دانشگاه زنجان

دانشکده فنی و مهندسی

گروه برق - الکترونیک

پایان نامه کارشناسی

عنوان:

تهدیدات امنیتی در فیبرهای نوری

استاد راهنما:

دکتر قمری ادیان

نگارش:

محسن برجی پور

تیرماه ۱۳۹۷

چکیده :

افزایش تقاضا در زمینه ی انتقال و خدمات رسانی اطلاعات و داده ها در چند سال اخیر، باعث سرعت بخشیدن و افزایش انتقال در پهنای باند قابل حمل شده است.که اکثریت آنها شامل اطلاعات حساس، داده های شخصی، حساب های بانکی، شماره کارت های اعتباری، اسناد خصوصی و ... است همچنین افزایش اهمیت مبحث انتقال مطمئن داده ها در کارهایی با مرکزیت شبکه ای، وجود ایمنی در سیستم های مخابراتی را یک جزء حیاتی از امنیت بین المللی کرده است.

در بخش اول، درباره ی یک تقسیم بندی که امنیت در سیستم های نوری را به دو بخش تقسیم بندی میکند، بحث میکنیم.

این دو تقسیم بندی شامل: 1 ایمن سازی داده های کاربر و 2ایمن سازی شبکه های مخابراتی می شود.

مورد اول بعنوان الگوریتم های رمزنگاری مطرح میشود و غیرقابل شکست است، به نحوی که به پیچیدگی الگوریتم بستگی ندارد اما شکستن و نفوذ در آن به اندازه ای دشوار است که نیازمند کامپیوتر های زنجیره ای است.

اما قسمت دوم تقسیم بندی، مبحثی است که خیلی خوب مطرح نمیشود مخصوصا در شبکه های فیبر نوری جدید

تلاش اول برای ایجاد یک cipher-text غیرقابل نفوذ، رمزنویسی کمّی است که از مکانیک کوانتومی ناشی میشود.این روش بر اصل همانند سازی نهادینه های خاص فوتون ها استوار است،همانند پلاریزاسیون یا قطبی سازی

در ادامه ما به آزمایش امنیت شبکه های نوری پیشرفته، فیبرهای نوری و FSO،رمزنگاری کوانتومی و توزیع کلیدهای کوانتومی میپردازیم که شامل اصل دورترارسانی میشود. همچنین به شناختن آسیب پذیری فیبر نوری و راه های ردیابی و راهکارهایی برای اقدامات متقابل و پیشگیری در مقابل حمله به شبکه های نوری میپردازیم.

در بخش دوم ، درباره ی راه های مختلفی که برای حمله به فیبر وجود دارد بحث میکنیم، از قبیل: خم کردن فیبر، شکافتن، اتصال ناپایدار فیبر، پراکندگی و ایجاد شیارهای V شکل که بسیاری از روش های ذکر شده نیازمند تجهیزات پیشرفته و نیازمند تخصص و مهارت است تا بتوان به وسیله آنها ماهیت فیزیکی فیبر را تغییر داد که این کار ریسک قابل توجهی هم دارد چراکه فیبر ممکن است آسیب ببیند یا بشکند یا که توسط کاربرها ردیابی شود. جدا از تمام تکنیک های ذکر شده، خم کردن فیبر،آسان ترین راه برای بیرون کشیدن نور از فیبر است چرا که حداقل ریسک آسیب یا ردیابی در این روش است. ما نیز بر روی محدود کردن تلفات خمش مورد نیاز برای یک حمله موفقیت‌آمیز در انتشار سیگنال در فیبرهای تک حالته بحث میکنیم، و خواصی از خمش را تحلیل خواهیم کرد که میتواند در ردیابی و تشخیص رخ دادن حمله به فیبر به ما کمک کندو به بحث در مورد مکانیسم های حملات فیبری نیز خواهیم پرداخت زیرا همانگونه که می دانیم، دانستن مکانیسم های مورد استفاده برای حملات فیبری، دید بهتری به ما برای ردیابی و جستجوی فعالانه ی حملات نوری غیرمجاز یا امنیت شبکه های در خطر اکتشاف میدهد.

در بخش سوم، در مورد تهدیدات مختلف امنیتی که وجود دارد بحثمیکنیم مثل:استراق سمع، حملات فیزیکی سازمانی ،تولید پارازیت و ... و اقدامات مختلف دفاعی در مقابل تهدیدات امنیتی مورد بررسی قرار خواهند گرفت مثل :

رمزگذاری نوری، دسترسی چندگانه ی تقسیم بندی های کد (cdma) ،ضد پارازیت بودن و ...

در بخش چهارم،به برآورد آسیب پذیری های شبکه‌های نوری مدرن امروزی می‌پردازیم و درباره روش‌های ارزیابی این معضل ها و معرفی امنیت های نوری و راه های موقعیت یابی نفوذ ها و ردیابی نفوذ بحث خواهیم کرد زیرا که در جهان امروز نیز ابزارهای حمله به مخابرات نوری که در شبکه‌های نوری عمومی و شخصی قرار دارد، امکان دست یابی بدون قید و شرط به تمامی اطلاعات ارسالی در هر بخش از فیبر را فراهم کرده اندکه این ها ابزارهای قانونی و ارزان از سازندگان متعدد در سرتاسر جهان هستند. این دستگاهها تجهیزات استاندارد حفاظت از شبکه اند که در روزمره مورد استفاده قرار می‌گیرد که اگر به

شکل بد استفاده شوند حملات نوری شکل می گیرد که روشی برای جاسوسی در داده های مخابراتی بدون امکان ردیابی شدن است.

تولید کنندگان تجهیزات شبکه های نوری، هنوز حفاظت کافی و تکنولوژی‌های ردیابی مناسب برای ردیابی آنی چنین نفوذ هایی در شبکه را در نظر نگرفته اند. بنابراین اعمال گران شبکه، توانایی حفاظت از سیگنال‌های نوری در شبکه های خود را نخواهند داشت. بنابراین نخواهند توانست از بیرون کشیدن داده های حساس جلوگیری کنند. شبکه های دولتی با اینکه به نسبت به خیلی ایمن‌تر هستند اما همچنان در برابر انواع حملات پیشرفته ی پسیو و اکتیو آسیب‌پذیر هستند

فهرست مطالب

فهرست اشکال

فصل اول:

امنیت در شبکه های نوری پیشرفته

۱-۱-معرفی

سیستم های مخابراتی فیبر نوری،بنیه ی تمامی شبکه‌های مخابراتی جدید محسوب می‌شوند ،به طوری که صوت،داده‌ها ،ویدیو، فکس، ایمیل، تلویزیون و ... با استفاده از ۱۸۰ میلیون مایل از کابلهای فیبر نوری در سرتاسر جهان انتقال می‌یابند. به همین خاطر موضوع بالا بردن امنیت در این نوع شبکه ها اهمیت ویژه ای پیدا می کند . جامعه مدرن امروزی نیز وابسته به برخی ویژگی های فیبر نوری از قبیل: در دسترس بودن ، اعتماد پذیری و یکپارچگی شبکه‌های نوری می باشد تا به درستی و به طور موثر عمل کنند.

با معرفی های گفته شده از فیبرهای نوری ،به طور خلاصه می‌توان گفت که انتقالات در شبکه های بر پایه فیبر نوری به طور ذاتی ایمن هستند ولی این نیز اثبات شده است که حمله به سیستم های مبتنی بر فیبر نوری آسان‌تر از شبکه‌های بر پایه ی مس سابق است،بعلاوه شبکه‌های نوری که مورد حمله قرار گرفته اند مستعد افشاء کردن اطلاعات بیشتری هستند.

ابزارهای مجاز ذکر شده که به این شکل استفاده می شوند، امکان استخراج اطلاعاتی از قبیل صداها یا داده های مخابراتی را در فیبر های نوری با کمترین خطر ردیابی فراهم می‌کنند.

همانند تمامی شبکه‌های مخابراتی دیگر ، اولین گام برای ایمن سازی شبکه مخابراتی به کاربردن پروتکل های رمزگذاری در بالاترین لایه های پُشته ی پروتکل است.به این خاطر است که باید مطمئن شد که لایه های فیزیکی سیستم نوری نیز ایمن سازی شده است.

مانند انواع دیگر شبکه ها،لایه فیزیکی شبکه نوری در مقابل تهدیدات مختلف آسیب پذیر است،بعلاوه بر این شبکه ها به خاطر داشتن بعضی ویژگی ها از دیگر شبکه ها متمایز هستند،به عنوان مثال سرعت انتقال داده هایی که آنها جابجا می کنند از Gb/sec۴۰ هم فراتر می رود.و این خاصیتی است که تنها با زمان افزایش پیدا میکند واین باعث به وجود آمدن یک رقابت منحصر به فرد برای کسب امنیت می‌شودو به همین علت است که مکانیسم های امنیتی در لایه های فیزیکی ،باید در زمان واقعی عملی باشد که با این سرعت انتقال، استفاده از محاسبات الکترونیکی متداول امکان‌پذیر نیست .برای غلبه بر این موضوع

یک سیگنال نوری ماندگار به صورت موازی و با سرعت بالا باید اعمال شود تا ایجاد امنیت در زمان واقعی بتوانند شکل بگیرد.اگر چه به انجام رساندن و ایجاد یک امنیت در زمان واقعی در لایه های نوری یک مشکل تکنیکی و رقابتی است اما نتایج و دستاوردهای آن بسیار قابل توجه است:

اولا، ایمن سازی لایه های نوری منجر به افزایش امنیت به کار رفته در لایه های بالاتر پشته های پروتکل می‌شود و این منجر به دستیابی به سیستمی می‌شود که روی هم رفته ایمن‌تر هست.

دوما، برخلاف نقطه مقابل این شبکه ،یعنی شبکه های الکترونیکی، سیستم های مخابرات نوری احتمال دریافت حمله ی کانال جانب کمتری را دارند و به خاطر اینکه دستگاه های نوری ،اثر الکترومغناطیسی از خود ساطع نمی کنند از این رو آسیب پذیری کمتری نسبت به استراق سمع کانال جانب الکترومغناطیسی دارند.

با بکارگیری فرایند سیگنال های نوری، مجموعه‌ی مخابرات نوری با چندین راه برای ایمن سازی در قسمت های لایه ای مواجه می‌شد:برای مثال: رمزگذاری نوری، پهنا نگاری نوری و شبکه‌های نوری پایدار.

مثلاً رمزگذاری نوری امکان رمز شدن سیگنال ها با کمترین تاخیر و بیشترین سرعت را میدهد(سرعتی که برای شبکه های الکتریکی متداول غیرممکن است)

علاوه بر این، این کار بدون انتشار اثرات فرکانس رادیویی صورت می‌پذیرد.پهنا نگاری نوری نیز، یک لایه اضافی را مهیا می کند که قادر به تکمیل رمزگذاری داده ها به وسیله مخفی سازی انتقال داده ها در کانال انتقال عمومی است.

جنبه های بیشماری از امنیت در شبکه های نوری وجود دارد، در این بخش،درباره سه جنبه امنیتی شبکه های نوری بحث میکنیم:

۱-اثبات قابلیت اعتماد شبکه های مخابراتی

۲-حمایت از پوشیده بودن و اختفاء این نوع شبکه ها یا احتمال خیلی کم ردیابی شدن

۳-اطمینان دادن در دسترس بودن این شبکه ها

شکل گیری و گسترش سریع بخش تسهیمات با طول موج انبوه (dwdm) در شبکه های مخابراتی مدرن نوری موجب فراهم شدن پهنای باند قابل انتقال بی سابقه در فیبرهای نوری تک حالته شده است.امکان دسترسی به تنگناها و آسانی آن نسبت به گذشته بعلت وجود فیبر نوری یا وجود سیستم های پیشرفته ی بی سیم، باعث افزایش تقاضا از سوی کاربران شده است و همانگونه که ذکر شد این شبکه ها میتوانند شامل اطلاعات حساسی باشند که همین موضوع باعث مهیا شدن شرایط برای هکرها و حمله کننده ها برای برداشتن اطلاعات یا کپی کردن منبع و یا عوض کردن داده ها و نفوذ به شبکه می شود که موجب بروز نگرانی های عمومی در ارگان های شخصی و دولتی شده است.

در حالت کلی سه نوع تهدید امنیتی در شبکه های مخابراتی وجود دارد

۱- داده های کاربر

۲- شبکه های فیزیکی و مادی

۳- مدیریت شبکه و تامین امنیت

داده های کاربر همانطور که گفته شد ،بعنوان الگوریتم های رمزگذاری مطرح شدهو نفوذ به آن بسیار دشوار است.

مبحث دوم یعنی امنیت شبکه های فیزیکی در شبکه های فیبر نوری مدرن،موضوعی جدید است که دلیل نگرانی در این نوع تهدید دقیقا مشابه مورد اول است.

در مورد سوم اگر دسترسی توسط یک متجاوز شبکه صورت گیرد او میتواند اقدام به ارسال پیام ها و عملگرهای گمراه کننده کند و با اینکار اقدام به عوض کردن اطلاعات شبکه یا ارسال اطلاعات از یک راه دیگر نماید.

۱-۲- سطوح امنیتی در حوزه ی رمز نویسی :

یک مدل رمزنویسی مطلوب و برجسته شامل حافظه و عملگرهای ثبت وضعیت، الگوریتم های رمزنگاری،کلیدهای صفر (شامل محرمانه و عمومی)، متن ها و متون رمز شده می‌باشد.

بعضی افراد وسوسه ی دست یابی به این حوزه ها به منظور فهمیدن مکانیسم رمزنویسی یا الگوریتم ها و کلیدهای آنرا دارند.

برای حفظ این حوزه ها از اینگونه دسترسی های ناخواسته از FIPS 140-2 و ضمایم آن (A,B,C,D) که شامل چهار سطح امنیتی هستند استفاده میکنیم.

خلاصه ای از این سطوح امنیتی به شرح زیر است :

امنیت سطح اول (SL-1) ،دارای کمترین سطح امنیتی است و هیچگونه نیاز فیزیکی خاصی برای این سطح درنظر گرفته نشده است و عملکرد آن اینگونه است که موقع اجرای حفاظت فیزیکی، همه ی plaintext ها (پیام های عادی درشکل رمز) و کلیدهای شخصی و دیگر پارامترهای حیاتی، بصورت رویه ای یا خودگردان تبدیل به صفر میشوند.

امنیت سطح دوم (SL-2) بخاطر پوشش بازتابنده و خاصیت محکم سازی و مهر و موم کردن و داشتن قفل هایی در پوشش ها و قسمت دَر،قویتر از SL-1 میباشد.

امنیت سطح سوم (SL-3)،بخاطر مکانیسم های امنیتی فیزیکی و مکانیسم گزارش دهی آن، قوی تر شده ی امنیت سطح دو است.این سطح از امنیت نیازمند پورت های ورودی خروجی جداگانه برای متون رمز شده و پلین تکست ها میباشد و هرگونه تخلف و تجاوز به این نوع سطح از امنیت موجب صفر شدن کلیدهای رمز نویسی در حوزه میشود.

امنیت سطح چهار (SL-4)، یک نوع ایمن سازی فیزیکی سرتاسری در اطراف حوزه ی رمزگذاری در برابر هرگونه نفوذ برای دسترسی به کلید رمزنگاری و یا عوض کردن شرایط محیطی بیرونی و یا هرگونه نوسان را ایجاد میکند.این نوع از رمز نویسی، شامل مکانیسم های محافظ،نارسایی های محیطی (EFP)

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

در غیر اینصورت اگر M(j , i)={attack,flag} باشد

داده هارا از مسیر دیگری ارسال کن و

M,(i,j)={o.k. , not mine} برگردانده شود.

۵-۳-نتیجه گیری:

در اینجا ما به معرفی الگوریتم هایی پرداختیم که در مبحث مکان یابی و تشخیص انواع حملات بسیار مفید بودند و به این نتیجه رسیدیم که این الگوریتم های ما ضمانت کننده عملکرد صحیح شبکه ها و از دست نرفتن اطلاعات نیز هستند بعلاوه اینکه الگوریتم های ذکر شده بستگی به تعداد گره های شبکه ندارند.

ردیابی محل خطا با استفاده از الگوریتم های ذکر شده فارغ از مسافتی که داده ها طی میکردند بود، پس این الگوریتم ها هیچ وابستگی به این موارد نداشتند و حتی در شبکه محلی و شبکه های مناطق بزرگتر نیز قابل استفاده بودند.

۵-۴-خلاصه :

در ابتدا، به بحث در مورد سطوح و لایه های امنیتی شبکه های نوری، فیبرهای نوری و شبکه های فضای آزاد نوری پرداختیم. ما در مورد روش های امنیتی پیشرفته، مثل رمزگذاری کوانتومی و توزیع کلید کوانتومی که شامل اصول دورترارسانی بود صحبت کردیم، همچنین نقاط آسیب پذیر شبکه های فیبری را شناختیم و در مورد روش های اقدامات متقابل در مقابل حمله های فیزیکی شبکه بحث کردیم.

در ادامه، در مورد آسیب پذیری های شبکه های نوری در مقابل انواع مختلف تهدیدهای امنیتی که می‌توانند در لایه‌های نوری شبکه ظاهر شوند و همچنین انواع مختلف تکنیک های نوری برای مقابله با آسیب‌های امنیتی مشابه بحث کردیم.

با استفاده از تکنیک های نوری فهمیدیم که استفاده از سیگنالهای نوری زمان-حقیقی برای بهبود امنیت شبکه های نوری مناسب است. همچنین با رمزگذاری های نوری برای افزایش خاصیت اعتماد پذیری در

سرعت خطوط، انواع مختلف گیت‌های XOR نوری با یا بدون فیدبک، که به طور آزمایشی ساخته شدند، آشنا شدیم.

که با این تکنیک ها قادر به تولید رشته کلید های طولانی از کلید های کوچک برای تولید رجیسترهای مورد استفاده در رمزنگاری ورنام برای ایجاد رمز نگاری ایمیل نوری هستیم.

به واسطه عملکرد باند گسترده ی فیبرهای نوری، قابلیت ضد پارازیت از طریق تبدیلات فرکانس نوری به دست آمد تا ما بتوانیم سیگنال را بیرون از باند پارازیت ارسال کنیم.

طیف های پهن که به طور ذاتی از پالسهای نوری به دست می‌آید اجازه ی پنهان سازی نوری را برای دستیابی آسان از طریق مسیرهای موقتی برپایه ی پراکندگی شتاب گروهی را در فیبرها یا فیبرهای cfbg را میدهد.

یک پوشش فاز نوری می‌تواند به سیگنال های نهان اضافه شود تا امنیت آن افزایش یابد. همچنین درباره ی کدگذاری ocdma، برای افزایش در دسترس بودن و قابلیت اعتماد پذیری شبکه های نوری با استفاده از ساختارهای نوری پایدار و کدگذاری های متعامد بحث کردیم.

۵-۵-نتیجه گیری نهایی :

مخابرات، یک فاکتور اساسی در تکنولوژی مدرن اطلاعات امروزی و خدمات بر پایه ی آن است.

تجارت های جهانی نیز وابسته به ساختار حساس مخابراتی است و وابسته به دسترسی پذیری، اعتماد پذیری و یکپارچگی داده ها ارسال وویس ها است.

داده های مخابراتی حساس به طور غیرقانونی از شبکه‌های شخصی و عمومی بیرون کشیده می‌شوند، می‌توانند بطور قاچاق برای مقصود های مالی سیاسی و غیره استفاده شوند.

رقیبان جهانی نیز به شدت به دنبال چنین مزایای قابل رقابتی هستند.

تروریست ها که به دنبال ایجاد تخریب و اختلال در یکپارچگی و دسترسی پذیری شبکه‌های مخابراتی هستند، باید به عنوان سازمان هایی در نظر گرفته شوند که از ابزارهای فوق پیشرفته برای حمله استفاده می‌کنند.

شبکه‌های نوری به خاطر انتقال حجم بالایی از اطلاعات به صورت ارزان و موثر در جهان شهرت دارند.

شبکه‌های مخابراتی امروزی شامل تمامی انواع شبکه های فیبر نوری هستند.

مزایای تکنولوژی بیشتر و کاهش قیمت، باعث تبدیل فیبرهای نوری به سازه‌هایی با بیشترین استفاده نسبت به زمان شده و سازه های امروزی نیز به شدت، به خدمات فراهم شده توسط فیبرهای نوری محتاج اند.

روشهای حمله نوری، امکان استخراج و مرتب سازی حجم زیادی از داده های انتقالی ارسالی از طریق فیبرهای نوری را فراهم می کنند.

نا امن بودن ذاتی فیبرهای نوری و این عقیده که این فیبرها حتما خواهند بود، شاید بزرگترین تصور غلط در صنعت مخابرات امروز باشد و شرکتها و موسساتی که اینگونه خطرات را نادیده می‌گیرد باید منتظر مواجه شدن با یک تلفات چشمگیر باشند.

اجرا کننده های این شبکه ها نیز باید آسیب پذیر بودن این شبکه های پرسروصدا را مطرح کرده و پیشنهاد حفاظت و بیمه های قراردادی را در مقابل حملات احتمالی به مشتری‌های خود بدهند.

دولت نیز باید حفاظتش را در مقابل انواع حملات نوری بیشتر کرده و به گسترش آموزش بپردازد و به سازمان‌ها و نهادها و شهروندان در مقابل چنین حملاتی قدرت ببخشد.

منابع

[1]. Kartalopoulos, Stamatios V. "Security in advanced optical communication networks." *Communications, 2009. ICC'09. IEEE International Conference on*. IEEE, 2009.

[2]. Shaneman, Keith, and Stuart Gray. "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection & prevention." *Military Communications Conference, 2004. MILCOM 2004. 2004 IEEE*. Vol. 2. IEEE, 2004.

[3]. Fok, Mable P., et al. "Optical layer security in fiber-optic networks." *IEEE Transactions on Information Forensics and Security* 6.3 (2011): 725-736.

[4]. Iqbal, M. Zafar, Habib Fathallah, and Nezih Belhadj. "Optical fiber tapping: Methods and precautions." *High Capacity Optical Networks and Enabling Technologies (HONET), 2011*. IEEE, 2011.

[5]. UMOH, GABRIEL ETIM, et al. "The Vulnerability of Fiber-Optics Communication Systems: The Role of Optical Tapping."

[6]. Médard, Muriel, Poompat Saengudomlert, and Stephen R. Chinn. "Attack detection in all-optical networks." *Optical Networks and Their Applications*. Optical Society of America, 1998.

[7]. Furdek, Marija. "Physical-layer attacks in optical WDM networks and attack-aware network planning." *European Journal of Operational Research* 178.2 (2011): 1160-1167.

[8]. Bergman, Ruth, Muriel Médard, and Serena Chan. "Distributed Algorithms for Attack Localization in All-Optical Networks." *NDSS*. 1998.