

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

دانشگاه یزد
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 شبکه‌های حسگر بی سیم
سلسله مراتبی

استاد راهنما:
دکتر مهدی آقا صرام

استاد مشاور:
دکتر فضل‌الله ادیب‌نیا

پژوهش و نگارش:
طاهره امینی علویجه

تقدیم به

مهربان فرشتگانی که سخات 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 عالمنازه من آموخت تا چگونه در عرصه زندگی، ایستادگی را تجربه نمایم

مادر عزیزتر از جانم،

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

یگانه خواهرم:

برای همه رهنمون باو و لوسوزی های خالصانه اش

برادرانم:

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

پروردگارا، شروع تایش را به حمد تو آغاز می‌کنم و به نعمت و احسانت راه حق و صواب را می‌جویم

و یقین دارم که تو مهربانترین مهربانان عالمی

پاس بی‌کران پروردگاریت را که هستی مان‌بخشید و به طریق علم و دانش را، نمونه‌ان شد

و به، همشینی رهروان علم و دانش مفتخرمان نمود

و خوشه‌چینی 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 وامی 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 بیکرانیشان در حق اینجانب غیر قابل توصیف و جبران است. باشد که این کلام، الطاف ایشان را در مسیر تهیه این پایان نامه باز 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 یافتیم.

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 پیش از نطق نطق زندگی ام مدیون همراهی و همیاریشان هستم.

و تشکر بی شائبه من از سه دوست گرانقدر خانم مهندس محمدزاده، مهندس سالارزایی و مهندس رحیمی و تمام کسانی که در مسیر زندگی، 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 ارائه 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. بهره‌گیری 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

صفحه	عنوان
۹	فصل اول: مقدمه‌ای بر شبکه‌های حسگر بی‌سیم.....
۱۱	۱-۱ معرفی شبکه‌های حسگر بی‌سیم.....
۱۲	۲-۱ ساختار کلی شبکه حسگر بی‌سیم.....
۱۳	۳-۱ مدل‌های شبکه.....
۱۵	۴-۱ کاربردهای شبکه‌های حسگر بی‌سیم.....
۱۶	۵-۱ هدف از پژوهش.....
۱۷	۶-۱ ساختار کلی پایان‌نامه.....
۱۹	فصل دوم: امنیت در شبکه‌های حسگر بی‌سیم.....
۲۱	۱-۲ مقدمه.....
۲۲	۲-۲ رمزنگاری.....
۲۳	۳-۲ تهدیدات و حملات.....
۲۴	۴-۲ آسیب‌پذیری‌های امنیتی و نیازمندی‌های آن.....
۲۴	۱-۴-۲ آسیب‌پذیری‌های امنیتی.....
۲۶	۲-۴-۲ نیازمندی‌ها و معیارهای اساسی در برقراری امنیت.....
۳۱	فصل سوم: روش‌های توزیع کلید در شبکه‌های حسگر بی‌سیم.....
۳۳	۱-۳ مقدمه.....
۳۴	۲-۳ استفاده از کلید به روش شبکه‌ای و روش دو سویه کامل.....
۳۵	۳-۳ شیوه‌های پیش‌توزیع کلید.....
۳۵	۱-۳-۳ مسئله پیش‌توزیع کلید تصادفی (طرح پایه).....
۳۷	۲-۳-۳ پروتکل‌های برقراری کلید بر مبنای پیش‌توزیع کلید تصادفی.....
۴۱	۳-۳-۳ پروتکل‌های برقراری کلید بر مبنای چندجمله‌ای‌های متقارن.....

۴۳	شیوه‌های کلید عمومی: ECC و RSA
۴۴	مدیریت کلید سلسله مراتبی (شبکه‌های همگن و غیرهمگن)
۴۴	مدیریت کلید سلسله مراتبی در شبکه‌های همگن
۴۶	مدیریت کلید سلسله مراتبی در شبکه‌های غیرهمگن
۴۹	فصل چهارم: روش پیشنهادی
۵۱	۱-۴ مقدمه
۵۱	۲-۴ مدل کردن آرایش شبکه
۵۲	۱-۲-۴ یک مدل آرایش عمومی
۵۲	۲-۲-۴ مدل آرایش بر مبنای گروه
۵۳	۳-۲-۴ توزیع آرایش
۵۶	۳-۴ سیستم‌های خم بیضوی
۵۶	۴-۴ فرضیات
۵۶	۱-۴-۴ علائم و تعاریف مورد نیاز
۵۸	۲-۴-۴ مدل شبکه
۵۸	۱-۲-۳-۴ مرحله بارگذاری و پیش‌آرایش
۵۹	۲-۲-۳-۴ مرحله آرایش
۶۰	۳-۳-۴ مسیریابی
۶۱	۴-۴ شکل‌گیری خوشه‌ها و گروه‌بندی امن پیشنهادی
۶۵	۵-۴ برقراری کلید متقارن
۶۷	۵ فصل پنجم: تحلیل امنیت و ارزیابی کارایی
۶۹	۱-۵ معیارهای ارزیابی
۶۹	۱-۱-۵ اتصال محلی
۶۹	۲-۱-۵ حافظه مصرفی

۶۹.....	۳-۱-۵	سربار محاسباتی
۷۰.....	۴-۱-۵	انعطاف پذیری در مقابل گره تسخیر شده
۷۰.....	۲-۵	اتصال محلی
۷۱.....	۳-۵	ذخیره‌سازی فضای حافظه
۷۳.....	۴-۵	سربار محاسباتی
۷۴.....	۵-۵	انعطاف پذیری در مقابل گره تسخیر شده
۷۶.....	۶-۵	فسخ گره
۷۷.....		فصل ششم : نتیجه‌گیری و پیشنهادات.....
۷۹.....	۱-۶	نتایج
۸۰.....	۲-۶	پیشنهادات
۸۱.....		لغت نامه انگلیسی به فارسی
۸۵.....		مراجع.....

فهرست شکل‌ها

عنوان	صفحه
شکل ۱-۱: ساختار کلی شبکه‌های حسگر بی‌سیم	۱۳
شکل ۲-۱: مدل‌های شبکه: (a) ساختار سلسله‌مراتبی، (b) ساختار توزیعی	۱۴
شکل ۳-۱: مدل‌های شبکه: الف) ساختار غیرهمگن، ب) ساختار همگن	۱۴
شکل ۱-۳: مثالی از روش پیش‌توزیع کلید [۱۴]	۳۶
شکل ۲-۳: مثالی از شیوه پیش‌توزیع کلید Q-جزیی [۱۴]	۳۸
شکل ۳-۳: به اشتراک گذاری کلید بین مخازن کلید همسایه [۱۵]	۳۹
شکل ۱-۴: نقاط آرایش (هر نقطه معرف یک نقطه آرایش)	۵۵
شکل ۱-۵: احتمال مصالحه شدن [۲۲]	۷۶

فهرست جداول

صفحه	عنوان
۲۳	جدول ۱-۲: مقایسه‌ای بین حسگرهای بی‌سیم نوعی
۵۷	جدول ۱-۴: علائم و توضیحات آن
۷۱	جدول ۱-۵: مقایسه اتصال محلی با روش‌های مختلف
۷۲	جدول ۲-۵: مقایسه حافظه مورد نیاز
۷۳	جدول ۳-۵: حافظه مورد نیاز برای هر گره حسگر
۷۴	جدول ۴-۵: تعداد رمزنگاری/رمزگشایی در زمان تشکیل خوشه‌ها و برقراری کلید مشترک

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 Spanning Tree
PDF	Probability Density Function
RSA	Registration/Admission/Status
SNR	Signal to Noise Ratio
SPT	Shortest path Tree
WSN	Wireless Sensor Networks

