دانشگاه تربیت مدرس

دانشکده فنی و مهندسی

پایان نامه کارشناسی ارشد

مهندسی برق - مخابرات

رمزنگاری و مکانیزم‌های امنیتی در شبکه‌های کامپیوتری

صیاد نجفی

استاد راهنما

آقای دکتر محمد رضا عارف

زمستان ۱۳۷۳

موضوع

رمزنگاری و مکانیزمهای امنیتی در شبکه‌های کامپیوتری

توسط

صیـــــــاد نجفـــــی

پایان‌نامه

برای دریافت درجه‌کارشناسی ارشد

رشته مهندسی برق - گرایش مخابـــــرات

از این پایان‌نامه در تاریخ ۱۳۷۳/۱۲/۲۲ در مقابل هیئت داوران دفاع به عمل آمد و مورد تصویب قرار گرفت.

اعضای محترم هیئت داوران

۱- خانم/آقای دکتر محمد رضا عارف	استاد راهنما
۲- خانم/آقای دکتر سید احمد رضا شرافت	استاد مشاور
۳- خانم/آقای دکتر ــــــــــ	استاد مشاور
۴- خانم/آقای دکتر مسعود کهریزی	استاد ممتحن
۵- خانم/آقای دکتر کیوان فرورقی	استاد ممتحن
۶- خانم/آقای دکتر کیوان فرورقی	مدیر گروه

تقدیم به :

استاد معظم، جناب آقای دکتر محمدرضا عارف که بزرگترین استاد زندگیم بوده‌اند؛

و به پدر بزرگوارم که تحصیلم را مرهون مشقت‌های فراوان در زندگی‌اش می‌دانم؛

و به مادر مهربانم که معنی عشق و عاطفه را از او آموختم؛

و به برادران و خواهران عزیزم که مایهٔ دلگرمی زندگیم هستند؛

تقدیر و تشکر

بر خود لازم می‌دانم که:

از جناب آقای دکترمحمدرضا عارف که در طول دوران تحصیل و راهنمایی این پایان‌نامه مرا یاری داده‌اند و معلم اخلاقم بوده‌اند تشکر و قدردانی نمایم.

و نیز از آقای دکتر سیداحمدرضا شرافت بخاطر مشاوره و راهنمایی اینجانب در تدوین رساله، و نیز از آقایان دکتر مسعود کهریزی و دکتر کیوان فرورقی بخاطر شرکت در جلسه دفاعیه، تشکر و سپاسگزاری نمایم.

چکیده

شبکه‌های محلی سیستم‌های مخابره داده هستند که بخش های مستقل را قادر می‌سازند با ارتباط با همدیگر در سرعت انتقال های بسیار بالا و در محدوده جغرافیایی نسبتاً محدود بتوانند با یکدیگر همکاری کنند. با دقت در تعریف شبکه‌های محلی (LAN) در می‌یابیم که LANها یکی از ناامن‌ترین کانال های انتقال داده بوده و هر کاربری توانایی دسترسی به اطلاعات روی رسانه را دارد. این شبکه‌های با به کار گرفتن سیستم‌های مخابراتی برای برقراری ارتباط بین LANها، توجه مراکز تحقیقاتی، تجارتی، سیاسی و نظامی را به خود جلب کرده است. ایجاد امنیت در این شبکه‌ها از ضرورت هایی است که کاربران شبکه به آن نیاز دارند.

در شبکه های محلی مبتنی بر مدل ۷ لایه‌ای استاندارد (OSI) نظیر رینگ، اترنت و توکن باس برای ایجاد امنیت و اعتبار داده‌های ارسالی از سیستم‌های رمزنگاری کلید عمومی جهت توزیع کلید جلسه بین کاربران و روشی برای کاهش دادن حافظه لازم در گره‌های شبکه استفاده کرده‌ایم. همچنین برای ایجاد کانال امن بعد از تبادل کلید جلسه بین گره‌های مبداء و مقصد از سیستم‌های رمزنگاری کلید عمومی با اجرای نرم افزاری در لایه هفتم مدل مرجع استاندارد و همچنین از سیستم‌های رمزنگاری قالبی یا پی در پی با اجرای سخت افزاری در لایه‌های اول یا دوم، داده‌های خروجی را رمز کرده و بدین طریق از دسترسی غیر مجاز دشمن به داده‌های شبکه و حمله تحلیل ترافیک گرفته شده و امنیت پیام حفظ می‌شود.

برای ایجاد ارتباط امن در شبکه‌های گسترده (WAN) متشکل از LANها، از دروازه‌هایی که سیستم‌های رمزنگاری قالبی یا پی در پی و مدول امنیتی روش رمزنگاری گره بر گره در آنها تعبیه شده است، استفاده کرده‌ایم.

فهرست

فصل چهارم : مروری بر سیستم‌های رمزنگاری

فصل پنجم : کاربرد سیستم‌های رمزنگاری

فصل ششم : نتیجه‌گیری و پیشنهادات

فصل اول

مقدمه

از زمانی که انسان نیاز به ارتباط گفتاری و مکاتبه‌ای با دیگر همنوعان خود پیدا کرد، همواره افرادی بوده‌اند که در این ارتباط علاقمند به مکالمه سری جهت پنهان کردن محتویات گفتار از دیگران هستند. در پاره‌ای از این ارتباطات، به خاطر حفظ منافع گروهی و فردی مخفی کردن محتوای پیام‌های مبادله ضروری است. بنابر این پیدایش رمزنگاری را می‌توان مقارن با شروع توانایی انسان برای ارتباط با دیگر افراد دانست، هر چند که شروع رمزنگاری را در تاریخ بشری به صورت مکتوب و پذیرفته شده نمی‌توان یافت.

همواره در راستای این مبادله اطلاعات، افراد دیگری نیز بوده و هستند که برای حفظ منافع خود یا مقابله با گروه‌های قبلی، سعی درکشف و بدست آوردن محتوای پیام‌های ارسالی دارند. بنابر این تکامل رمزنگاری نتیجه تلاش این دو گروه بوده و هر یک سیستم‌های رمزنگاری جدیدی با توجه به پیشرفت علوم و تکنولوژی ابداع کرده و گروه مقابل و همچنین خود ابداع کنندگان سیستم، جهت شکستن و مقاوم کردن سیستم تلاش مستمر می‌کنند.

امروزه شبکه‌های مخابراتی، کامپیوتری و بانک‌های اطلاعاتی (نمونه‌ای از مراکز ذخیره داده) به گونه‌ای رشد یافته‌اند که دسترسی غیر مجاز به داده‌های ارسالی یا ذخیره شده در پاره‌ای از موارد می‌تواند سرنوشت یک سازمان یا گروه عظیمی از انسان‌ها را تحت شعاع جدی قرار داده و در ارتباطات نظامی و سیاسی امنیت جانی انسان‌ها را به خطر اندازد.

مراکز تحقیقاتی، تجاری، سیاسی، نظامی و بانک‌های اطلاعاتی؛ جهت نیل به اهداف مختلف خود، همواره در ارتباط تنگاتنگ با دیگر همکاران خود که در مکان‌های مختلف دور از هم قرار دارند، هستند. این ارتباط از طریق شبکه‌های مخابراتی و کامپیوتری برای مبادله اطلاعات صوتی و تصویری و داده‌های کامپیوترها، صورت می‌گیرد. امروزه شبکه‌های کامپیوتری محلی و گسترده زیادی ارتباط کاربران در نقاط مختلف شبکه‌ها به خدمت گرفته شده و روز به روز روند رشد و توسعه را طی می‌کنند. چرا که با ساخت و تولید ریزپردازنده‌ها امروزه دنیای کامپیوتر

متحول شده است و هر روز سیستم‌های میکروپروسسوری ارزان قیمت جدیدی به بازار عرضه می‌شود. همچنانکه با ابداع کامپیوترهای شخصی و پیشرفت، بهبود سرعت و امکانات جانبی آنها، دیگر کمتر سازمانی علاقمند به خرید کامپیوترهای بزرگ است. شبکه‌های کامپیوتری نیز خیلی متأثر از این پیشرفت بوده و امروزه با داشتن یک مدم و کامپیوتر شخصی از خدمات شبکه اینترنت[1] و دیگر شبکه‌ها، می‌توان بهره‌مند بود.

شبکه‌های محلی سازمان‌ها و مراکزتحقیقاتی نیز با بکارگرفتن کامپیوترهای کوچک پر قدرت و کارت‌های شبکه مناسب، نیازکاربران شبکه را به نحو مطلوب برآورد می‌کنند. همانند ظهور کامپیوترهای شخصی و به کارگرفتن تعدادی از آنها که کار یک کامپیوتر بزرگ را انجام می‌دهند و در نتیجه کم شدن مصرف‌کنندگان سیستم‌های بزرگ، شبکه‌های محلی نیز بهتر و ارزان‌تر از شبکه‌های گسترده، نیازکاربران را برآورد خواهند کرد و با اتصال شبکه‌های محلی از طریق سیستم‌های مخابراتی (خطوط تلفن، کابل هم محور، فیبر نوری و لینک‌های ماهواره‌ای) یک شبکه گسترده (متشکل از[2] LAN ها) تشکیل می‌شود. با شروع و راه‌اندازی شبکه‌های مخابرات ماهواره‌ای با ارتفاع کم[3](LEO) و استفاده از خطوط ارتباطی آنها جهت ارسال داده‌های بین شبکه‌های محلی و گسترده، انقلابی در خدمات ارائه شده توسط شبکه‌های کامپیوتری بوجود خواهد آمد.

با توجه به اینکه از شبکه‌های کامپیوتری امروزه و در آینده برای ارسال داده‌ها استفاده می‌شود، بنا بر این همواره حجم وسیعی از این داده‌ها نیاز به "**ارسال امن**" خواهند داشت. ابداع و بکارگیری سیستم‌های رمزنگاری در شبکه‌های محلی و گسترده هر روز شکل پیچیده‌تری به خود می‌گیرد و بررسی چنین تحقیقاتی برای ایجاد "**امنیت و اعتبار**" در شبکه‌های مزبور،

---

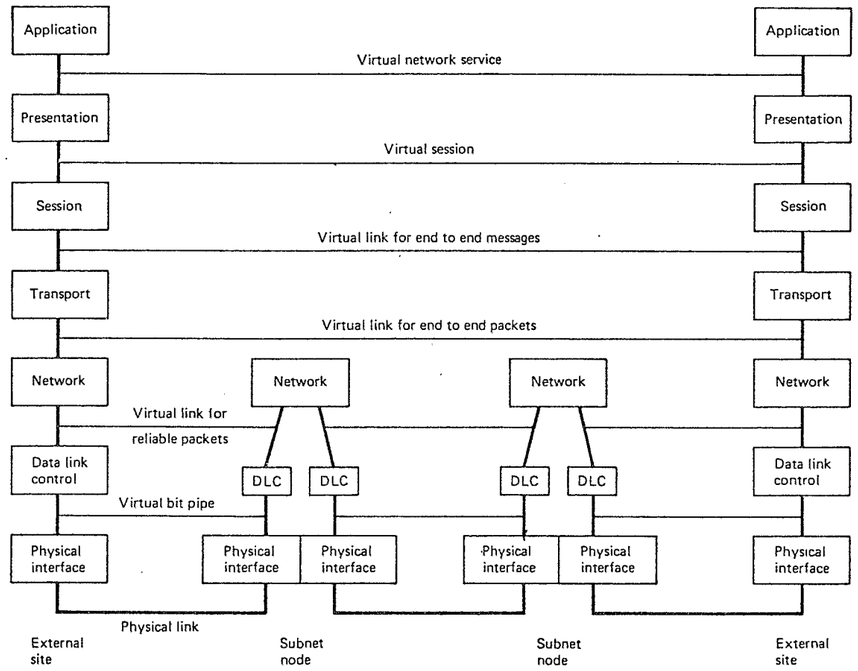
1 - Internet

2- Local Area Network

3 - Low Earth Orit

ضروری می‌نماید و ما برای نیل به این هدف گام کوچکی را شروع به برداشتن کرده‌ایم.

در این تحقیق ما شبکه‌های محلی و گسترده مبتنی بر مدل هفت لایه‌ای استاندارد (OSI[1]) شکل (۱-۱) را در نظر گرفته و کاربرد رمزنگاری را برای ایجاد ارتباط امن بین کاربران شبکه را بررسی کرده‌ایم.



شکل ۱-۱ مدل مرجع ۷ لایه‌ای استاندارد OSI[1].

---

1 - Open Systems Interconnection

در فصل دوم با مروری بر شبکه‌های محلی به تعریف، مشخصات، اهداف و کاربرد شبکه‌های محلی پرداخته و در ادامه به طبقه‌بندی LANها بر اساس توپولوژی شبکه‌ها پرداخته و در انتها، شبکه‌های محلی مسیر عمومی را که در مراکز کامپیوتری مورد استفاده زیاد قرارگرفته‌اند را بررسی می‌کنیم.

در فصل سوم، استانداردهای شبکه‌های محلی LAN یعنی استانداردهای IEEE 802.3 ، IEEE 802.4 و IEEE 802.5 که مبتنی بر مدل مرجع (OSI) ابداع شده و در مراکز اداری و صنعتی و غیره، کاربرد پیدا کرده‌اند پرداخته‌ایم و در انتهای فصل شبکه گسترده WAN[1] متشکل از LAN ها که توسط دروازه‌هایی به هم متصل شده‌اند را بررسی می‌کنیم.

در فصل چهارم، سیستم‌های رمزنگاری کلاسیک و مدرن را بررسی کرده و سیستم‌های رمزنگاری قالبی و پی‌درپی (سیستم‌های متقارن یا تک کلیدی) و همچنین سیستم کلید همگانی (سیستم دو کلیدی) را جهت به کارگیری در شبکه‌های محلی و گسترده مبتنی بر مدل OSI برای برقراری ارتباط امن کاربران شبکه می‌پردازیم.

در فصل پنجم، کاربرد رمزنگاری در شبکه‌های و مدهای مختلف به کارگرفته شده و مقایسه آنها و سیستم‌های رمزنگاری پیشنهادی و روشی جهت توزیع کلید در شبکه‌های محلی و گسترده متناظر و همچنین مدهای رمزنگاری پیشنهادی را جهت استفاده در شبکه‌های مدل OSI را بررسی می‌کنیم.

در فصل آخر، نتایج و پیشنهادات برای ادامه تحقیق جهت رسیدن به روشهای مطلوب و عملی ایجاد امنیت در شبکه‌های محلی و گسترده را می‌آوریم.

---

1 - Wide Area Network

فصل دوم

مروری بر شبکه‌های کامپیوتری