ششمین همایش بین‌المللی افق های نویـن در
مهندسی برق، کامپیوتـر و مکانیک
6th International Conference on the New Horizons in
Electrical Engineering, Computer and Mechanical
www.mhconf.ir

بررسی پیاده‌سازی و مدیریت شبکه‌های خصوصی مجازی امن (VPN) و شبکه‌های محلی مجازی (VLAN) در سناریوهای استاتیک و موبایل

مهدی دهقانی[1]، دکترمحمدرضا سلطان آقایی[2]

[1] مهدی دهقانی - دانشجوی دکتری نرم افزار کامپیوتر دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد اصفهان(خوراسگان) ، اصفهان
Mhd.ir_esf@yahoo.com

[2] محمدرضا سلطان آقایی، استادیار دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد اصفهان(خوراسگان) ، اصفهان Mersa4@gmail.com

چکیده

امروزه، تقاضا برای ارتباط بین دفاتر راه دور یک شرکت، یا بین آن‌ها مکان‌های تحقیقاتی، و تحرک دائمی فزاینده کاری (تا حدودی به دلیل وضعیت بحرانی کنونی پاندمی)دست در دست هم با کیفیت و سرعت ارتباطات پهنای باند افزایش‌یافته است. نتیجه منطقی این سناریو استفاده فزاینده از اتصالات شبکه خصوصی مجازی (VPN)است. آن‌ها به فرد اجازه می‌دهند تا به طور ایمن دو انتهای یک اتصال را از طریق یک شبکه اختصاصی، معمولا با استفاده از اینترنت و کاهش هزینه‌های خطوط شبکه تحویل محتوا (CDN)(اتصالات اختصاصی)متصل کند. در عین حال، شبکه‌های ناحیه مجازی (VLAN ها)قادر به کاهش تاثیر برخی مسائل مقیاس پذیری شبکه‌های بزرگ هستند. با توجه به پیشینه فوق، این مقاله بر مشاهده و بررسی پیشرفت‌های اصلی مربوط به VPN ها و VLAN ها در شبکه‌های بی‌سیم، با جمع‌آوری مهم‌ترین نقش در این زمینه و توصیف چگونگی پیاده‌سازی آن‌ها متمرکز شده‌است. ما بیان می‌کنیم که مسائل امنیتی در VLAN ها را می توان به طور موثری از طریق ترکیبی از شیوه‌های مدیریت خوب شبکه، طراحی موثر شبکه و کاربرد محصولات امنیتی پیشرفته کاهش داد. با این حال، بدیهی است که اجرای VPN ها و VLAN ها مسائل خاصی را در رابطه با اطلاعات و امنیت شبکه به وجود می‌آورد، از این رو راه‌حل‌های مناسبی نیز مورد بررسی قرار گرفته‌است.

کلمات کلیدی
QoS, VPN, mobile VPN, security, MANETs

۱. مقدمه

در دهه گذشته، راه‌حل‌ها و ویژگی‌های امنیتی در WPAN، WLAN، WMAN و سیستم‌های بی‌سیم توزیع‌شده به طور فزاینده‌ای اجباری شده‌اند [۱، ۲]. تعداد پیاده‌سازی‌های شبکه خصوصی مجازی (VPN)به دلیل جذابیت زیاد استفاده از زیرساخت عمومی برای پیاده‌سازی یک لینک امن بین مکان‌های مختلف یک شرکت (به عنوان مثال، یک دانشگاه) [۳]، که شامل معماری‌های سلولی نیز می‌شود، به سرعت افزایش‌یافته است. چندین مزیت برای اجرای یک VPN وجود دارد، که مواردی از آنها در ادامه آمده است.

(الف) اثربخشی هزینه (هزینه زیرساخت کم‌تر است، و انتخاب مناسب مرحله اجرا به افراد اجازه می‌دهد تا بهترین راه‌حل را با کم‌ترین هزینه پایدار انتخاب کنند)، (ب) سادگی (این تکنولوژی خیلی بالغ است و به مهارت‌های باطنی نیازی ندارد)، (پ) ایمنی (تکنولوژی براساس استانداردهای باز است و عمدتا به طور جهانی ایمن است). بنابراین، با تلاش کم، امکان دستیابی به یک مصالحه خوب بین سهولت دسترسی و ایمنی معقول وجود دارد.

مفهوم VPN کاملا ساده است، براساس الگوی "هاب و صحبت کردن"، با یک مکان مرکزی است که از آن یک مجموعه بزرگ از اتصالات به مکان‌های دوردست منتقل می‌شود. با استفاده از قوانین مناسب، این امکان وجود دارد که تصمیم بگیریم که آیا هر سایت راه دور منحصرا به گره مرکزی دسترسی دارد یا اینکه آیا ترافیک بین حومه شهر باید فعال شود. راه‌حل‌های پیاده‌سازی این نوع دسترسی‌ها بسیار گسترده و متفاوت هستند، اعم از یک سرور ساده مجهز به نرم‌افزار متن باز تا لوازم اضافی گران‌قیمت در دسترس پذیری بالا (HA). انتخاب دقیق بستگی به هزینه‌ها، درجه یکپارچگی با زیرساخت‌های موجود، پهنای باند مورد نیاز، حجم کار و یا انتقاد از لینک (فقط چند عامل که بر انتخاب سیستم VPN تاثیر می‌گذارند). علاوه بر این، اخیرا، مصرف انرژی راه‌حل‌های امنیتی اتخاذ شده به یک جنبه برای در نظر گرفتن تبدیل شده‌است [۴]. در واقع، با عملیات کلی یک VPN، تمام ترافیک بین دو نقطه پایانیVPN در تونل‌های از پیش ایجاد شده محصور شده‌است که می‌تواند در سطوح مختلف مدل ISO / OSI (IPSEC یا IKEv2 IPSEC در لایه سوم، PPTP در لایه پنجم، L2TP در لایه دوم و OpenVPN یا شبح تونل مجازی در لایه چهارم)باشد [۵ ,۱۴]. این مقاله بر ارائه یک مرور عمیق بر اجرای احتمالی VPN ها و شبکه‌های محلی مجازی (VLAN ها)و پیشرفت‌های اخیر آن‌ها در سناریوهای بی‌سیم و سیار متمرکز شده‌است. به طور خاص، هدف اصلی ما ارائه یک بررسی دقیق از کارایی است. پیاده‌سازی VPN برای سناریوی موبایل در واقع، راه‌حل‌های VPN مرسوم (همانطور که در بالا اشاره شد)به شبکه‌های ایستا (بدون گره‌های متحرک)اختصاص‌داده شده‌اند. مشخص شده‌است که در سناریوی موبایل، ارتباطات به اندازه حالت سیمی قابل‌اعتماد نیستند، اثرات تحرک، به طور واضح، عملکرد VPN را منعکس می‌کند، که منجر به ارتباطات با سرعت پایین، از دست دادن بسته و خروجی پایین می‌شود. با گسترش سریع دستگاه‌های تلفن همراه و سرعت‌های بالا (به عنوان مثال، با نسل پنجم (5G))، کاربران تمایل بیشتری به استفاده نه تنها از دستگاه‌های خانگی خود بلکه از دستگاه‌های تلفن همراه خود (مانند تلفن‌های هوشمند و تبلت ها)، با در نظر گرفتن ارتباطات و خدمات فرصت طلبانه دارند [۱۵، ۱۶]. رایانش ابری (CC)به درجه بالایی از توسعه رسیده‌است و امروزه، کاربران به منظور دسترسی به خدمات ابری خود، با دستگاه‌های تلفن همراه خود به ابر متصل می‌شوند. در سناریوی بالا، واضح است که ایجاد یک جلسه معتبر ضروری است و VPN ها اولین "ابزار" هستند که می‌توانند برای تضمین امنیت و استحکام مورد استفاده قرار گیرند. متاسفانه VPN ها تنها با اتصالات شبکه پایدار به خوبی کار می‌کنند. اگر تلفات اتصال یا تنزل خدمات رخ دهد، اتصالات VPN قطعا شکسته خواهد شد، و کاربران از نتایج راضی نخواهند شد، که می‌تواند شامل از دست دادن داده‌ها و شکست‌های جلسه پیوسته باشد. بنابراین، هدف اصلی این کار بررسی و بررسی راه‌حل‌های VPN اصلی برای شبکه‌های ایستا (گره‌های ثابت)و پویا (گره‌های متحرک)از نقطه‌نظر عملی است. یک جایگزین معتبر برای VPN ها، فن‌آوری VLAN است. این امر به شبکه‌ها اجازه می‌دهد تا به صورت منطقی گروه‌بندی شوند نه با مکان فیزیکی، و تقسیم‌بندی شبکه به شبکه‌های مجازی یا گروه‌های مجازی را ممکن می‌سازد (یک ویژگی که توسط اکثر سوئیچ‌های شبکه پشتیبانی می‌شود).

هدف اصلی این مقاله را می توان به صورت زیر خلاصه کرد:

(الف)یک بررسی گسترده از مقالات ارائه شده‌است، که بینشی نسبت به مشارکت‌های کلیدی در حوزه پیاده‌سازی‌های VPN و VLAN در شبکه‌های استاتیک و پویا را برای خواننده فراهم می‌کند، (ب)جزییات متعددی در مورد پروتکل‌ها و سیگنال دهی مورد استفاده در سیستم‌های VPN / VLAN داده شده‌است، که اطلاعات جزئی در مورد مدیریت امنیت در سناریوی مورد نظر را برای خواننده فراهم می‌کند، (پ)مسائل تحرک مورد بررسی قرار می‌گیرند، و برخی راه‌حل‌ها (مانند ابزارهای نرم‌افزاری موجود)با جزئیات توصیف می‌شوند و برای برخی محیط‌های سیار پیشنهاد می‌شوند، (ت)برخی از خطوط فرمان نیز توصیف شده‌اند، و به خواننده دستورالعمل‌های مربوط به چگونگی رسیدگی به برخی از مسائل امنیتی VPN را ارائه می‌دهند.

ادامه مقاله به شرح زیر است:

بخش ۲ به VPN ها در شبکه‌های استاتیک و دینامیک می‌پردازد، در حالی که بخش ۳ ویژگی‌های اصلی VLAN ها را نشان می‌دهد. بخش ۴ بهترین راه‌حل برای مدیریت تحرک در VPN ها و VLAN ها را نشان می‌دهد، در حالی که بخش ۵ برخی از پیاده‌سازی‌های امنیت واقعی را شرح می‌دهد. بخش ۶ به نتیجه‌گیری مقاله می‌پردازد.

۲. شبکه‌های خصوصی مجازی در شبکه‌های استاتیک و پویا

این بخش نقش اصلی را از نظر کاربردها و پروتکل‌ها برای شبکه‌های استاتیک و دینامیک بررسی می‌کند.

۲,۱ راه‌حل‌های VPN کلاسیک برای شبکه‌های ایستا

چندین پروتکل برای اجرای VPN های امن وجود دارد (اجرای تنها VPN هیچ رمزگذاری یا محرمانگی را برای عبور ترافیک از آن فراهم نمی‌کند):

(الف)پروتکل تونل زنی لایه ۲ IPsec / (L2TP) [۷] یک راه‌حل داخلی برای تمام سیستم‌های عامل مدرن و دستگاه‌های توانمند VPN است. پروتکل L2TP از پورت UDP 1701 و IPsec پورت ۵۰۰ و ۴۵۰۰ برای اهداف NAT استفاده می‌کند. این امر نیازمند پیکربندی پیشرفته (ارسال پورت)هنگام استفاده از یک فایروال است (این برخلاف SSL است که می تواند از پورت TCP 443 استفاده کند تا آن را از ترافیک معمولی HTTPS متمایز نکند). از سوی دیگر، رمزنگاری IPsec با استفاده از الگوریتمی مانند AES بسیار ایمن در نظر گرفته می‌شود و به عنوان یک استاندارد "غیر عملی" در نظر گرفته می‌شود.

(ب)OpenVPN یک فناوری متن‌باز بسیار جدید است که از پروتکل‌های کتابخانه Open Secure Sockets Layer (OpenSSL) [۹] و [10] SSLv3/TLSv1 (TLS مخفف امنیت لایه حمل‌ونقل) استفاده می‌کند که توسط شرکت OpenVPN (6200Stoneridge Mall Road Pleasanton, CA 94588, USA) ارائه شده است. این می تواند یک راه حل VPN قوی و قابل اعتماد ارائه دهد. می توان آن را به گونه ای تنظیم کرد که در هر پورتی از جمله TCP 443 اجرا شود. پروتکل انتقال پیش‌فرض آن UDP با پورت ۱۱۹۴ است. استفاده از پورت TCP 443 باعث می‌شود که ترافیک آن از ترافیک HTTPS قابل تشخیص نباشد و بنابراین مسدود کردن آن بسیار دشوار است. یکی دیگر از مزایای OpenVPN این است که کتابخانه OpenSSL چندین الگوریتم رمزگذاری (مانند AES، Blowfish، 3DES، CAST-128 و غیره) را فراهم می کند [۱۱]. سرعت اجرای یک اتصال OpenVPN به سطح کدگذاری مورد استفاده بستگی دارد، اما به طور کلی سریعتر از IPsec است.

(پ)پروتکل سوکت تونلینگ امن (SSTP)[۱۲] توسط مایکروسافت (Redmond، WA، USA)در ویندوز ویستا SP1 معرفی شد و اگرچه در حال حاضر برای هر پلتفرم لینوکس در دسترس است، اما هنوز هم تا حد زیادی یک پلتفرم ویندوز است. SSTP از SSL v3

استفاده می‌کند و مانند OpenVPN کار می‌کند (همچنین توانایی استفاده از TCP پورت ۴۴۳ برای جلوگیری از مشکلات دیواره آتش NAT را دارد). این سیستم در ویندوز یکپارچه شده است و ممکن است استفاده از آن آسان‌تر و پایدارتر در نظر گرفته شود.

(ت)پروتکل تونل زنی نقطه به نقطه (PPTP)[۱۳] یک محصول ماکروسافت برای ایجاد شبکه‌های تلفنی مبتنی بر VPN است، که از دیرباز پروتکل استانداردی برای شرکت‌های خصوصی بوده‌است. این یک پروتکل VPN مبتنی بر روش‌های مختلف احراز هویت است که قادر به تضمین امنیت است، به عنوان مثال، پروتکل احراز هویت دست تکانی چالش مایکروسافت v2 (MS - CHAP) با تغییر MS - CHAP –v2با پروتکل احراز هویت توسعه‌پذیر حفاظت‌شده (PEAP)سطح امنیتی PPTP افزایش می‌یابد، اگرچه توصیه می‌شود که از L2TP / IPsec [۸] یا پروتکل تونل زنی سوکت امن (SSTP)[۱۲] استفاده شود.PPTP یک کلاینت یکپارچه را برای تقریباً همه پلتفرم ها از جمله گوشی های هوشمند ارائه می دهد. اجرای آن نیاز به سربار محاسباتی بسیار کم دارد و راه اندازی آن بسیار آسان است و مدیریت سریع داده را ممکن می سازد.

(ث) نسخه تبادل کلید اینترنت نسخه ۲ (IKEv2)یک پروتکل تونل زنی مبتنی بر IPSec است که توسط مایکروسافت و سیسکو (San Jose، CA، USA)توسعه‌یافته و به صورت پیش‌فرض در ویندوز ۷ و بالاتر نصب شده‌است. این یک پروتکل VPN واقعی نیست، بلکه یک پروتکل کنترل برای تبادل کلید IPSec است که توسط دستگاه‌های بلک بری (Waterloo، ON، Canada) پشتیبانی می‌شود. این قابلیت را می توان به صورت مستقل توسعه داد و به صورت باز شدن مجدد در لینوکس، BSD و دیگر OSes های اختصاصی اجرا کرد. IKEv2 استقرار مجدد خودکار یک اتصال VPN را زمانی فراهم می‌کند که کاربران به طور موقت اتصالات اینترنتی خود را از دست می‌دهند؛ علاوه بر این، از پروتکل‌های تحرک و چند شکلی پشتیبانی می‌کند [۱۷]. این ویژگی برای کاربران تلفن همراه که برای مثال تلفن‌های هوشمند خود را به یک شبکه WiFi وصل می‌کنند عالی است، اما سپس براساس بهترین سیگنال یا دسترسی به WiFi به اتصال داده تلفن همراه روی می‌آورند. IKEv2 از PPTP، SSTP و L2TP سریع‌تر است، چون شامل سربار مربوط به آن نمی‌شود. با پروتکل‌های نقطه به نقطه (PPP) این سیستم بسیار پایدار و ایمن است (رمزهای AES۱۲۸، AES۱۹۲، AES۲۵۶ و ۳ DES را پشتیبانی می‌کند) و نصب آن سمت کلاینت آسان است، اگرچه هنوز در بسیاری از پلتفرم‌ها پشتیبانی نمی‌شود.

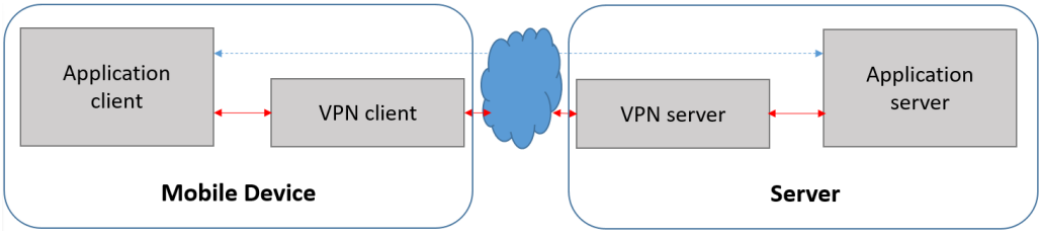
۲،۲. راه‌حل‌های احتمالی هنگام مواجهه با تحرک در VPN ها

چندین نقش در این تحقیق برای مقابله با تحرک در VPN ها وجود داشته‌است. زمانی که تونل باید در طول جلسات تلفن همراه حفظ شود، کلاینت VPN باید قادر به ارائه اطلاعات جلسه کافی باشد. به منظور اجتناب از این تبادل داده‌های پیوسته بین کلاینتها و سرورها، مکانیزم‌های ذخیره‌سازی پیشنهاد شده‌اند [۱۸]، که تلاش می‌کنند قطع ارتباط یا اتصال مجدد تونل‌های VPN را در لایه کاربرد پنهان کنند (به طور شفاف برای کاربران). در واقع، نویسندگان [۱۹] روشی را برای اصلاح OpenVPN به منظور غلبه بر مساله قطع مکرر کلاینت ارائه کرده‌اند. ایده آن‌ها مبتنی بر ذخیره‌سازی بسته‌هایی است که به رسمیت شناخته نشده اند و از آن‌ها اجتناب می‌شود. از دست دادن داده‌ها، تنزل خدمات و عملیات مرتبط با ارسال مجدد TCP (مانند شروع کند و غیره)که توان عملیاتی کلی را کاهش می‌دهد.

نوع دیگری از پیشنهادی که برای غلبه بر اثرات تحرک VPN ها معرفی شده است، تقسیم اتصال است که توسط چندین فروشنده عمدتاً Columbitech که اخیراً با Sectra Communications ادغام شده است (Kirjatyöntekijänkatu 14, 00170 Helsinki, Finland) [۲۰،۲۱]. راه‌حل نرم‌افزاری پیشنهادی، VPN موبایل نامیده می‌شود که دسترسی امن و قابل‌اطمینان به داده‌ها و برنامه‌های کاربردی را برای کاربران سیار فراهم می‌کند. این راه‌حل از یک احراز هویت دو عاملی با رمزگذاری AES 256 بیتی پشتیبانی می‌کند. هسته اصلی این ایده شامل تقسیم اتصال به سه اتصال فرعی است: (a)اتصال TCP / UDP بین برنامه کاربردی و

کلاینتها VPN (نصب‌شده بر روی دستگاه سیار)، (b)اتصال UDP بین کلاینت VPN و سرور VPN، و (c)اتصال TCP / UDP بین VPN و سرورهای برنامه.

به این ترتیب، برنامه کاربردی بر روی دستگاه تلفن همراه به طور مستقیم به سرور برنامه کاربردی متصل می‌شود، در حالی که تنها به کلاینت VPN متصل است (همانطور که در شکل ۱ نشان‌داده شده‌است). نشست VPN بین کلاینت سیار و سرور توسط امنیت لایه انتقال بی‌سیم(WTLS)راه‌اندازی شده‌است [۲۲].



شکل ۱. نمونه ای از تکنیک تقسیم VPN: اتصال تقسیم (خطوط محکم) و اتصال شفاف (خط نقطه چین).

نویسندگان [۲۳] یک رویکرد جدید را برای فراهم کردن جلسات تلفن همراه OpenVPN برای کاربران در حال حرکت بین سلول‌های WiFi پیشنهاد کردند. ایده اصلی شامل پیکربندی مجدد تونل OpenVPN بلافاصله پس از رویدادهای تحویل کاربر تلفن همراه است. این امر با اطلاع‌رسانی به سرور VPN در مورد تونل VPN جدید پس از اینکه کاربر سیار آدرس جدید را دریافت می‌کند، به دست می‌آید. برخلاف روش‌های ذخیره‌سازی، از اتلاف بسته اجتناب نمی‌شود بلکه به سادگی به حداقل می‌رسد. تعداد بسته‌های گم‌شده به طور مستقیم متناسب با زمان صرف‌شده توسط کاربران تلفن همراه برای تکمیل عملیات تحویل است. در [۲۴]، یک بسط از Sell امن (SSH)پیشنهاد شده‌است تا به برنامه‌های کاربردی این امکان را بدهد که بعد از یک قطع فیزیکی کوتاه و موقتی از شبکه، جلسات خود را ادامه دهند. هسته اصلی این ایده امکان از سرگیری یک اتصال از قبل ایجاد شده می‌باشد، اگرچه اتصالات TCP جدید باید پس از اتصال مجدد ایجاد شوند. برای انجام این کار، یک بافر اطلاعات سوکت قبلی را ذخیره می‌کند، سپس کپی می‌شود و پس از ایجاد سوکت جدید دوباره ارسال می‌شود. در این نوع رویکرد، زمانی که کلیدهای جلسه جدید مجبور به مذاکره مجدد شوند، مقدار سربار غیر قابل چشم پوشی معرفی می شود. کار در [۲۵] تلاش گروه کاری سیار شبکه IETF را توصیف و افزایش می‌دهد [۲۶].

نویسندگان طرح تحرک امن شبکه خود (SeNEMO)را به عنوان تعمیمی از VPN موبایل از [۲۴]، معرفی پروتکل آغاز جلسه (SIP)و پیاده‌سازی یک سیستم جدید اختصاص‌داده‌شده به برنامه‌های زمان واقعی در VPN پیشنهاد کرده‌اند. عملکرد ایده پیشنهادی توسط چندین مدل تحلیلی و شبیه‌سازی تایید شده‌است.

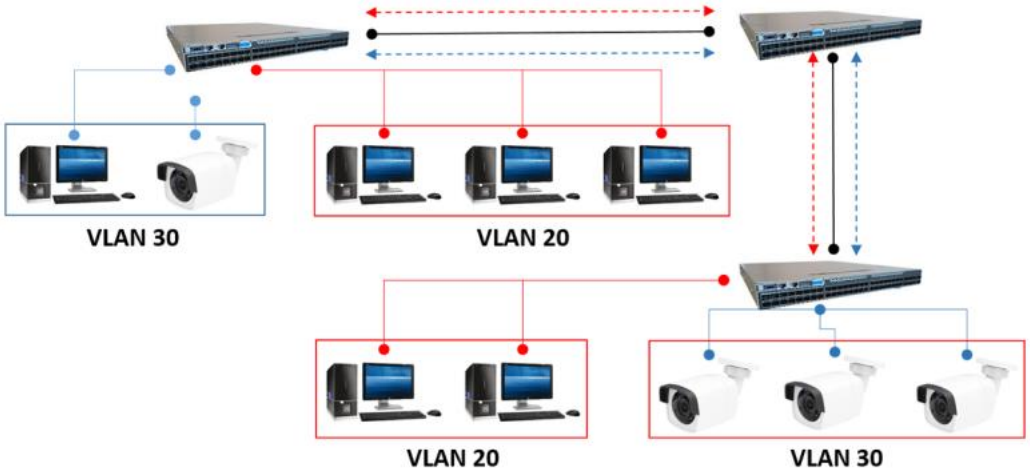
۳. قطعه‌بندی شبکه محلی مجازی در شبکه‌های استاتیک و دینامیک

همانطور که قبلا ذکر شد، با VPN می توان یک "تونل" بین دو دستگاه ارتباطی ایجاد کرد که از ارتباطات ایمن و مرور امن اینترنت پشتیبانی می کند. در چنین پیکربندی، بسته اصلی (شامل داده ها و سرصفحه های آنها، که ممکن است حاوی اطلاعاتی مانند آدرس مبدا و مقصد، نوع اطلاعات ارائه شده، طول و شماره توالی بسته) رمزگذاری شده است. سپس در بسته دیگری کپسوله می‌شود که فقط حاوی آدرس‌های IP دو دستگاه ارتباطی (i.e., routers) است. این پیکربندی از ترافیک و محتویات آن در برابر دسترسی غیرمجاز محافظت می‌کند و اجازه دسترسی به VPN را فقط برای دستگاه‌هایی با «کلید» صحیح می‌دهد. دستگاه های شبکه بین سرویس گیرنده و سرویس دهنده قادر به دسترسی یا مشاهده داده ها نخواهند بود. تفاوت اصلی بین HTTPS (SSL/TLS) و VPN در این است که

HTTPSفقط داده های واقعی یک بسته را رمزگذاری می کند، در حالی که با VPN می توان کل بسته را رمزگذاری کرد و برای ایجاد یک بسته کپسوله کرد بنابراین، VPN یک روش امن برای اتصال به یک شبکه خصوصی از طریق یک شبکه عمومی نا امن مانند اینترنت فراهم می کند.

یک جایگزین معتبر برای VPN، فن‌آوری شبکه محلی مجازی (VLAN)است. این روش به شبکه‌ها اجازه می‌دهد تا به صورت منطقی گروه‌بندی شوند نه با مکان فیزیکی، و تقسیم‌بندی شبکه به شبکه‌های مجازی یا گروه‌های مجازی را ممکن می‌سازد (یک ویژگی که توسط اکثر سوئیچ‌های شبکه پشتیبانی می‌شود). تنها کاربران در یک گروه خاص می‌توانند داده‌ها را تبادل کنند یا به منابع خاصی در شبکه دسترسی داشته باشند. پروتکل اصلی مورد استفاده در پیکربندی VLAN ها IEEE 802.1 Q است، که هر فریم یا بسته را با بایت اضافی برای نشان دادن شبکه مجازی که بسته به آن تعلق دارد، برچسب می‌زند.

در شکل ۲، VLAN ها بر روی کلیدهای مختلف تنظیم شده‌اند. اول، هر یک از دو LAN مختلف به VLAN 20 و VLAN 30 تقسیم می‌شوند.



شکل۲. نمونه ای از تقسیم بندی VLAN

لینک‌های بین سوییچ‌ها، داده‌ها را بین VLAN های مختلف حمل می‌کنند. تنها اعضای همان VLAN می‌توانند داده‌ها را، چه در یک شبکه و چه در شبکه‌های مختلف، مبادله کنند (مثال، تفکیک یک شبکه ویدیویی از یک شبکه شرکتی را نشان می‌دهد).

VLANها را می توان به روش های مختلف پیکربندی کرد و بسته به نوع آن، فناوری متفاوتی اعمال می شود. در عمل، ما می توانیم دو نوع برنامه کاربردی پیدا کنیم: VLAN های مبتنی بر پورت و VLAN های برچسب گذاری شده.

(۱)VLAN مبتنی بر پورت (Trunked VLAN): در داخل یک سوئیچ، هر شرکت‌کننده شبکه به یک پورت هدایت می‌شود. همچنین برای اتصال سوئیچ‌ها به یکدیگر استفاده می‌شوند. اگر دو VLAN باید از یک شبکه فیزیکی به دست آید، پورت های مرتبط به شبکه مجازی مطلوب اختصاص داده می‌شوند. پیکربندی از طریق سوئیچ‌های مختلف زمانی که نصب VLAN مبتنی بر پورت بر روی شبکه‌های کوچک اجرا شده و در داخل یک سوئیچ انجام می‌شود نیز امکان پذیر است. بنابراین، برای مثال، درگاه‌های یک تا سه در اولین سوئیچ و درگاه‌های یک در دومین سوئیچ می‌توانند به یکدیگر متصل شوند. برای انجام این کار، دو سوئیچ باید با دو کابل به یکدیگر متصل شوند و اتصالی برای هر VLAN فراهم کنند. مدیران شبکه پورت ها را به VLAN های مربوطه خود تنظیم و تخصیص می دهند. در این مورد، VLANبه عنوان ثابت تعریف می شود. اگر VLAN ها نیاز به پیکربندی متفاوت داشته باشند، هنگام پیکربندی سوئیچ، پورت ها باید دوباره توزیع شوند. علاوه بر این، هر پورت (و بنابراین، هر دستگاه متصل به آن) فقط به یک VLAN اختصاص دارد. به این نوع اتصال

"ترانکینگ" می گویند و سوئیچ ها دارای یک یا چند پورت هستند که برای این منظور طراحی شده اند. مستقل ازلایه PHY فرقی نمی کند که از کابل های مسی یا فیبر نوری یا اتصال بی سیم استفاده شود.

(۲)VLAN مبتنی بر فریم (یا VLAN برچسب‌گذاری شده): در این مورد، تخصیص به VLAN پویاتر است، به این معنا که توسط یک برچسب در قاب بسته تضمین می‌شود، که تنظیمات دائمی در سوئیچ را جایگزین می‌کند. برچسب حاوی اطلاعاتی است که نشان می‌دهد فریم به کدام VLAN تعلق دارد. هر کلید تشخیص می‌دهد که در کدام بخش ارتباط رخ می‌دهد و براساس آن، ارتباط را ارسال می‌کند. پیغام دادن. هر VLAN شماره خود را دارد. VLAN های علامت‌گذاری شده را نیز می توان به طور مستقیم بر روی کارت‌های شبکه پیاده‌سازی کرد (برای مثال، لینوکس استاندارد را به طور پیش‌فرض پشتیبانی می‌کند). ساختار چارچوب از استاندارد IEEE 802.1Q پیروی می‌کند [۲۷]، که بیش‌ترین استفاده را دارد (راه‌حل‌های دیگری نیز وجود دارد، مانند پروتکل لینک بین سوییچ سیسکو (ISL)[۲۸]، که قادر به خلاصه کردن چارچوب داده کامل برای فعال کردن چندین VLAN است).

مزیت یک VLAN برچسب گذاری شده در مقایسه با VLAN اختصاص‌داده‌شده به پورت، اتصال بین سوئیچ‌های مختلف است. برای VLAN های مبتنی بر پورت، حداقل دو کابل باید بین سوییچ‌ها قرار داده شود، زیرا هر LAN مجازی به اتصال خود نیاز دارد. از سوی دیگر، برای کنترل در VLAN های برچسب گذاری شده، تنها یک کابل مورد نیاز است، زیرا داده‌ها از طریق اطلاعات قاب توزیع می‌شوند. VLAN دقیق است و آن را به سوئیچ مقصد ارسال می‌کند، که در آن برچسب حذف می‌شود و فریم به گره مقصد درست ارسال می‌شود. اساسا، دو پروتکل برای مدیریت VLAN ها وجود دارد.

(۱)پروتکل VLAN ها: IEEE 802.1Q مرجع استاندارد برای VLAN ها است [۲۹]، به ویژه برای آن‌هایی که برچسب گذاری شده‌اند. این یک پروتکل کپسوله سازی لایه ۲ است که امکان جداسازی منطقی جریان‌های ترافیک مختلف را فراهم می‌کند، گویی آن‌ها مسیرهای فیزیکی متمایز را دنبال می‌کنند. IEEE 802.1Q فریم اصلی را کپسوله نمی کند، اما ۴ بایت به هدر اضافه می کند (شکل ۳) ۲بایت اول به برچسب شناسه پروتکل TPID مربوط می شود (بر روی 8100*0 تنظیم شده است که نشان می دهد فریم در قالب IEEE 802.1Q است) ۲ بایت بعدی،TCI Tag for Control Information (همچنین به نام VLAN Tag) است. TCI به صورت زیر تقسیم می‌شود، ۳ بیت برای نقطه اولویت کد (PCP)، مورد استفاده برای نشان دادن یک سطح اولویت برای فریم ، ۱ بیت برای Drop Eligible Indicator (DEI)، نشان دهنده توانایی پرش از فریم در صورت تراکم، ۱۲ بیت برای VLAN ID (VID)، نشان دهنده شناسه VLAN ها (تا ۴۰۹۶، اما فقط ۴۰۹۴ واقعاً موجود است، زیرا شناسه‌های ۰ و ۴۰۹۵ رزرو شده‌اند). بقیه فریم اترنت به عنوان اصلی باقی می ماند. به طور مشخص، از آنجایی که هدر تغییر می‌کند (بنابراین فریم تغییر می‌کند)، مکانیسم کپسوله‌سازی IEEE 802.1Q نیاز به محاسبه مجدد فیلد FCS در تریلر اترنت دارد.

(۲)پروتکل VLAN های تقویت‌شده: پروتکل VLAN ترانکینگ (VTP)[۳۰، ۳۱] یک پروتکل لایه ۲ اختصاصی سیسکو است، که اجازه مدیریت اطلاعات VLAN را می‌دهد، و آن را برای تمام سوییچ‌های شبکه در دسترس قرار می‌دهد. این پروتکل به وجود یک سرور VTP نیاز دارد: زمانی که یک VLAN ایجاد یا اصلاح می‌شود، اطلاعات با استفاده از اعلان‌های VTP در همه سوئیچ‌های دامنه VTP توزیع می‌شود. عملیات تبلیغات VTP شامل پیام‌های به روز رسانی دعوت در مدیریت VLAN (VLAN پیش‌فرض)است. به همین دلیل است که تمام اتصالات تنه بین سوییچ‌ها باید طوری کانفیگور شوند که ترافیک به VLAN1 اجازه دهد. برای پی بردن به این که کدام پیکربندی اخیر است، اطلاعات VTP با یک شماره بازبینی، شماره بازبینی پیکربندی VTP (CRN)ارائه می‌شود، که با هر اصلاح VLAN ها افزایش می‌یابد. اساسا سه نوع پیام وجود دارد:

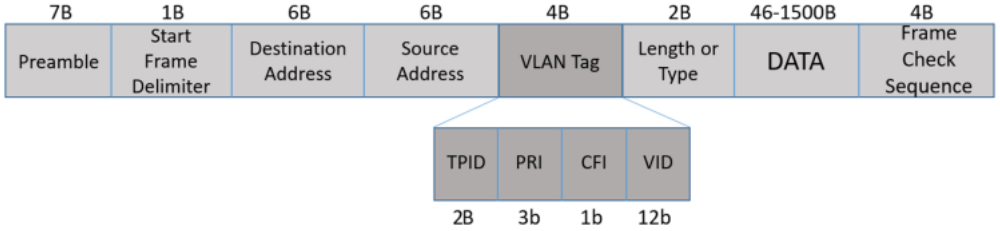
(a)خلاصه اعلان‌ها: سوییچ‌ها هر ۵ دقیقه یکبار یا به محض تغییر در پایگاه‌داده VLAN آن‌ها را ارسال می‌کنند، این پیغام‌ها حاوی نام دامنه VTP و VTP CRN هستند. اگر یک VLAN اضافه، حذف یا اصلاح شود، سرور تعداد بازبینی را افزایش می‌دهد و خلاصه به روز رسانی ارسال می‌کند.

سوئیچ یک به روز رسانی حاوی نام دامنه VTP متفاوت نسبت به نام دامنه خودش دریافت می‌کند، اطلاعات VTP به سادگی نادیده گرفته می‌شود. اگر نام منطبق باشد، آنگاه شماره بازبینی بررسی می‌شود اگر این تعداد بیشتر از شماره موجود در مالکیت باشد، یک درخواست تبلیغاتی ارسال می‌شود.

(b)درخواست‌های تبلیغاتی: کلاینتها VTP از این پیام‌ها برای درخواست اطلاعات درباره VLAN ها استفاده می‌کنند. درخواست‌های به روز رسانی بلافاصله پس از راه‌اندازی مجدد سوئیچ، تغییر نام دامنه VTP، یا شماره بازبینی جدید؛

(c)تبلیغات فرعی: به محض این که یک سرور، تغییرات در VLAN ها را دنبال می‌کند، شماره بازبینی را افزایش می‌دهد و خلاصه به روز رسانی را ارسال می‌کند، برخی پیام‌های "زیرمجموعه" حاوی اطلاعات در VLAN های فردی را دنبال می‌کند. اگر VLAN های متعددی وجود داشته باشند، پیام‌های زیرمجموعه متعددی ایجاد می‌شوند؛

شماره بازبینی را ایجاد می‌کند و خلاصه به روز رسانی را ارسال می‌کند، و برخی پیام‌های "زیرمجموعه" حاوی اطلاعات در VLAN های فردی را دنبال می‌کند. اگر VLAN های متعددی وجود داشته باشند، پیام‌های زیرمجموعه متعددی ایجاد می‌شوند:



شکل۳. فرمت فریم اترنت کپسوله شده برای IEEE802.1Q

علاوه بر این، یک سوئیچ VTP ممکن است سه نقش ممکن داشته باشد:

(a)سرور: این حالت پیش‌فرض است که در آن VLAN ها می‌توانند ایجاد، حذف و تغییر یافته، و همچنین توانایی تنظیم نسخه VTP. سپس کلیدهای سرور با دیگر کلیدهای حوزه VTP از طریق اتصالات تنه، هر ۵ دقیقه یا بلافاصله براساس یک رویداد جدید هماهنگ می‌شوند.

(b)کلاینت: این حالتی است که اجازه می‌دهد همه تغییرات در پایگاه‌داده VLAN دریافت شوند. سوئیچ می‌تواند به روز رسانی های دریافتی را ارسال کند، اما نمی‌تواند اطلاعات پایگاه‌داده VTP را تغییر دهد. با این حال، اگر ...

اطلاعات ارسال‌شده "شماره بازبینی" بالاتری نسبت به اطلاعات موجود بر روی کلاینتها و سرورها دارد، به صورت محلی اصلاح خواهد شد، یعنی پایگاه‌داده VLAN محلی به روز رسانی خواهد شد.

(c)شفاف: در این حالت سوئیچ در هیچ حوزه VTP شرکت نمی‌کند؛ با این حال، انتقال اطلاعات VTP به پورت های تنه را انجام می‌دهد، در نتیجه از قطع در تبادل اطلاعات بین گیرنده و سرور جلوگیری می‌کند.

هر دو VLAN و VPN راه‌حل‌های خوبی برای مدیریت دسترسی به شبکه براساس خواسته‌های اجرایی هستند. VLAN ها زمانی مناسب‌تر هستند که یک سازمان بخواهد شبکه محلی موجود را به بخش‌های کوچک‌تر تقسیم کند تا به کنترل بهتری برسد. با توجه به حفاظت و امنیت، در عوض VPN انتخاب بهتری است. جدول ۱ مقایسه مختصری را بین ویژگی‌های اصلی VPN ها و VLAN نشان می‌دهد.

جدول ۱. مقایسه بین VLAN و VPN.

VPNs	VLANs
آنها از سطح یک تا سطح سه عمل می کنند	صرفا یک ساختار سطح دو
یک زیر شبکه کوچکتر در یک شبکه موجود بزرگتر ایجاد می‌کند نسبت به VLAN	برای گروه بندی چندین رایانه استفاده می شود که معمولاً در داخل آنها قرار ندارند همان مناطق جغرافیایی در همان حوزه پخش
برای انتقال امن داده ها بین دو مجزا استفاده می شود موجودیت ها (مورد نقطه به نقطه)	آنها می توانند رایانه های موجود در یک شبکه محلی بزرگتر را به شبکه ها برای هر اداره یا بخش کوچکتر جدا کنند
یک تونل مجازی برای انتقال امن داده ها از طریق اینترنت ایجاد می‌کند.	آنها می توانند از داده ها محافظت کنند تا طوری رفتار نکنند که انگار در همان شبکه هستند حتی اگر روی همان سوئیچ باشد.
رمزگذاری و ناشناس سازی را ارائه می‌دهد	آنها امکان گروه بندی دستگاه های پراکنده در چندین فیزیکی را فراهم می کنند، مکان ها در یک حوزه انتقال واحد.
آنها کارایی کلی یک شبکه را که درچندین مکان جغرافیایی توزیع شده اند، افزایش می دهند	آنها را می توان به عنوان زیر مجموعه ای از VPN ها در نظر گرفت.
در یک محیط آنلاین ناامن عمل می کند	بهینه برای تقسیم یک شبکه به بخش های منطقی برای مدیریت بهتر ، اما آنها هیچ ویژگی امنیتی ارائه نمی دهند.
با ارائه یک اتصال رمزگذاری شده از طریق اینترنت، کاربران را قادر می سازد تا داده های حساس را به طور قابل اعتماد ارسال و دریافت کنند.	کاهش نیاز به روترها و هزینه های مدیریت آنها.
آنها به شرکای اتصال اجازه می دهند تا به طور ایمن انتقال داده های حساس را انجام دهند.	آنها تاخیر در شبکه را حذف می کنند و کارایی آن را بهبود می بخشند، مدیریت و مقیاس پذیری آن را تسهیل می کنند و منابع شبکه HW را ذخیره می کنند.
کاهش تلاش های دسترسی توسط هکرهای مخرب توسط سوء استفاده از هرگونه اطلاعات محرمانه.	آنها از برچسب لایه دو فریم برای کپسوله کردن استفاده می کنند و مقیاس آنها می تواند تا ۴۰۰۰ VLAN باشد.

۴. مدیریت تحرک عملی در صحنه‌های مدرن

با گسترش عظیم دستگاه‌های تلفن همراه، و بنابراین، انواع مختلف تحرک (عابر پیاده، وسایل نقلیه، مستقل، سواری، و غیره)، شبکه‌های مدرن باید تاثیرات حرکت را تطبیق دهند، به شدت به لایه فیزیکی دستگاه‌های درگیر منتقل شوند (تغییرات داپلر، محوشدگی، از دست دادن مسیر، سایه اندازی، بازگشت، شکست، و غیره). راه‌حل‌های استاندارد، مانند VLAN ها و VPN ها، که در اصل برای شبکه‌های استاتیک طراحی شده‌اند، ذاتا برای مدیریت تحرک آماده نیستند، بنابراین چندین راه‌حل پیشنهاد شده‌اند. در این بخش، راه‌حل‌های اصلی موجود را مرور می‌کنیم که فرصت مدیریت تحرک را می‌دهند، در حالی که مزایای راه‌حل‌های قبلی را حفظ می‌کنند.

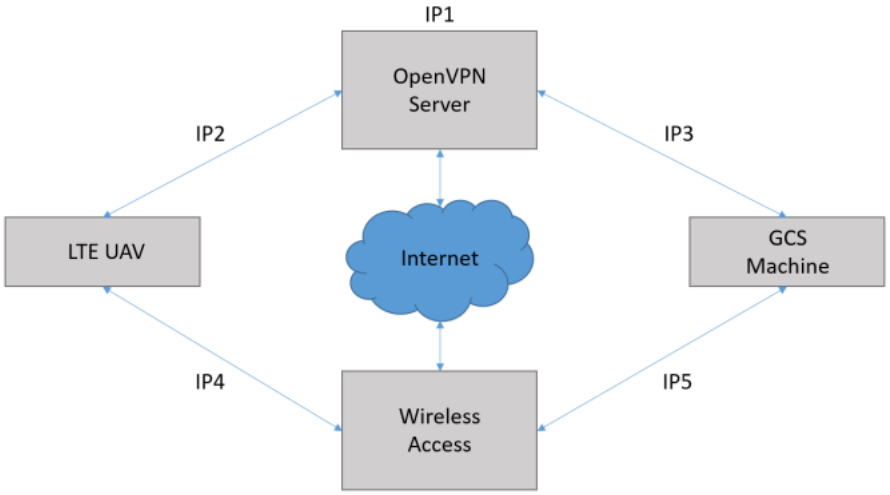
۴،۱ مقابله با تحرک از طریق برنامه‌های VPN

WireGuard [۳۲-۳۵] یک نرم افزار رایگان (علائم تجاری ثبت شده Jason A. Donenfeld) است. اخیراً در بازار فناوری اطلاعات برای ایجاد VPN تأسیس شده است.

تنظیم دسترسی به منابع شبکه خاص و جدا کردن داده‌های کاربران از دنیای خارج. همچنین به عنوان نرم‌افزار نسل آینده شبکه کرنل تونل [۳۶] شناخته می‌شود و به چارچوب پروتکل نویز تعلق دارد [۳۷]. این یک ابزار رایگان تحت مجوز GPLv2 است، که به زبان‌های C و Go نوشته شده و با Windows، macOS، BSD، iOS و اندروید کار می‌کند. این الگوریتم بهینه‌سازی‌هایی را برای دستگاه‌های تلفن همراه و سیستم‌های IoT ارائه می‌دهد. با توجه به ویژگی‌های عالی آن، به طور مستقیم با هسته لینوکس ترکیب شده‌است، و آن را به صورت مجازی در تمام دستگاه‌های متصل در سراسر جهان در دسترس قرار داده‌است، که این امر نیز امکان پذیر است چون نسبتا سبک است و الزامات سخت‌افزاری بسیار کمی دارد. امنیت براساس چیزی است که به آن معروف است.

رمزنگاری مسیریابی، که در آن آدرس‌های IP تونل در یک حالت یک به یک به کلید عمومی peer's برای رمزگشایی بسته‌های ورودی اختصاص داده می‌شوند، که تنها در صورتی تحویل داده می‌شوند که از آدرس متناظر با کلید باشند. گارد امنیتی در مورد پایگاه‌های رمزنگاری دست دادن به صورت جداگانه مذاکره نمی‌کند، بلکه تنها زیر مجموعه‌ای از آن‌ها است. اگر یکی از پایگاه‌های رمزنگاری دیگر امن نباشد، نسخه جدیدی از پروتکل برای حفاظت از داده منتشر می‌شود. یکی از نقاط قوت نگهبان سیمی کد پایه آن است، که شامل حدود ۴۰۰۰ خط کد در مقایسه با خطوط OpenVPN یا IPsec است که به ترتیب ۱۰۰۰۰ و ۶۰۰۰۰۰ هستند، و بنابراین ذاتا امن‌تر است زیرا به راحتی قابل نگهداری و با حداقل سطح حمله است. این کدباز امنیت بیشتر و امنیت بیشتر را تضمین می‌کند.

پایگاه کد امنیت بیشتر و عملکرد بالاتر را تضمین می کند. با ارائه سرعت انتقال بالاتر و تأخیر کمتر نسبت به پروتکل‌های تاریخی، اگر هیچ داده‌ای از تونل عبور نمی‌کند، WireGuardدر حالت استراحت است، بنابراین میزان انرژی مصرف‌شده را کاهش می‌دهد. به لطف پشتیبانی رومینگ از شبکه Wi-Fi به شبکه تلفن همراه و بالعکس، ویژگی های بسیار مفیدی را برای استفاده در دنیای تلفن همراه و IOTارائه می دهد. در واقع، در [۳۳]، پروتکل زیربنایی WireGuard به طور عمیق توسط دستیار اثبات CryptoVerif تجزیه و تحلیل و آزمایش می شود. نویسندگان تجزیه و تحلیل گسترده و عمیقی از پیام‌های سیگنالینگ WireGuard (مانند پیام‌های داده‌های انتقال) انجام دادند و خوب بودن VPN را از نظر محرمانه بودن، احراز هویت، منحصربه‌فرد بودن جلسه، حملات مجدد و غیره اثبات و تأیید کردند. نویسندگان [۳۴] در عوض، نشان داد که چگونه امنیت داده ها را می توان توسط WireGuard در یک VPN واقعی، شامل یک آزمایشگاه و چندین دانشگاه آفریقایی تضمین کرد. نویسندگان WireGuard و Apache Guacamole را با هم ترکیب کردند و قدرت VPNدر نظر گرفته شده را از نظر استحکام رازداری آزمایش کردند. در[۳۵]، WireGuard VPNدر زمینه برش شبکه ۵ Gبرای موفقیت در عملکرد امنیتی آن در نظر گرفته شده است .اهمیت [۳۵] شامل نمایش عملی قدرت Wireguard است که با اجرای یک شبکه واقعی، ایمن، پروتکل تونل زنی در یک شبکه ۵ Gواقعی انجام می شود که عملکردهای شبکه مجازی را ارائه می دهد. نفوذ OpenVPNبه بازار و Wireguard با ادغام آنها در برخی از دستگاه های ثابت و موبایل جدید، مانند پهپادها و 37) RaspberryPi Hills Rd، Cambridge CB2 1NF، (UK (از نسخه دو به بعد) و همچنین در پیشرفته ترین سیستم های حسگر اینترنت اشیا، حتی اگر همیشه می‌توان از نرم‌افزاری مانند OpenWRT [۳۸،۳۹] به عنوان واسطه MQTT [۴۰-۴۲] در نقاط پایانی برای انتقال ایمن ترافیک استفاده کرد. شکل ۴ یک مورد استفاده معمول از VPN (که می تواند توسط WireGuard ادغام شود) را بر روی یک اتصال بین یک وسیله نقلیه هوایی بدون سرنشین متصل به LTE (یا متصل به 5G) و ایستگاه کنترل زمینی (GCS) نشان می دهد، که می تواند همچنین از طریق LTE یا 5G متصل شود.



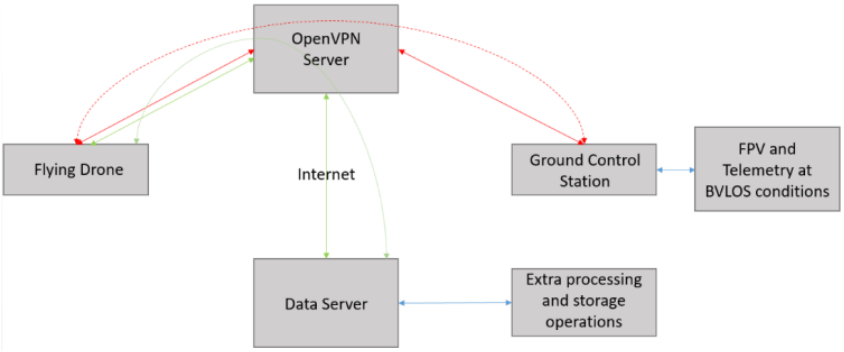
شکل۴. نمونه ای از مدیریت VPN برای وسیله نقلیه هوایی بدون سرنشین (پهپاد) و یک دستگاه ایستگاه کنترل زمینی (GCS) تکامل طولانی مدت (LTE).

هم UAV و هم GCS آدرس‌های IP خود را براساس ارائه‌دهنده خدمات خود دارند (ما فرض می‌کنیم که UAV به طور مستقیم به GCS متصل نیست، زیرا آدرس‌های IP آن‌ها برای یکدیگر قابل‌رویت نیستند).

مدیریت صحیح می‌تواند توسط یک VPN (شکل ۴)به دست آید، ما فرض می‌کنیم که سرور آدرس استاتیک IP1 دارد، در حالی که UAV آدرس IP4 خود را از شبکه بی‌سیم LTE و همچنین GCS با IP5 به دست آورده‌است. سرور OpenVPN بر روی دستگاه IP1 اجرا می‌شود، در حالی که کلاینتها OpenVPN بر روی دستگاه‌های IP4 (UAV)و IP5 (GCS)اجرا می‌شوند، بنابراین آن‌ها می‌توانند آدرس‌های VPN را همانطور که نشان‌داده‌شده دریافت کنند، یعنی IP2 برای UAV .

IP3 برای GCS آدرس‌های IP2 و IP3 به شبکه VPN مشابه تعلق دارند، بنابراین UAV می‌تواند به طور مستقیم با GCS ارتباط برقرار کند. علاوه بر این، در [۴۳]، یک اتصال امن UAVs با GCSs از طریق VPN ارائه شده‌است (شکل ۵). نویسندگان امکان استفاده از یک اتصال 4G برای ارتباط مستقیم با یک سرور داده (سبز و خط نقطه‌چین کوتاه)را نشان دادند، که در آن داده‌های "جالب" (صوتی، تصویری، تله‌متری و غیره)می‌توانند برای پردازش بیشتر ذخیره شوند. اتصال VPN دوم (خط نقطه‌چین طولانی قرمز)بین هواپیماهای بدون سرنشین و GCS، به منظور اجرای عملیات نمایش اول شخص (FPV)در خط دید (LOS)یا فراتر از LOS بصری تحقق می‌یابد.

شرایط (BVLOS). ایده مبتنی بر VPN پیشنهادی قادر به ایجاد یک اتصال با دامنه بلند و ظرفیت بالا می‌باشد (آن‌ها آزمایش‌ها بر روی جریان صوتی و تصویری را با ایجاد تونل VPN به سمت اینترنت عمومی و به سمت GCS پایه‌ریزی کرده‌اند). معماری پیشنهادی بر نیاز به غلبه بر مسائل امنیتی در سناریوهای UAVs تاکید دارد [۴۵].



شکل۵. یک نمایش منطقی از معماری VPN در نظر گرفته شده در [۳۷].

۴ - ۲ مسائل و راه‌حل‌های احتمالی هنگام برخورد با تحرک در VLAN ها یکی از مسائل اصلی در زمان برخورد با VLAN در محیط‌های سیار، مدیریت آدرس‌های IP است. به طور کلی، سرورهای DHCP مسئول تخصیص آدرس IP هستند، اما افزایش عظیم در دستگاه‌های تلفن همراه موجود، چالش‌های بزرگی را در ارتباط با عملکرد DHCP ایجاد می‌کند. یک اقدام متقابل با تنظیم مجدد زمان‌های اجاره IP نشان داده می‌شود و آدرس به صورت پویا ذخیره می‌شود و آن‌ها را با رفتار کاربر WiFi سازگار می‌کند. در حالت اول، زمان‌های اجاره براساس الگوی زمانی تاریخی برای بازیابی آدرس‌های IP تنظیم می‌شوند، در حالی که در حالت دوم آدرس‌های IP در سراسر VLAN ها مهاجرت می‌کنند.

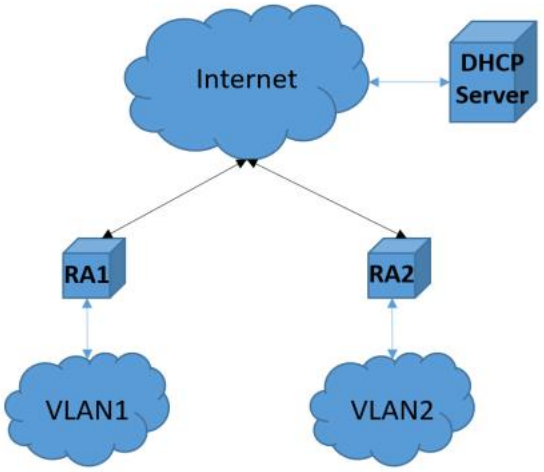
اساس همبستگی تحرک فضایی - زمانی CEC است. با توجه به منابع آدرس، برای تعداد بیشتری از کلاینتها، پیام‌های DHCP (به طور کلی پیام‌های پخش)پهنای باند بیشتری مصرف خواهند کرد. راه‌حل اصلی تقسیم شبکه کلی به زیرمجموعه‌ای از VLAN ها بدون اجرای سرور DHCP برای هر VLAN است. بهره‌برداری از مزایای استفاده از یک عامل رله DHCP [۴۷] برای هر VLAN ممکن است، که قادر به تغییر ویژگی‌های بسته DHCP پخش‌شده توسط کلاینت در دامنه پخش خود و ارسال آن به سرور DHCP است (شکل ۶). به این ترتیب، بیشتر ترافیک از شبکه قطع می‌شود و خروجی کلی را افزایش می‌دهد.

با توجه به زمان اجاره IP، سه حالت اصلی برای اجاره یک آدرس وجود دارد:

(a)مقداردهی اولیه: آدرس IP پس از مجموعه‌ای از تبادلات پیام بدست می‌آید (پیام را از کلاینت C برای پخش B کشف کنید، پیام را از سرور S به C، پیام درخواست تک پست را از C به S و تایید را از S به C ارائه دهید)؛

(b)برگرداندن: در این حالت، یک پیغام توسط کلاینت (اگر هنوز در شبکه وجود داشته باشد)به سرور فرستاده می‌شود، و درخواست تمدید (در زمان)اجاره می‌دهد؛ این یک پیام دوره‌ای است (دوره برابر با نصف زمان اجاره است)؛

(c)انتشار: این حالت در صورتی رخ می‌دهد که گیرنده یک پیام انتشار روشن را به سرور ارسال کند (زیرا می‌خواهد شبکه را ترک کند)یا اگر پیام تمدید دوره‌ای ارسال نشده باشد. پس از این ملاحظات، روشن است که زمان اجاره باید به اندازه کافی تنظیم شود: اگر خیلی بالا باشد، مخزن آدرس می‌تواند به زودی از کار بیفتد، در حالی که اگر خیلی پایین باشد، سرورهای DHCP می‌توانند بیش از حد بارگذاری شوند. بنابراین، یکی از بهترین راه‌حل‌ها ارزیابی رفتار کاربران از نظر درخواست‌های DHCP است، و سپس زمان اجاره به شبکه به صورت مورد نیاز از نظر الگوی زمانی آنلاین برای بازیابی IP در زمان است.



شکل۶. ساختار معمولی یک شبکه تقسیم‌بندی شده VLAN و حضور عوامل رله DHCP (RAs) [۴۰].

۵. اجرای امنیت واقعی برای VPN ها و VLAN ها

این بخش به تشریح مسائل امنیتی و اقدامات متقابل مربوط به VPN ها و VLAN ها اختصاص دارد.

مثال‌هایی از اسناد واقعی به منظور یادگیری نحوه پیکربندی مناسب دستگاه‌ها ارائه شده‌است.

۱,۵مسائل امنیتی و اقدامات متقابل در VLAN ها

در این بخش، ما بر روی امنیت VLAN و نحوه اعمال آن در یک محیط شرکتی تمرکز می‌کنیم. به عنوان یک مرجع، ما از سوئیچ‌های سیسکو استفاده می‌کنیم،

قانون کلی، علاوه بر این، اجتناب از استفاده از ترافیک داده‌های VLAN 1 (VLAN پیش‌فرض)و هرس VLAN است. VLAN پیش‌فرض در تمام دستگاه‌های شبکه وجود دارد و همچنین برچسب نخورده است، زیرا برای تبادل اطلاعات از طریق پروتکل‌ها مانند پروتکل کشف سیسکو (CDP)و VTP استفاده می‌شود. یک تکنیک خوب دیگر که یک مدیر شبکه باید در نظر بگیرد، اصلاح است، که تنها VLAN های ضروری را در هر لینک مجاز می‌داند.

ویژگی کلیدی دیگر برای امنیت VLAN، محدودیت مسیریابی بین VLAN از طریق لیست‌های دسترسی است. مسیریابی بین VLAN باید مجاز باشد، اما برای اطمینان از سطح بالاتری از امنیت، مسیریابی می‌تواند به اندازه کافی محدود شود [۴۸].

برخی مثال‌های پیاده‌سازی VPN واقعی را می توان در [۴۹ - ۵۱] یافت.

۲,۵ مسائل امنیتی و اقدامات متقابل در VPN ها

امروزه، تمام دستگاه‌های شبکه، عملکردهای VPN را فراهم می‌کنند. اول از همه، یک حفاظت VPN پایه شامل دیواره آتش است که باید همیشه در یک شبکه وجود داشته باشد. اکثر راه‌حل‌های امنیتی اخیر، ادغام دیواره‌ای آتش با سیستم‌های تشخیص نفوذ پیچیده (IDS)[۵۲] یا سیستم‌های پیش‌گیری از نفوذ (IPSs)[۲۳، ۵۳] را به منظور بهبود عملکرد امنیتی VPN نشان می‌دهند. ما یک مقدمه کوتاه به IDS ها خواهیم داد، سپس ادغام آن‌ها با VPN ها نشان داده خواهد شد.

۱,۲,۵.IDS ها، IPSs ها و سیستم‌های تشخیص و پیش‌گیری از نفوذ (IDPSs)

IDS به یک مولفه نرم‌افزاری یا یک دستگاه سخت‌افزاری با یک نرم‌افزار اختصاصی تعبیه‌شده اشاره می‌کند که برای تحلیل ترافیک در حال انتقال به یا از یک شبکه خاص که در آن نصب شده‌است، سازگار شده‌است. هدف از داشتن یک IDS در یک شبکه (معمولا یک LAN)نظارت بر ترافیک به منظور شناسایی هر چیزی است.

فعالیت مشکوک و / یا فعالیت مخرب نسبت به هر میزبان (چه گیرنده و چه سرور)در شبکه. چنین سیستم‌هایی اغلب قادر به ایجاد هشدار و ثبت فایل‌ها براساس فعالیت‌ها یا تجزیه و تحلیل خود هستند که آن‌ها به پایگاه‌داده‌های رابطه‌ای دسترسی خواهند داشت، در حالی که اطلاعات مربوط به ترافیک شبکه خاص را ذخیره می‌کنند که از نقطه‌نظر مدیر شبکه "جالب" است.

به جای آن، یک IPS متشکل از یک جز نرم‌افزاری یا سخت‌افزاری است که درون یک شبکه قرار دارد و هدف آن جلوگیری از تلاش برای حمله به شبکه است. رایج‌ترین اقدامات پیشگیرانه اتخاذ شده توسط IPS عبارتند از: کنارگذاری بسته یا نشست، تنظیم مجدد نشست و اضافه کردن به یک لیست سیاه میزبانی که حمله را حرکت داد. IDS و IPS فن‌آوری‌های مکمل در زمینه امنیت شبکه هستند و قادر به کار در همکوشی هستند. هر دو براساس تطبیق بین قوانین خاص ارائه‌شده توسط شبکه و انتقال بسته‌ها فعال می‌شوند (هشدار یا پیش‌گیری). به این دلایل، IDS و IPS با هم پیاده‌سازی می‌شوند، و یک سیستم ترکیبی به نام سیستم تشخیص و پیش‌گیری از نفوذ (IDPSs)به دست می‌آورند.

چهار نوع مختلف از تکنولوژی‌های IDPS وجود دارد:

(a)IDPS های مبتنی بر شبکه (NB - IDPSs): این موارد ترافیک را با توجه خاص به لایه‌های برنامه و شبکه نظارت می‌کنند. به طور معمول آن‌ها بر روی لبه توپولوژی شبکه (قبل از دیواره‌ای آتش و دروازه)یا بر روی محدودیت‌های شدید مناطق غیر نظامی (DMZs)نصب می‌شوند؛

(b)IDPS های بی‌سیم: اینها فقط به نظارت بر ترافیک بی‌سیم، به ویژه، اختصاص داده می‌شوند.

توجه به پروتکل‌های شبکه سازی:

(c)تحلیل رفتار شبکه IDPSs (NBA - IDPSs): این ها بسته‌ها را برای شناسایی تهدیدهایی که ترافیک مشکوک غیر معمول را برای یک شبکه، مانند تلاش برای انکار پراکنده سرویس (DDoS)تولید می‌کنند، بررسی می‌کنند. آن‌ها همچنین اغلب برای نظارت بر ترافیک داخلی در همان شبکه و یا برای دسترسی به اشخاص ثالث خارجی استفاده می‌شوند.

IDPSs(d) مبتنی بر میزبان (HB - IDPSs): اینها به نظارت بر هر چیزی که

در یک میزبان واحد که به آن تعلق دارند، آن‌ها معمولا یک سرور هستند، از خارج از شبکه قابل دسترسی هستند، یا یک کلاینت با دسترسی عمومی. آن‌ها داده‌ها را از فرآیندهای در حال اجرا بر روی دستگاه، دسترسی فایل، لاگ های سیستم و غیره نظارت می‌کنند.

زمینه کلی استفاده از IDPSs کسب‌وکار است: پردازش داده‌های حساس توسط شرکت‌ها، آن‌ها را ملزم به استفاده از سیستم‌های حفاظت از داده مناسب و موثر در شبکه‌های داخلی خود به منظور جلوگیری از نقض سیاست‌های امنیتی شرکت می‌کند. اکثر IDPS از تکنولوژی‌های تشخیص مختلف، به طور بالقوه در ترکیب، برای ارائه درجه بهتری از دقت استفاده می‌کنند.

سه تکنولوژی اصلی وجود دارد:

(a)مبتنی بر امضا: مقایسه امضاهای مدیریت‌شده توسط شبکه و انتقال بسته ها انجام می‌شود. این فن‌آوری در شناسایی تهدیدهای شناخته‌شده‌ای که الگوهای حمله ایستا دارند بسیار موثر است، اما آن‌ها تقریبا در برابر تهدیدهای ناشناخته بی‌فایده هستند؛

(b)تشخیص مبتنی بر ناهنجاری آماری: این تکنولوژی براساس حفظ یک دیدگاه است.

از داده‌های آماری مربوط به جریان‌های عادی شبکه و ایجاد شرایط هشدار دهنده در هنگام انحراف پارامترهای مورد نظر از مقادیر استاندارد آن‌ها استفاده شده‌است. بدیهی است که آمارهای اولیه در مورد "فعالیت نرمال" نیاز به مطالعه مقدماتی شبکه به منظور تعیین این دارند که کدام مقادیر نرمال هستند؛

(c)تجزیه و تحلیل پروتکل قانونی: در این مورد، جریان‌های شبکه تجزیه و تحلیل می‌شوند، و آن‌ها را با پروفایل های خاص مقایسه می‌کنند (به عنوان مثال، یک کاربر دسترسی به یک سرور FTP دارد، بدون این که هنوز امتیازات احراز هویت را کسب کرده باشد). این نوع تجزیه و تحلیل بسیار پیچیده است اما در عین حال بسیار دشوار و پیچیده است زیرا پروفیل‌ها باید برای هر پروتکل ایجاد شوند و تمام موارد استفاده ممکن را با هزینه محاسباتی بالا پوشش دهند.

۲,۲,۵.ادغام IDS ها و IPSs با VPN ها

چندین کار در مقالات مرتبط با موضوع تقویت سطح امنیتی در VPN ها با IDS ها و IPSs وجود دارد. برای مثال، در [۵۲] نویسندگان حمله DoS را براساس زمینه TCP SYN در نظر گرفتند، که قادر به شروع اتصالات TCP بر روی سرورهای HTTP است.

در زمان بسیار کوتاه و به صورت دوره‌ای، با استفاده از آدرس‌های IP جعلی. البته دیواره‌ای آتش می‌توانند مانع از حمله شوند، اما قربانی می‌شوند. بنابراین لازم است که یک IDS با تشخیص به موقع ایجاد شود و در نتیجه مشکل حل شود. پس از تشخیص حمله، حمله

می‌تواند با ایجاد یک فهرست کنترل دسترسی اختصاصی (ACL)با موفقیت مسدود شود، که قادر به مسدود کردن حمله باشد. مسدود کردن خودکار DoS و حملات مشابه از طریق یکپارچه‌سازی VPN با یک IPS امکان پذیر است. در [۲۳]، نویسندگان با مساله اجرای یک IPS در شبکه‌های بی‌سیم مواجه هستند (به طور کلی راه‌حل یک WIPS بی‌سیم است): ایده آن‌ها VPN مبتنی بر WTLS (WBVPN)نامیده می‌شود، که توسط آن یک مسیر واحد بین دستگاه بی‌سیم و مقصد آن‌ها ساخته می‌شود، و از ویژگی ازسر گیری نشست WTLS بهره‌برداری می‌کند. به این ترتیب، IPS می‌تواند ترافیک را تجزیه و تحلیل کند و از عملیات غیر مجاز جلوگیری کند. نویسندگان همچنین یک مورد واقعی را در نظر گرفتند که نشان‌دهنده عملکرد خوب طرح پیشنهادی است. مقاله در [۵۳] بر تلاش‌های اضافی تمرکز دارد که می‌تواند برای غلبه بر مسائل امنیتی در یک شبکه از طریق VPN انجام شود و یک چارچوب جدید را پیشنهاد می‌دهد. این مقاله در مورد به حداکثر رساندن همزمانی سرویس‌های امنیتی و در عین حال کاهش ترافیک هوایی بحث می‌کند. ۶. نتیجه‌گیری

در این مقاله ما دانش عمیقی از اقدامات متقابل اصلی برای جلوگیری و مبارزه با مسائل امنیتی در شبکه‌های ایستا و پویا ارائه می‌دهیم. به طور خاص، VPN ها و VLAN ها در نظر گرفته شده‌اند و تاکید ویژه‌ای بر روش‌هایی دارند که تحرک و امنیت را می توان تضمین کرد. ما تصمیم گرفتیم سهم اصلی در این زمینه‌های مورد علاقه را با توجه به تقاضای زیاد برای ارتباطات بین مکان‌های دور دست در حین حرکت با پایا در یک وسیله نقلیه خلاصه کنیم. ما بر قابلیت VPN برای اتصال دو نقطه پایانی از طریق یک تونل اختصاصی و ایمن تاکید می‌کنیم، در حالی که VLAN ها قادر به کاهش تاثیر برخی مسائل مقیاس پذیری شبکه‌های بزرگ هستند. جدیدترین راه‌حل‌ها نشان‌داده شده‌اند، که به خواننده امکان درک نحوه رفتار را می‌دهد.

شبکه شرکتی خود فرد. البته، اجرای VPN ها و VLAN ها مشکلات خاصی را در مورد امنیت ایجاد می‌کند، بنابراین برخی راه‌حل‌های خوب نیز در نظر گرفته‌شده و توصیف می‌شوند.

مسائل امنیتی در VLAN ها را می توان به طور موثری از طریق ترکیب شیوه‌های مدیریت شبکه خوب، طراحی موثر شبکه و استفاده از محصولات امنیتی پیشرفته کاهش داد. برای VPN ها، در دسترس بودن پشتیبانی احراز هویت قوی، الگوریتم های رمزگذاری قوی، پشتیبانی برای نرم‌افزار آنتی ویروس و خدمات IDS / IPS، امنیت پیش‌فرض قوی برای پورت های مدیریت و نگهداری، پشتیبانی از گواهی دیجیتال، پشتیبانی برای ضبط و حسابرسی، و توانایی تخصیص آدرس‌ها به کلاینتها در یک شبکه خصوصی در حالی که اطمینان از اینکه تمام آدرس‌ها خصوصی نگه‌داشته می‌شوند، وجود دارد.

منابع

1. De Rango, F.; Lentini, D.C.; Marano, S. Static and dynamic 4-way handshake solutions to avoid denial of service attack in Wi-Fi
protected access and IEEE 802.11i. EURASIP J. Wirel. Commun. Netw. 2006, 2006, 047453. [CrossRef]
2. De Rango, F.; Marano, S. Trust-based SAODV protocol with intrusion detection and incentive cooperation in MANET. In
Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World
Wirelessly, Leipzig, Germany, 21–24 June 2009; pp. 1443–1448.
3. Jahan, S.; Rahman, M.S.; Saha, S. Application specific tunneling protocol selection for Virtual Private Networks. In Proceedings of
the International Conference on Networking Systems and Security (NSysS), Dhaka, Bangladesh, 5–8 January 2017.
4. Lupia, A.; de Rango, F. Evaluation of the Energy Consumption Introduced by a Trust Management Scheme on Mobile Ad-hoc
Networks. J. Netw. 2015, 10, 240–251. [CrossRef]
5. De la Cruz, J.E.C.; Goyzueta, C.A.R.; Cahuana, C.D. Open VProxy: Low Cost Squid Proxy Based Teleworking Environment with
OpenVPN Encrypted Tunnels to Provide Confidentiality, Integrity and Availability. In Proceedings of the IEEE Engineering
International Research Conference (EIRCON), Lima, Peru, 21–23 October 2020.
6. Duddu, S.; Sai, A.R.; Sowjanya, L.S.; Rao, G.R.; Siddabattula, K.S. Secure Socket Layer Stripping Attack Using Address Resolution
Protocol Spoofing. In Proceedings of the 4th International Conference on Intelligent Computing and Control Systems (ICICCS),
Madurai, India, 13–15 May 2020.
7. Floissac, N.; L'Hyver, Y. From AES-128 to AES-192 and AES-256, How to Adapt Differential Fault Analysis Attacks on Key
Expansion. In Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography, Milan, Italy, 17 September 2011.
8. Luo, J.; Ji, Q. Password Acquisition and Traffic Decryption Based on L2TP/IPSec. In Proceedings of the IEEE 20th International
Conference on Communication Technology (ICCT), Nanning, China, 28–31 October 2020.
9. Gui-hong, L.; Hua, Z.; Gui-zhi, L. Building a Secure Web Server Based on OpenSSL and Apache. In Proceedings of the
International Conference on E-Business and E-Government, Guangzhou, China, 7–9 May 2010.
10. Rhee, M.Y. Transport Layer Security: SSLv3 and TLSv1. In Wiley Wireless Mobile Internet Security; Book Chapter; Wiley: New York,
NY, USA, 2013.
11. Semwal, P.; Sharma, M.K. Comparative study of different cryptographic algorithms for data security in cloud computing.
In Proceedings of the 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA),
Dehradun, India, 15–16 September 2017.
12. Kim, Y.-J.; Kolesnikov, V.; Kim, H.; Thottan, M. SSTP: A scalable and secure transport protocol for smart grid data collection. In

Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20
October 2011.
13. Jones, J.; Wimmer, H.; Haddad, R.J. PPTP VPN: An Analysis of the Effects of a DDoS Attack. In Proceedings of the IEEE
SoutheastCon, Huntsville, AL, USA, 11–14 April 2019.
14. Kent, S.; Seo, K.; Network Working Group. Request for Comments: 4301. 2005. Available online: https://www.rfc-editor.org/
rfc/pdfrfc/rfc4301.txt.pdf (accessed on 18 May 2021).
15. Socievole, A.; Caputo, A.; de Rango, F.; Fazio, P. Routing in mobile opportunistic social networks with selfish nodes. Wirel.
Commun. Mob. Comput. 2019, 2019, 6359806. [CrossRef]
16. Socievole, A.; de Rango, F.; Caputo, A. Wireless contacts, Facebook friendships and interests: Analysis of a multi-layer social
network in an academic environment. In Proceedings of the 2014 IFIP Wireless Days (WD), Rio de Janeiro, Brazil, 12–14 November
2014; pp. 1–7.
17. Karbasioun, M.M.; Berenjkub, M.; Taji, B. Securing mobile IP communications using MOBIKE protocol. In Proceedings of the
IEEE International Conference on Telecommunications, St. Petersburg, Russia, 16–19 June 2008.
18. Goff, T.; Moronski, J.; Phatak, D.S.; Gupta, V. Freeze-TCP: A true end-to-end TCP enhancement mechanism for mobile environ-
ments. In Proceedings of the IEEE INFOCOM Annual Joint Conference of the IEEE Computer and Communications Societies, Tel
Aviv, Israel, 26–30 March 2000; Volume 3, pp. 1537–1545.
19. Alshalan, A.; Pisharody, S.; Huang, D. MobiVPN: A Mobile VPN Providing Persistency to Applications. In Proceedings of
the International Conference on Computing, Networking and Communications, Wireless Networks, Kauai, HI, USA, 15–18
February 2016.
20. A VPN for a New Era, Sectra Communications. Available online: https://communications.sectra.com/product/secure-mobile-
vpn-up-to-restricted/ (accessed on 13 May 2021).
21. Columbitech App for Iphone. Available online: https://apps.apple.com/it/app/columbitech-mobile-vpn/id1046769589 (ac-
cessed on 14 April 2021).
22. Dong, L.; Kang, X.; Song, J. A WTLS-based virtual private network for wireless intrusion prevention. In Proceedings of the
International Conference on Computer Application and System Modeling (ICCASM), Taiyuan, China, 22–24 October 2010;
Volume 3.
23. Zúquete, A.; Frade, C. Fast vpn mobility across wi-fi hotspots. In Proceedings of the IEEE Security and Communication Networks
(IWSCN), 2nd International Workshop on, Karlstad, Sweden, 26–28 May 2010; pp. 1–7.
24. Schonwalder, J.; Chulkov, G.; Asgarov, E.; Cretu, M. Session resumption for the secure shell protocol. In Proceedings of the
IFIP/IEEE International Symposium on Integrated Network Management, Long Island, NY, USA, 1–5 June 2009; pp. 157–163.

25. Chen, T.-C.; Chen, J.C.; Liu, Z.H. Secure Network Mobility (SeNEMO) for Real-Time Applications. In Proceedings of the IEEE
Transactions on Mobile Computing, Abu Dhabi, United Arab Emirates, 10 October 2011; Volume 10, pp. 1113–1130.
26. Ernst, T.; Tj, K. Network Mobility Working Group, IETF. Available online: https://datatracker.ietf.org/wg/nemo/about/
(accessed on 18 May 2021).
27. Xinzhan, L.; Chuanqing, C. Discuss on VLAN Stacking in Packet Network. In Proceedings of the International Symposium on
Intelligent Ubiquitous Computing and Education, Chengdu, China, 15–16 May 2009.
28. CISCO ISL Protocol for LAN Switching. Available online: https://www.cisco.com/c/en/us/support/docs/lan-switching/8021
q/8758-43.html (accessed on 18 May 2021).
29. IEEE 802.1Q-2018—IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks. Available online:
https://standards.ieee.org/standard/802_1Q-2018.html (accessed on 25 May 2021).
30. Verma, R.O.; Shriramwar, S.S. Effective VTP Model for Enterprise VLAN Security. In Proceedings of the International Conference
on Communication Systems and Network Technologies, Gwalior, India, 6–8 April 2013.
31. Understanding VLAN Trunking Protocol, Cisco. Available online: https://www.cisco.com/c/en/us/support/docs/lan-
switching/vtp/10558-21.html?dtid=osscdc000283 (accessed on 19 May 2021).
32. WireGuard. Available online: https://www.wireguard.com/ (accessed on 22 May 2021).
33. Lipp, B.; Blanchet, B.; Bhargavan, K. A Mechanised Cryptographic Proof of the WireGuard Virtual Private Network Protocol. In
Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019.
34. Kossingou, G.M.S.; Dégboé, B.M.; Ouya, S.; Mendy, G. Mutualisation of ICT laboratory resources between West and Central
African universities in post-crisis situations: The case of Senegal and the Central African Republic. In Proceedings of the Sixth
International Conference on e-Learning (econf), Sakheer, Bahrain, 6–7 December 2020.
35. Haga, S.; Esmaeily, A.; Kralevska, K.; Gligoroski, D. 5G Network Slice Isolation with WireGuard and Open Source MANO: A
VPNaaS Proof-of-Concept. In Proceedings of the IEEE Conference on Network Function Virtualization and Software Defined
Networks (NFV-SDN), Leganes, Spain, 9–12 November 2020.
36. Donenfeld, J.A. WireGuard: Next Generation Kernel Network Tunnel. NDSS. 2017. Available online: https://www.wireguard.
com/papers/wireguard.pdf (accessed on 26 May 2021).
37. Trevor Perrin, Noise Protocol Framework. Available online: http://www.noiseprotocol.org/ (accessed on 27 May 2021).
38. Palazzi, C.E.; Brunati, M.; Roccetti, M. An OpenWRT solution for future wireless homes. In Proceedings of the IEEE International
Conference on Multimedia and Expo, Singapore, 19–23 July 2010.
39. OpenWrt, a Writable Filesystem with Package Management. Available online: https://openwrt.org/ (accessed on 24 May 2021).
40. Silva, C.R.M.; Silva, F.A.C.M. An IoT Gateway for Modbus and MQTT Integration. In Proceedings of the SBMO/IEEE MTT-S

International Microwave and Optoelectronics Conference (IMOC), Aveiro, Portugal, 10–14 November 2019.
41. Message Queue Telemetry Transport (MQTT), the standard for IoT messaging. Available online: https://mqtt.org (accessed on
30 April 2021).
42. de Rango, F.; Potrino, G.; Tropea, M.; Fazio, P. Energy-aware dynamic Internet of Things security system based on Elliptic Curve
Cryptography and Message Queue Telemetry Transport protocol for mitigating Replay attacks. Pervasive Mob. Comput. 2020, 61,
101105. [CrossRef]
43. Guirado, R.; Padró, J.C.; Zoroa, A.; Olivert, J.; Bukva, A.; Cavestany, P. StratoTrans: Unmanned Aerial System (UAS) 4G
Communication Framework Applied on the Monitoring of Road Traffic and Linear Infrastructure. Drones 2021, 5, 10. [CrossRef]
44. de Rango, F.; Tropea, M.; Fazio, P.; Marano, S. Overview on VoIP: Subjective and objective measurement methods. Int. J. Comput.
Sci. Netw. Secur. 2006, 6, 140–153.
45. Álvares, P.; Silva, L.; Magaia, N. Blockchain-Based Solutions for UAV-Assisted Connected Vehicle Networks in Smart Cities: A
Review, Open Issues, and Future Perspectives. Telecom 2021, 2, 108–140. [CrossRef]
46. Miao, C.; Wang, J.; Ji, T.; Wang, H.; Xu, C.; Li, F.; Ren, F. BDAC: A Behavior-aware Dynamic Adaptive Configuration on DHCP in
Wireless LANs. In Proceedings of the IEEE 27th International Conference on Network Protocols (ICNP), Chicago, IL, USA, 7–10
October 2019.
47. Patrick, M. DHCP Relay Agent Information Option; 2001. Available online: https://www.rfc-editor.org/info/rfc3046 (accessed on
26 May 2021).
48. Malatesta, L. Articoli e Configurazioni. Available online: https://www.malatesta.biz/ (accessed on 26 May 2021).
49. Progetto Cogito. Available online: https://www.icar.cnr.it/progetti/cogito-sistema-dinamico-e-cognitivo-per-consentire-agli-
edifici-di-apprendere-ed-adattarsi/ (accessed on 20 May 2021).
50. Distretto Domus Cosenza. Available online: https://www.gruppotim.it/it/archivio-stampa/mercato/2016/TIM-Distretto-
Domus-Cosenza-14Dicembre2016.html (accessed on 19 May 2021).
51. Progetto Res Novae. Available online: https://www.cueim.org/progetti/res-novae-reti-edifici-strade-nuovi-obiettivi-virtuosi-
per-lambiente-e-lenergia-smart-city/ (accessed on 23 May 2021).
52. Fosi´

c, I.; Žagar, D. VPN network protection by IDS system implementation. In Proceedings of the 34th International Conven-tion
MIPRO, Opatija, Croatia, 23–27 May 2011.
53. Dong, L.; Yu, S.; Xia, T.; Liao, R. WBIPS: A Lightweight WTLS-Based Intrusion Prevention Scheme. In Proceedings of the Interna-
tional Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–25 September 2007.