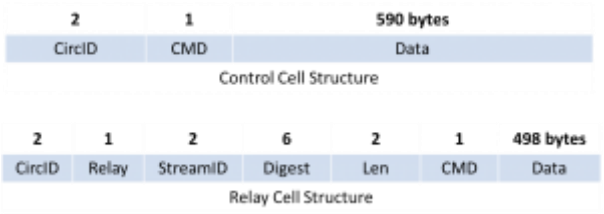
شکل(۳-۱۴)اطلاعات *TOR*

روند ایجاد جریان ارتباطی *Tor* را در تصویر زیر می توانید مشاهده کنید که *Alice* با استفاده از جریان دوگام می خواهد به محتوای یک سایت دسترسی پیدا کند:



شکل(۳-۱۵)روند ایجاد جریان

بعد از اینکه جریان ارتباطی *Tor* برقرار شد می توان *Cell* ها را ارسال کرد*Cell* . پکت هایی با سایز ثابت ۵۱۲ بایت (جهت سخت تر نمودن تحلیل ترافیک) و فرمت خاصی است *Cell*می تواند *Control Cell* و یا *Relay Cell* باشد که ساختار آنها را در تصویر زیر می توانید مشاهده کنید.



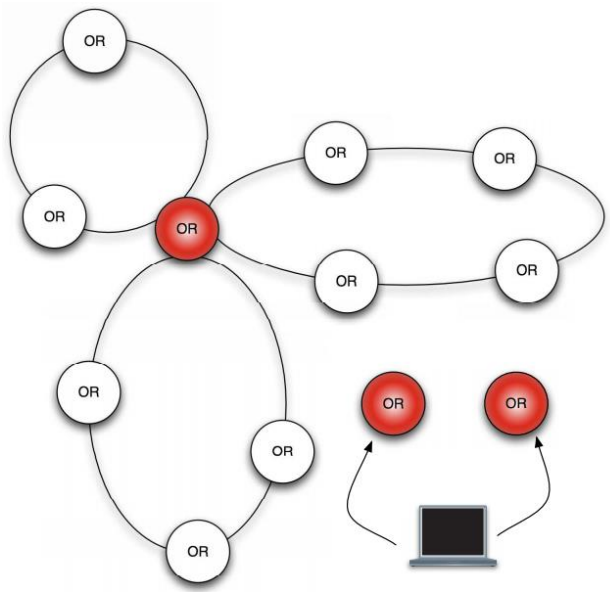
شکل(۳-۱۶)*CELL*

*Relay Cell*در واقع پکت های *end-to-end* است، برای مثال هنگامی که کاربر نیاز دارد تا داده خود را از طریق *Tor* ارسال کند *Relay Cell* ایجاد خواهد شد *Onion proxy* .پکت را ایجاد می کند و *Digest* را محاسبه می کند که این فیلد نقش *Checksum* را خواهد داشت و بعد با *AES(k_n)* و سپس *AES(k_{n-۱}),.., AES(k_۱)* انکریپت می شود و ارسال می کند.

۳-۷ حملات *Tor* و ازبین رفتن گمنامی کاربران

در کنفرانس بین المللی*ACSAC* سال ۲۰۱۱ حمله ای بصورت*brute-force* برروی *TOR* ارائه شد که در این حمله بخشی از *Node* ها بلوکه می شوند که این حمله نیز در واقعیت صورت گرفت، کشور چین در سال ۲۰۰۹ تقریبا ۸۰ درصد از *relay* ها را بلاک کرد. این حمله براساس *super-node* انجام می شود. اصطلاح *Super-node* در شبکه های *TOR*را به نودهایی می گوییم که دارای چرخه زندگی طولانی تر و مشارکت پهنای باند بیشتر و پایداری بالاتری نسبت به بقیه نودها باشد. هنگامی که برروی *super-node* ها بجای هر *relay* متمرکز می شویم می توانیم نتیجه های بهتری و حملات موثرتر داشته باشیم که حمله برروی یک *super-node* درای تاثیر برابر با حمله بر ۴ نود عادی می باشد. همانطور که در قبل هم به بعضی حملات پرداختیم حملات مختلفی برروی این شبکه معرفی شده اند مانند:*Cell Flood* ، *Selective Attack*، *loop Attack*، *Collusion Attack*، *Sybil Attack* و ...

یکی از حملات پیشنهادی ایجاد حلقه در جریان ارتباطی و داشتن یک *OR(Onion Router)* تحت کنترل در شبکه است [۲]. هدف اصلی از ایجاد *Loop* مشغول نمودن دیگر *OR* ها تا در جریان های ارتباطی انتخاب نشوند یعنی می توان گفت *DOS* برروی دیگر *OR* ها انجام می دهد و هنگامی که آنها *Busy*باشند *OR* های تحت کنترل در هنگام ایجاد جریان ارتباطی انتخاب می شود.



شکل (۳-۱۷)طرح حمله

- در تصویر بالا طرح کلی از حمله را مشاهده می کنیم که چگونه گمنامی یک کاربر را خدشه دار کند. در تصویر سه *OR* تحت کنترل به شبکه وارد شده است که یکی از آنها وظیفه *Busy*نمودن دیگر *OR* ها را خواهد داشت، در حین *Busy* نمودن دو *OR* تحت نفوذ دارای منابع آزاد خواهد بود و جهت ایجاد ارتباط مورد استفاده قرار خواهد گرفت.
- حمله ای دیگر [۳] معرفی گردید که بر دروغ گفتن منابع خود به *DB* تکیه دارد و احتمال اینکه بعنوان روتر *Entry* یا *Exit* انتخاب شود زیاد خواهد بود. این حمله نیز مشکلاتی را گاها خواهد داشت مثلا اگر پهنای باند غیرواقعی باشد جوابگو ترافیک های دریافتی نخواهد بود. حمله دیگری در سطح *AS* معرفی گردید که اگر *Entry* و *Exit* در یک *AS*باشند بتوان حمله ای باتوجه به این خاصیت انجام داد[۴]. البته با بهبود در روند انتخاب مسیر *TOR* دیگر آنالیز ترافیک در سطح *AS* بی فایده است زیرا محدودیت هایی در *Entry Guard*و همچنین انتخاب *OR* در ساب نت متفاوت بایستی باشد. شاید در آینده جهت بهبود بهتر انتخاب ها براساس کشورها باشد. افرادی از دانشگاه *MIT*حمله ای را بصورت *Browser-Based*ارائه کردند [۵]. در واقع این حمله *Time-Based* می باشد و با توجه به رفتاری که مرورگر در برابر دستکاری نمودن ترافیک *HTTP* از خود نشان می دهد حمله صورت می گیرد. در این حمله دو *OR*نیاز است: *Exit* و *Entry* می بایست تحت کنترل نفوذگر باشد. در این حمله وجود هر دو *OR* در یک جریان ارتباطی نیاز نخواهد بود. روتر *Entry* برای تجزیه و تحلیل ترافیک و روتر *Exit* برای تغییر ترافیک *HTTP* که می تواند بصورت افزودن ویا تغییر کدهای جاوا اسکریپت و *HTML* جهت برقراری ارتباط با سرور تحت کنترل، باشد. جهت جلوگیری از این حمله در مرورگر خود می بایست اجرای کدهای فعال مانند *Flash, Java, ActiveX* و جاوا اسکریپت غیرفعال نمود.
- *Exit node*در واقع حمله *MITM* را برروی ترافیک *HTTP* کاربر انجام می دهد بنابراین تانلینگ *HTTP* برروی *SSL* از این حمله جلوگیری خواهد نمود. هرچند در دنیای واقعی این کار بی فایده است زیرا اغلب کاربرها سرتیفیکیت های *self-signed* را با وجود اخطارهایی که مرورگر می دهد بعنوان یک

سرتیفیکیت معتبر تایید می کنند. یکی از مشکلاتی که در این حمله مطرح خواهد می شود بحث *Entry Guard*است که برای توضیحات بیشتر به منابع مراجعه نمایید.

- در این مقاله قصد آنالیز بدافزار را نداریم ولی جهت آشنایی و ذکر مثال می توان کیلاگر *ChewBacca* را نام برد که برنامه *TOR* را بصورت *Drop* همراه خود داشته است و توسط آن با *C&C server* خود ارتباط برقرار می کند. حال این گونه عمل نمودن حجم فایل بدافزار را افزایش می دهد که گاها نامعقول خواهد بود. تکنیک دیگری که توسط بدافزارها جهت ارتباط با *C&C server* مورد استفاده قرار می گیرد استفاده از سایت *tor۲web*است که نحوه استفاده آن خیلی راحت تر نسبت به قبل خواهد بود. هنگامی که می خواهیم توسط خود برنامه *TOR* به یک سرویس پنهان ارتباط برقرار نماییم از آدرس آن با. *onion*استفاده می نماییم ولی *tor۲web* امکانی را می دهد که بتوانیم بدون دانلود *TOR* بتوانیم به سرویس های پنهان نیز دسترسی داشته باشیم بدین صورت که در آدرس بجای *onion*.می بایست. *tor۲web.org*استفاده نماییم و این سایت را بعنوان یک پروکسی بین خود و سرویس پنهان قرار دهیم. ولی این روش نیز بدی های خود را دارد که براحتی می توان ترافیک آن را فیلتر کرد و یا راه حل دیگر ایجاد نمودن *tor۲web* بصورت اختصاصی است.

۳-۸ نتیجه‌گیری

در دنیا کامپیوتر باید ما مسیر خود به نحوه خود مشخص کنیم و الگوریتم مورد نظر خود را به درستی انتخاب کنیم امروزه الگوریتم های مسیریابی بسیاری در دنیا وجود دارد هرکدام نقطه قوت و ضعفی دارن ما در این پایان‌نامه به تفسیر کامل الگوریتم مسیریابی پیازی در شبکه های تور پرداختیم و یاد کرفتیم که برای ناشناس ماندن در شبکه بهترین الگوریتم استفاده از مسیریابی پیازی است.معایب این الگوریتم اینه به صورت متمرکز است و اگر نودها نابود شوند کل شبکه مختل می‌شود.

منابع

۱-شبکه های کامپیوتری(رویکرد *TOP-DOWN*) جلد اول *KUROSE.ROSE* ترجمه دکتر بهزاد اکبری ومهدی ایمانی

۲- *www.cisco.com*

۳-*www.optionrouting.com*

۴-*www.routingbase.com*