ارتباطات ایمن

رویداد ملی علم و فناوری سورنا

رویداد سورنا از فناوری تا مقاومت

جوشش

شبکه رویدادپردازی دانشجویان ایران

به نام خدا

پیشینه‌ی مسئله:

ایده‌ی امنیت در مخابرات از زمان‌های قدیم در سیستم‌های نظامی مطرح بوده است. از رمزنگاری‌های اولیه مانند رمز سزار که در امپراتوری روم استفاده می‌شد تا سیستم‌های پیشرفته‌ی قرن بیستم مانند انیگما در جنگ جهانی دوم، همواره امنیت اطلاعات نقش کلیدی داشته است. رمزنگاری انیگما، که در آن زمان پیچیده‌ترین سیستم رمزنگاری بود، توسط متحدین شکست و اهمیت امنیت مخابراتی را برجسته کرد. در دهه‌های اخیر، با ظهور فناوری‌های دیجیتال و گسترش ارتباطات بی‌سیم، تهدیدات نیز پیچیده‌تر شده‌اند. ظهور اینترنت، شبکه‌های بی‌سیم و فناوری‌های مبتنی بر ابر، چالش‌های امنیتی جدیدی از جمله حملات سایبری پیشرفته، سرقت داده‌ها، و اختلال در سرویس‌ها را به همراه داشته است.

در طول دهه گذشته، تحقیقات و فناوری‌های متعددی در زمینه امنیت مخابراتی توسعه یافته‌اند. فناوری‌هایی مانند رمزنگاری کوانتومی، بلاک‌چین، و شبکه‌های تعریف‌شده توسط نرم‌افزار (SDN) پتانسیل بزرگی برای ارتقای امنیت در سیستم‌های مخابراتی دارند. با این حال، نیاز به طراحی سیستم‌هایی که قابلیت اجرایی شدن در شرایط نظامی را داشته باشند، همچنان چالش بزرگی باقی مانده است.

علت اهمیت :

در عصر دیجیتال کنونی، که با پیشرفت بی‌سابقه‌ی فناوری‌های مخابراتی و افزایش حجم داده‌های مبادله شده همراه است، اهمیت سیستم‌های مخابراتی امن به یک ضرورت انکارناپذیر تبدیل شده است .داده‌های حساس و حیاتی، از اطلاعات شخصی و مالی گرفته تا اسرار تجاری و دولتی، به‌طور فزاینده‌ای در معرض تهدیدات سایبری و فیزیکی قرار دارند .این تهدیدات، از حملات ساده‌ی فیشینگ و بدافزارها تا جاسوسی‌های پیچیده و حملات هدفمند دولتی، طیف وسیعی را در بر می‌گیرند .در این شرایط، تضمین امنیت اطلاعات در محیط‌های مختلف، اعم از شبکه‌های بی‌سیم، اینترنت اشیا و ارتباطات ماهواره‌ای، بیش از هر زمان دیگری حیاتی است.

هرچه ارزش اطلاعاتی که در دست داریم بالا می‌رود، اهمیت حفظ محرمانگی و تمامیت آن نیز افزایش می‌یابد .اطلاعات، به‌عنوان یک دارایی ارزشمند، نیازمند محافظت در برابر دسترسی‌های غیرمجاز، تغییر، تخریب و افشا است .سیستم‌های مخابراتی امن، با استفاده از روش‌های رمزنگاری پیشرفته، مانند رمزنگاری کلید عمومی و خصوصی، به ایجاد کانال‌های ارتباطی امن و محافظت از داده‌ها در برابر شنود و دستکاری کمک می‌کنند.

از سوی دیگر، با رشد نمایی توان محاسباتی کامپیوترها، الگوریتم‌های رمزنگاری نیز به‌طور مداوم در معرض حملات جدید و پیچیده‌تر قرار می‌گیرند .این موضوع، نیاز به تحقیق و توسعه‌ی الگوریتم‌های رمزنگاری قوی‌تر و مقاوم‌تر در برابر حملات را دوچندان می‌کند .بنابراین، سرمایه‌گذاری در تحقیقات مربوط به رمزنگاری و آموزش متخصصان امنیت سایبری، برای تضمین امنیت مخابرات در آینده امری ضروری است. یک سیستم مخابراتی امن و قابل اعتماد، ستون فقرات یک جامعه‌ی دیجیتال پویا و ایمن را تشکیل می‌دهد.

شرح مسئله :

مخابره‌ی داده‌ها یک نیاز اساسی جهان امروز، چه در زمینه‌های تجاری و چه در زمینه‌های نظامی است. در مخابرات نظامی، رمزنگاری داده‌ها و محافظت آن‌ها در برابر شنود و اختلال اهمیت بیشتری پیدا می‌کند. مسئله اصلی این پروژه طراحی سیستمی است که بتواند ارتباطات مخابراتی را در شرایط حساس نظامی به‌گونه‌ای امن کند که:

۱. **محرمانگی:** اطمینان حاصل شود که تنها طرفین مجاز به اطلاعات دسترسی دارند.

۲. **یکپارچگی:** اطمینان از عدم تغییر یا دستکاری داده‌ها طی انتقال.

۳. **دسترس‌پذیری:** اطمینان از امکان برقراری ارتباط در حضور تلاش‌های اختلال‌گرایانه.

۴. **عدم انکار:** توانایی اثبات تبادل اطلاعات توسط فرستنده و گیرنده.

این سیستم باید بتواند در برابر تهدیداتی چون حملات سایبری، حملات فیزیکی به زیرساخت‌ها و استراق سمع از سوی دشمن مقاومت کند. علاوه بر این، لازم است تا قابلیت تعامل و ادغام با سایر زیرساخت‌های موجود را داشته باشد.

همچنین سیستم موردنظر دارای ویژگی‌های خاصی باید باشد، از جمله:

۱. **منابع محدود:** محدودیت در توان پردازشی، مصرف انرژی و پهنای باند به‌ویژه در تجهیزات قابل حمل.

۲. **قابلیت حمل و استقرار سریع:** تجهیزات باید سبک، قابل حمل و در محیط‌های نظامی به‌سرعت مستقر شوند. این امر به ویژه در مأموریت‌های میدانی حیاتی است.

۳. **مقاومت در برابر شرایط محیطی:** سیستم باید در شرایط سخت محیطی مانند دمای بالا، گردوغبار، رطوبت و تداخل‌های الکترومغناطیسی عملکرد مطلوب داشته باشد.

۴. **پایداری در برابر اختلال‌ها:** سیستم باید در برابر اختلالات عمدی مانند جَمینگ (Jamming)مقاوم باشد و از فناوری‌های ضد جَمینگ استفاده کند.

۵. **سازگاری با تجهیزات موجود:** طراحی باید با سیستم‌های مخابراتی موجود سازگار باشد تا بتواند بدون نیاز به تغییرات بزرگ، جایگزین یا مکمل شود.

۶. **امنیت فیزیکی تجهیزات:** تجهیزات باید به گونه‌ای طراحی شوند که در صورت افتادن به دست دشمن، اطلاعات ذخیره‌شده قابل بازیابی نباشد.

رشته‌های هدف :

پروژه‌های مرتبط با مخابرات امن، ماهیتاً بین‌رشته‌ای هستند و نیازمند همکاری متخصصان از حوزه‌های مختلف می‌باشند. با توجه به زیرساخت‌های ریاضی پیچیده‌ی الگوریتم‌های رمزنگاری و همچنین نیاز به طراحی و پیاده‌سازی سیستم‌های سخت‌افزاری و نرم‌افزاری، این پروژه‌ها می‌توانند بستری مناسب برای همکاری دانشجویان رشته‌های مختلف فراهم کنند.

دانشجویان مهندسی برق، به‌ویژه گرایش‌های مخابرات، الکترونیک و سیستم‌های دیجیتال، می‌توانند در طراحی و پیاده‌سازی لایه‌های فیزیکی و پیوند داده‌ی سیستم‌های مخابراتی امن، نقش کلیدی ایفا کنند. آشنایی آن‌ها با مفاهیمی مانند مدولاسیون، کدینگ، انتشار امواج و طراحی مدارهای مجتمع، برای بهینه‌سازی عملکرد و امنیت سیستم ضروری است.

دانشجویان مهندسی کامپیوتر، به‌ویژه گرایش‌های معماری کامپیوتر، شبکه‌های کامپیوتری و امنیت اطلاعات، می‌توانند در طراحی و پیاده‌سازی پروتکل‌های امنیتی، سیستم‌های عامل امن و نرم‌افزارهای کاربردی مخابراتی امن مشارکت داشته باشند . تسلط آن‌ها بر مفاهیم رمزنگاری، احراز هویت، کنترل دسترسی و تحلیل بدافزارها برای تضمین امنیت سیستم حیاتی است.

دانشجویان علوم ریاضی و کامپیوتر، به‌ویژه گرایش‌های رمزنگاری، نظریه‌ی اعداد و جبر، می‌توانند در طراحی و تحلیل الگوریتم‌های رمزنگاری و ارزیابی امنیت آن‌ها نقش موثری داشته باشند. دانش عمیق آن‌ها از مفاهیم ریاضی زیربنایی رمزنگاری، برای توسعه‌ی الگوریتم‌های مقاوم در برابر حملات ضروری است.

این رویکرد بین‌رشته‌ای، منجر به طراحی و پیاده‌سازی سیستم‌های مخابراتی امن، کارآمد و قابل اعتماد خواهد شد.