
بسم الله الرحمن الرحیم

دانـــشگاه یـــــزد

دانشکده مهندسی برق و کامپیوتر

گروه مهندسی کامپیوتر

پایان نامه

برای دریافت درجه کارشناسی ارشد

مهندسی فناوری اطلاعات- شبکه‌های کامپیوتری

بهبود مکانیزم توزیع کلید در شبکه های حسگر بی سیمِ سلسله مراتبی

استاد راهنما:

دکتر مهدی آقا صرام

استاد مشاور:

دکتر فضل‌الله ادیب‌نیا

پژوهش و نگارش:

طاهره امینی علویجه

اسفند ۱۳۹۱

تقدیم به

مهربان فرشتگانی که لحظات ناب باور بودن، لذت و غرور دانستن، جسارت خواستن، عظمت رسیدن و تمام تجربه های یکتا و زیبای زندگیم، مدیون حضور سبز آنهاست...

روح پاک پدری،

که عالمانه به من آموخت تا چگونه در عرصه زندگی، ایستادگی را تجربه نمایم

مادر عزیزتر از جانم،

دریای بی کران فداکاری و عشق، که وجودم برایش همه رنج بود و وجودش برایم همه مهر

یگانه خواهرم:

برای همه رهنمون ها و دلسوزی های خالصانه اش

برادرانم:

بهترین های بی بدیل زندگیم که وجودشان شادی بخش و صفایشان مایه آرامش من است.

پروردگارا، شروع ستایش را به حمد تو آغاز می کنم و به نعمت و احسانت راه حق و صواب را می جویم

و یقین دارم که تو مهربانترین مهربانان عالمی

سپاس بی کران پروردگار یکتا را که، هستی مان بخشید و به طریق علم و دانش رهنمونمان شد

و به همنشینی رهروان علم و دانش مفتخرمان نمود

و خوشه چینی از علم و معرفت را روزیمان ساخت...

تقدیر و تشکر

در طی مسیر این پایان نامه عزیزانی همراهیم کردند که حرمت همراهی و کسب فیض از حضورشان آدمی را به تشکر وا می دارد. اکنون که در سایه عنایت و الطاف خداوندی توفیقی حاصل شد، بر خود لازم می دانم که؛

مراتب سپاس و قدردانی خود را به محضر استاد راهنمای گرانقدرم، جناب آقای دکتر صرام تقدیم نمایم. بزرگواری که افتخار کسب علم و درس زندگی از محضرشان را داشته ام و راهنمایی های ایشان در کنار لطف، حمایت و مهربانی بیکرانشان در حق اینجانب غیر قابل توصیف و جبران است. باشد که این کلام، الطاف ایشان را در مسیر تهیه این پایان نامه بارز سازد.

از استاد مشاور محترم جناب آقای دکتر ادیب نیا نیز کمال امتنان را دارم، به خاطر آن که حرف هایشان روشنگر آینده من بود و به خاطر همه مهربانی های ایشان که درس انسانیت در کلام و رفتارشان یافتم.

در انتها، سپاسی را با تمام وجود از عزیزانی دارم که از آغاز همراه و همیارم بودند، مادر صبورم، خواهر مهربانم و برادران دوست داشتنی ام که گرمی نفسم از گرمای محبتشان است و بیش از لحظه لحظه زندگی ام مدیون همراهی و همیاریشان، هستم.

و تشکر بی شائبه من از سه دوست گرانقدر خانم ها مهندس محمدزاده، مهندس سالارزایی و مهندس رجبی و تمام کسانی که در مسیر زندگیم، چون استادی ناب، کلامی به من آموختند و چون دوستی ارزنده همراه و یاورم بودند. آنان که در راه کسب علم و معرفت برای من آنچه در توان داشتند انجام دادند و مشوق راه دانشم بودند.

چکیده

امنیت و مدیریت کلید یکی از مهمترین مسائل چالش برانگیز و سرویس‌های اساسی در شبکه‌های حسگر بی‌سیم محسوب می‌شود. اولین مرحله در تأمین امنیت، انتخاب یک الگوریتم رمزنگاری مناسب است. در این پایان‌نامه ما از یک الگوریتم رمزنگاری خم بیضوی استفاده کرده‌ایم. این انتخاب نه تنها به دلیل اندازه کوتاه طول کلید و سربار کم محاسباتی است که این الگوریتم ایجاد می‌کند، بلکه الگوریتم خم بیضوی امنیت یکسانی را در مقایسه با سایر روش‌های رمزنگاری کلید عمومی ارایه می‌دهد. ارزیابی کارایی و بررسی امنیت نشان می‌دهد استفاده از این الگوریتم سربار محاسباتی را کاهش می‌دهد و نیاز به حافظه کمتری دارد.

در این پژوهش از یک ساختار سلسله مراتبی و غیرهمگن بهره گرفته‌ایم. در این مدل از نحوه چیدمان گره‌ها آگاهی تقریبی داریم. براین اساس ناحیه آرایش به سلول‌های مربعی تقسیم شده و گره‌های حسگر نیز متناسب با تعداد سلول‌ها به گروه‌هایی تقسیم می‌شوند، به طوری که هر گروه از حسگرها در یکی از این سلول‌ها آرایش می‌یابند. بهره گیری از ساختار سلسله مراتبی و غیرهمگن به همراه آگاهی از نحوه چیدمان از برقراری کلیدهای غیر ضروری جلوگیری می‌کند.

کلمات کلیدی: شبکه حسگر بی‌سیم، شبکه حسگر غیر همگن، امنیت، مدیریت کلید، آگاهی از نحوه چیدمان.

فهرست مطالب

عنوان | صفحه

فهرست شکل‌ها

عنوان صفحه

فهرست جداول

عنوان صفحه

فهرست علائم اختصاری

AES	Advanced Encryotion Standard
AP	Asymmetric Predistribution
BS	Base Station
CH	Cluster Head
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
H-sensor	High-end-sensor
HSN	Heterogeneous Sensor Networks
LEAP	Localized Encryption and Authentication Protocol
L-sensor	Low-end-sensor
MST	Minnimum Spannimg Tree
PDF	Probability Density Function
RSA	Registration/Admission/Status
SNR	Signal to Noise Ratio
SPT	Shortest path Tree
WSN	Wireless Sensor Networks