



دانشگاه صنعتی اصفهان

دانشکده‌ی مهندسی برق و کامپیوتر

## مدیریت کلید در شبکه‌های حسگر بی‌سیم

رساله‌ی دکترای مهندسی برق - کامپیوتر

علی فانیان

استاد راهنما

دکتر مهدی برنجکوب



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

## مدیریت کلید در شبکه‌های حسگر بی سیم

رساله دکترای مهندسی برق-کامپیوتر

علی فانیان

استاد راهنما

دکتر مهدی برنجکوب



دانشگاه صنعتی اصفهان  
دانشکده مهندسی برق و کامپیوتر

رساله دکترای مهندسی برق- کامپیوتر آقای علی فانیان  
تحت عنوان

**مدیریت کلید در شبکه‌های حسگر بی‌سیم**

در تاریخ ۱۳۹۰/۱/۲۴ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

- |                           |                               |
|---------------------------|-------------------------------|
| دکتر مهدی برنجکوب         | ۱- استاد راهنمای رساله        |
| دکتر حسین سعیدی           | ۲- استاد مشاور رساله          |
| دکتر محمود سلماسی زاده    | ۳- استاد داور                 |
| دکتر پژمان خدیوی          | ۴- استاد داور                 |
| دکتر مهران سلیمان فلاح    | ۵- استاد داور                 |
| دکتر سید محمود مدرس هاشمی | سرپرست تحصیلات تکمیلی دانشکده |

## مشکر و قدردانی

می‌خواهم از خداوند یکتا به خاطر تمامی نعمت‌هایی که به من ارزانی داشت سپاسگزاری کنم. در اندیشه‌ام که چگونه! چون نمی‌توانم. پس پناه می‌برم به حدیث شریف "من لم یسکر المنعم من المخلوقین لم یسکر الله". پس از استاد راهبانی ارجمندم، جناب آقای دکتر بنگلوب که بار، بنمودهای دلسوزانه، در طول دوران تحقیق همراه من بودند قدردانی می‌کنم. از جناب آقای دکتر سعیدی به خاطر مشاوره‌های ارزنده‌شان سپاسگزارم. از اساتید گرانقدر آقایان دکتر محمود سلامی زاده، دکتر مهران سلیمان فلاح و پرتان خدیوی که زحمت داوری این پایان‌نامه را پذیرفتند و بار، بنمودهای خود به ارتقای آن کمک نمودند، صمیمانه قدردانی می‌نمایم.

دست‌اوپ بر سینم می‌گذارم و دستان مادرم، که با صبوری خود به من صبر کردن آموخت و پدرم، که با تلاش خود به من تلاش کردن آموخت می‌بوسم و از زحمات ایشان سپاسگزارم.

سپاسی صمیمانه از همسرم به خاطر بهیابی خالصانه‌اش، بی‌شک تلاش و از خودگذشتگی این عزیز باعث شد تا من با آسودگی خیال به امر تحقیق بپردازم. براسی که برای ایشان یکی از بزرگترین مواهب الهی بر من بوده است.

بر خود لازم می‌دانم که از توجه، راهبانی، تشویق و بهکاری دوستان بسیار ارجمند خود در آزمایشگاه تحقیقاتی رمزنگاری و امنیت سیستم‌های سپاسگزاری کنم.

از آقای دکتر سعیدی، نایندهی تحصیلات تکلیفی دانشکده، آقای دکتر مدرس هاشمی سرپرست تحصیلات تکلیفی و سرکار خانم کنونی به خاطر زحمات بی‌دینشان مشکر و قدردانی می‌کنم.

کلیه‌ی حقوق مادی مترتب بر نتایج مطالعات،  
ابتکارات و نوآوری‌های ناشی از تحقیق موضوع  
این رساله متعلق به دانشگاه صنعتی اصفهان است.  
این پایان نامه با حمایت مادی و معنوی مرکز  
تحقیقات مخابرات ایران به انجام رسیده است.

تقدیم به

محمدرضا

و

فرزند دلبندم علی رضا



## فهرست مطالب

عنوان	صفحه
فهرست مطالب	هشت
فهرست اشکال	دوازده
فهرست جداول	چهارده
چکیده	۱
<b>فصل اول: مقدمه</b>	۲
۱-۱ مقدمه	۲
۲-۱ شبکه‌های حسگر بی سیم	۳
۳-۱ مروری بر مفاهیم کلی امنیت	۵
۱-۳-۱ مؤلفه‌های امنیتی	۵
۲-۳-۱ حملات امنیتی	۶
۳-۳-۱ مکانیزم‌های پایه امنیتی	۷
۴-۳-۱ سرویس‌های امنیتی	۱۰
۴-۱ انگیزه انتخاب موضوع	۱۲
۵-۱ هدف رساله	۱۳
۶-۱ ساختار ادامه گزارش	۱۴
<b>فصل دوم: مروری بر پروتکل‌های مدیریت کلید در شبکه‌های حسگر</b>	۱۶
۱-۲ مقدمه	۱۶
۲-۲ انواع مدیریت کلید	۱۷
۱-۲-۲ مدیریت کلید متمرکز	۱۷
۲-۲-۲ مدیریت کلید کاملاً توزیع شده	۱۸
۳-۲-۲ مدیریت کلید تمرکززدایی شده	۱۸
۳-۲ مدل توزیع کلید و اطلاعات محرمانه بین حسگرها	۱۹
۱-۳-۲ توزیع کلیدها بدون در نظر گرفتن نحوه توزیع گره‌ها در شبکه	۱۹
۲-۳-۲ توزیع کلیدها بر اساس اطلاعات استقرار گره‌ها در شبکه	۲۰
۴-۲ پروتکل‌های پایه تولید کلید	۲۲
۱-۴-۲ استفاده از یک کلید اصلی	۲۲
۲-۴-۲ استفاده از مرکز توزیع کلید متمرکز	۲۳
۳-۴-۲ پروتکل‌های مبتنی بر پیش توزیع کلید ثابت	۲۴
۴-۴-۲ پروتکل‌های مبتنی بر کلید نامتقارن	۲۵
۵-۴-۲ توزیع کلید تصادفی	۲۵
۶-۴-۲ روش سطح آستانه‌ای Blom	۳۰
۷-۴-۲ چند جمله‌ای‌های متقارن	۳۳
۵-۲ نتیجه گیری	۳۶

۳۸	فصل سوم: ارائه چارچوبی فراگیر برای طراحی و ارزیابی پروتکل‌های مدیریت کلید
۳۸	۱-۳ مقدمه
۳۹	۲-۳ محدودیت‌های شبکه‌های حسگر
۴۱	۳-۳ کاربردهای شبکه‌های حسگر بی‌سیم
۴۵	۴-۳ معرفی پارامترهای مهم در کارایی پروتکل‌های مدیریت کلید
۴۵	۳-۴-۱ همبندی محلی
۴۹	۳-۴-۲ حافظه مصرفی
۵۰	۳-۴-۳ احتمال افشای کلید مستقیم
۵۴	۳-۴-۴ احتمال افشای کلید غیر مستقیم
۵۵	۳-۴-۵ سربار پردازشی
۵۶	۳-۴-۶ سربار ارتباطی
۵۶	۳-۴-۷ مدل تهدید
۵۸	۵-۳ چارچوب طراحی
۵۸	۳-۵-۱ توزیع گره‌ها
۶۱	۳-۵-۲ افراز ناحیه تحت پوشش شبکه
۶۲	۳-۵-۳ تحرک پذیری گره‌ها پس از استقرار در شبکه
۶۲	۳-۵-۴ توزیع متناسب کلیدها و یا اطلاعات محرمانه
۶۳	۳-۶ طرح مسئله
۶۴	۳-۷ نتیجه‌گیری
۶۵	فصل چهارم: ارائه پروتکل‌های جدید تولید کلید برای شبکه‌های حسگر
۶۵	۱-۴ مقدمه
۶۶	۴-۲ پروتکل مدیریت کلید مقاوم و توسعه‌پذیر
۶۸	۴-۲-۱ مدل امنیت در SKEP
۶۹	۴-۲-۲ پیش توزیع اطلاعات محرمانه در SKEP
۷۰	۴-۲-۳ تولید کلید مشترک مستقیم در SKEP
۷۱	۴-۲-۴ تولید کلید غیر مستقیم در SKEP
۷۲	۴-۳ پروتکل مدیریت کلید برای حسگرهای با منابع محدود
۷۴	۴-۳-۱ پیش توزیع اطلاعات محرمانه و کلیدها در KELR
۷۵	۴-۳-۲ تولید کلید مشترک مستقیم در KELR
۷۶	۴-۳-۳ تولید کلید مشترک غیر مستقیم در KELR
۷۶	۴-۴ پروتکل مدیریت با قابلیت تولید بین تمامی گره‌ها
۷۷	۴-۴-۱ مدل امنیت در HKEP
۷۹	۴-۴-۲ نظریه‌ی طراحی‌های ترکیبیاتی
۸۳	۴-۴-۳ توزیع سهم‌ها بین گره‌های حسگر در HKEP
۸۷	۴-۴-۴ توزیع کلیدهای تصادفی بین گره‌های حسگر
۸۹	۴-۵ پروتکل مدیریت کلید دارای امنیت کامل غیر آستانه‌ای

۸۹	..... پروتکل تولید کلید غیر آستانه‌ای
۹۱	..... توزیع کلیدها بین گره‌ها
۹۲	..... HKey طرح اول تولید کلید مبتنی بر پروتکل HKey
۹۳	..... HKey طرح دوم تولید کلید مبتنی بر پروتکل HKey
۹۴	..... HKey طرح سوم تولید کلید مبتنی بر پروتکل HKey
۹۵	..... HKey طرح چهارم تولید کلید مبتنی بر پروتکل HKey
۹۶	..... نتیجه گیری
۹۷	<b>فصل پنجم: ارزیابی پروتکل‌های مدیریت کلید</b>
۹۷	..... ۱-۵ مقدمه
۹۸	..... ۲-۵ مشخصات شبکه مورد ارزیابی
۹۹	..... ۳-۵ همبندی محلی
۹۹	..... ۱-۳-۵ احتمال تولید کلید مشترک بین دو گره در پروتکل SKEP
۱۰۳	..... ۲-۳-۵ احتمال تولید کلید مشترک بین دو گره در پروتکل KELR
۱۰۴	..... ۳-۳-۵ احتمال تولید کلید مشترک بین دو گره در پروتکل HKEP
۱۰۴	..... ۴-۳-۵ احتمال تولید کلید مشترک بین دو گره در پروتکل HKey
۱۰۵	..... ۵-۳-۵ احتمال تولید کلید مشترک بین گره‌ها در سایر پروتکل‌ها
۱۰۹	..... ۶-۳-۵ مقایسه همبندی محلی پروتکل‌های ارزیابی شده
۱۱۰	..... ۴-۵ حافظه مصرفی
۱۱۱	..... ۱-۴-۵ حافظه مصرفی در پروتکل SKEP
۱۱۲	..... ۲-۴-۵ حافظه مصرفی در پروتکل KELR
۱۱۲	..... ۳-۴-۵ حافظه مصرفی در پروتکل HKEP
۱۱۳	..... ۴-۴-۵ حافظه مصرفی در پروتکل HKey
۱۱۶	..... ۵-۴-۵ حافظه مصرفی در سایر پروتکل‌های مورد مقایسه
۱۱۸	..... ۵-۵ مقاومت در برابر افشای کلید مستقیم
۱۱۹	..... ۱-۵-۵ احتمال افشای کلید مستقیم در پروتکل SKEP
۱۱۹	..... ۲-۵-۵ احتمال افشای کلید مستقیم در پروتکل KELR
۱۲۱	..... ۳-۵-۵ احتمال افشای کلید مستقیم در پروتکل HKEP
۱۲۲	..... ۴-۵-۵ احتمال افشای کلید مستقیم در سایر پروتکل‌های مورد مقایسه
۱۲۹	..... ۶-۵ انرژی مصرفی
۱۳۰	..... ۱-۶-۵ میزان انرژی مصرفی در پردازش محاسبات
۱۳۳	..... ۲-۶-۵ میزان انرژی مصرفی در تبادل اطلاعات
۱۳۷	..... ۷-۵ ارزیابی سرجمع پروتکل‌های رقیب
۱۴۲	..... ۸-۵ نتیجه گیری
۱۴۳	<b>فصل ششم: نتیجه گیری</b>
۱۴۳	..... ۱-۶ مقدمه
۱۴۳	..... ۲-۶ مرور مطالب

۱۴۸.....	۳-۶ نوآوری‌ها
۱۵۰.....	۴-۶ پیشنهادات
۱۵۰.....	۱-۴-۶ پروتکل‌های مدیریت کلید در شبکه‌های حسگر سلسله مراتبی
۱۵۰.....	۲-۴-۶ پروتکل‌های مدیریت کلید در شبکه‌های حسگر نامتجانس
۱۵۰.....	۳-۴-۶ پروتکل‌های تولید کلید برای ارتباطات گروهی در شبکه‌های حسگر
۱۵۱.....	۴-۴-۶ طراحی پروتکل مسیریابی امن به همراه پروتکل مدیریت کلید
۱۵۱.....	۵-۴-۶ طراحی پروتکل مدیریت کلید برای شبکه‌های حسگر در محیط متفاوت
۱۵۲.....	۶-۴-۶ مدیریت کلید و سیستم‌های تشخیص نفوذ
۱۵۲.....	۷-۴-۶ مقایسه کارایی پروتکل‌های مدیریت کلید متقارن و نامتقارن در شرایط امنیت کامل
۱۵۳.....	۸-۴-۶ ارزیابی کارایی پروتکل‌های مدیریت کلید در شبکه‌های حسگر متحرک
۱۵۴.....	<b>پیوست ۱: فهرست مقالات مستخرج از رساله</b>
۱۵۵.....	<b>پیوست ۲: فهرست الفبایی واژگان و اصطلاحات تخصصی</b>
۱۵۹.....	<b>فهرست مراجع</b>

## فهرست اشکال

<u>صفحه</u>	<u>عنوان</u>
۵	شکل ۱-۱: ساختار کلی شبکه حسگر.....
۱۸	شکل ۱-۲: دسته‌بندی مدل‌های امنیتی متمرکز.....
۲۱	شکل ۲-۲: افراز شبکه به سلول‌های مربعی هم اندازه.....
۲۱	شکل ۳-۲: توزیع گره‌های اختصاص یافته به یک سلول.....
۳۰	شکل ۴-۲: اشتراک کلیدها در استخراج کلیدهای اختصاصی به هر سلول [۴۵].....
۳۱	شکل ۵-۲: اختصاص کلید مشترک بین دو گره $i$ و $z$ در روش Blom.....
۳۲	شکل ۶-۲: اختصاص تعدادی ماتریس به هر سلول و انتخاب $T$ ماتریس برای هر گره.....
۳۹	شکل ۱-۳: ساختمان داخلی یک گره حسگر [۸۰].....
۴۸	شکل ۲-۳: احتمال قرار گرفتن گره‌ها درون یک دایره. (الف) $i$ داخل دایره $z < R$ (ب) $i$ خارج از دایره $z > R$ .....
۵۹	شکل ۳-۳: تابع توزیع احتمال هر گروه.....
۶۰	شکل ۴-۳: توزیع حسگرها در شبکه با مقادیر مختلف $\sigma$ .....
۶۱	شکل ۵-۳: افراز شبکه به سلول‌های شش گوش منتظم.....
۶۲	شکل ۶-۳: فاصله بین نقطه توزیع در دو سلول مجاور.....
۷۰	شکل ۱-۴: افراز یک سلول به نواحی مجازی و تشکیل گروه.....
۷۱	شکل ۲-۴: نواحی تولید کلید مشترک مستقیم بین یک حسگر و حسگرهای واقع در آن نواحی.....
۷۵	شکل ۳-۴: افراز شبکه و گروه‌بندی سلول‌ها در KELR.....
۸۱	شکل ۴-۴: مربع لاتین از مرتبه ۴.....
۸۱	شکل ۵-۴: زمانبندی بازی ۸ تیم در ۷ دور.....
۸۱	شکل ۶-۴: سه MOLS از مرتبه ۴.....
۸۳	شکل ۷-۴: صفحه مستوی با پارامترهای 1,3,12.....
۸۳	شکل ۸-۴: صفحه تصویری با پارامترهای 1,3,13.....
۸۶	شکل ۹-۴: گروه‌بندی بین سلولی گره‌های حسگر در روش پیشنهادی.....
۸۷	شکل ۱۰-۴: نام‌گذاری نواحی یک گروه.....
۹۲	شکل ۱۱-۴: گروه‌بندی گره‌های حسگر در مدل HKey-LR.....
۹۳	شکل ۱۲-۴: گروه‌بندی طرح HKey-MR.....
۹۴	شکل ۱۳-۴: گروه‌بندی در طرح HKey_AMR.....
۹۵	شکل ۱۴-۴: گروه‌بندی طرح HKey-HP.....
۱۰۱	شکل ۱-۵: گروه‌های مشترک دو حسگر متعلق به دو سلول همسایه در پروتکل SKEP.....
۱۰۲	شکل ۲-۵: گروه‌های مشترک بین $C_{i,j}$ و $C_{i+1,j+2}$ .....
۱۰۲	شکل ۳-۵: نواحی مجازی سلول‌های $C_{i,j}$ و $C_{i+2,j+2}$ متعلق به یک گروه.....
۱۰۳	شکل ۴-۵: همبندی محلی پروتکل KELR به ازای مقادیر مختلف $m$ .....

- شکل ۵-۵: تولید کلید مشترک بین گره‌ها در پروتکل LAKE [۷۵]. ۱۰۶.....
- شکل ۵-۶: گروه‌بندی در LPBK. ۱۰۶.....
- شکل ۵-۷: گروه‌بندی در پروتکل Yu [۷۲]. ۱۰۷.....
- شکل ۵-۸: همبندی محلی پروتکل [۴۵] به ازای مقادیر مختلف  $m$ . ۱۰۸.....
- شکل ۵-۹: ماتریس Vandermonde. ۱۱۲.....
- شکل ۵-۱۰: احتمال افشای کلید مستقیم در روش Du-1 [۴۵]. ۱۲۴.....
- شکل ۵-۱۱: احتمال افشای کلید مستقیم در روش Du-2 [۷۱]. ۱۲۵.....
- شکل ۵-۱۲: احتمال افشای کلید مستقیم در روش‌های LAKE [۷۵]، LPBK [۷۶] و Yu [۷۲]. ۱۲۷.....
- شکل ۵-۱۳: احتمال افشای کلید مستقیم در روش‌های SKEP [۱۰۲]، KELR [۱۰۱]، HKEP [۱۰۰] و HKey. ۱۲۸.....
- شکل ۵-۱۴: شبه کد الگوریتم ضرب پیمان‌های. ۱۳۱.....
- شکل ۵-۱۵: احتمال تولید کلید مشترک در حداکثر ۳ گام. ۱۳۴.....

## فهرست جداول

صفحه	عنوان
۴۰	جدول ۱-۳: مشخصات سخت‌افزاری چند نمونه گره حسگر
۸۵	جدول ۱-۴: تعداد بلوک‌ها برای مقادیر مختلف $p$
۹۱	جدول ۲-۴: تطبیق کلید بین گره‌های حسگر
۹۲	جدول ۳-۴: کلیدهای تولید شده در فاز دوم
۱۰۵	جدول ۱-۵: همبندی محلی طرح‌های مختلف پروتکل HKey
۱۰۸	جدول ۲-۵: همبندی محلی پروتکل [۷۱] به ازای مقادیر مختلف $\tau$
۱۰۹	جدول ۳-۵: همبندی محلی پروتکل‌های مختلف
۱۱۰	جدول ۴-۵: همبندی محلی تعدادی پروتکل با $\sigma = 30$
۱۱۸	جدول ۵-۵: همبندی محلی پروتکل‌های مختلف
۱۳۰	جدول ۶-۵: مشخصات الکترونیکی ریزپردازنده ATMEGA128L
۱۳۳	جدول ۷-۵: انرژی مصرفی برای محاسبه کلید مشترک
۱۳۶	جدول ۸-۵: انرژی مصرفی برای محاسبه کلید مشترک
۱۳۹	جدول ۹-۵: کارایی پروتکل‌های مختلف در شرایط بحرانی و طول کلید ۶۴ بیت
۱۴۰	جدول ۱۰-۵: کارایی پروتکل‌های مختلف در شرایط وخیم و طول کلید ۶۴ بیت
۱۴۱	جدول ۱۱-۵: کارایی پروتکل‌های مختلف در شرایط بحرانی و طول کلید ۹۶ بیت
۱۴۲	جدول ۱۲-۵: کارایی پروتکل‌های مختلف در شرایط وخیم و طول کلید ۹۶ بیت

## چکیده

پیشرفت‌های اخیر در زمینه الکترونیک و مخابرات بی‌سیم، توانایی طراحی و ساخت حسگرهایی با توان مصرفی پایین، اندازه کوچک، قیمت مناسب و کاربری‌های گوناگون را به وجود آورده است. این حسگرهای کوچک که توانایی انجام اعمالی چون دریافت اطلاعات مختلف محیطی، پردازش اطلاعات و ارسال آن‌ها را دارند، موجب پیدایش ایده‌ای برای ایجاد و گسترش شبکه‌های موسوم به شبکه‌های حسگر بی‌سیم شده‌اند. یک شبکه حسگر متشکل از تعداد زیادی گره حسگر است که در یک محیط به طور گسترده پخش می‌شوند. با توجه به این که ممکن است گره‌های حسگر در محیط‌های عملیاتی ناامن قرار گیرند، مخصوصاً در کاربردهای نظامی، امنیت یکی از پارامترهای مهم و ضروری در این شبکه‌ها است. از این رو سرویس‌های امنیتی نظیر احراز اصالت و محرمانگی باید در این شبکه‌ها مورد استفاده قرار گیرند تا بتوان از عملکرد گره‌ها و در نهایت شبکه مطمئن بود. ارائه این سرویس‌ها در سطح شبکه مستلزم وجود یک زیر ساخت امنیتی بین گره‌های شبکه است که به شکل مناسبی کلیدهای مشترکی را برای احراز اصالت و محرمانگی گره‌ها فراهم نماید. چارچوبی که طی آن نیازمندی فوق برآورده می‌شود را مدیریت کلید می‌گویند. در چند سال اخیر روش‌های زیادی برای مدیریت کلید در شبکه‌های حسگر بی‌سیم ارائه شده است. اهم پروتکل‌های ارائه شده مبتنی بر سه روش توزیع کلید تصادفی، Blom و چند جمله‌ای متقارن هستند. برخی از این روش‌ها از همبندی محلی و مقاومت مناسبی در قبال افشای کلید برخوردار هستند اما نیاز به صرف منابع زیادی در گره‌های حسگر دارند به طوری که استفاده از آن‌ها در گره‌های حسگر مقدور نیست. در مقابل، برخی دیگر از این روش‌ها از نظر مصرف منابع مناسب هستند اما با چالش‌های امنیتی و یا کارایی روبرو هستند. در این رساله ابتدا با بررسی و شناخت چالش‌های فراروی شبکه‌های حسگر سعی در طراحی پروتکل‌های مدیریت کلیدی است که قابل به کارگیری در گره‌های حسگر باشند و همچنین کارآمدی و امنیت آن‌ها در سطح قابل قبولی باشد. به این منظور، پس از شناخت مسائل پیرامون مدیریت کلید در شبکه‌های حسگر چارچوبی برای طراحی پروتکل‌های مدیریت کلید جدید ارائه می‌گردد و به دنبال آن چهار پروتکل با نام‌های SKEP، KEPR، KEPR و HKey به منظور استفاده در کاربردهای مختلف ارائه می‌گردد. در پروتکل‌های پیشنهادی با استفاده از ساختارهای منظم در گروه‌بندی گره‌ها در شبکه سعی می‌شود دو گره قبل از هر گونه تماس با یکدیگر از امکان تولید کلید مشترک با یکدیگر با خبر باشند. برای ارزیابی کارایی پروتکل‌های پیشنهادی و اهم پروتکل‌های در دسترس پارامترهای مختلفی از قبیل همبندی محلی، حافظه مصرفی، امنیت کلیدهای ارتباطی در مقابل تبانی گره‌های تسخیر شده و انرژی مصرفی از طریق شبیه‌سازی و یا اثبات ریاضی مورد مقایسه قرار می‌گیرند. به منظور مقایسه عادلانه پروتکل‌ها از نظر میزان حافظه و انرژی مصرفی در گره‌ها، شرایط امنیت کامل در نظر گرفته می‌شود. از سوی دیگر برای اینکه بتوان با یک مقایسه اجمالی کارایی پروتکل‌های مختلف را مشاهده نمود، با انتخاب یک گره حسگر معروف مقدار پارامترهای تأثیرگذار در کارایی پروتکل‌های مختلف به طور سرجمع مورد مقایسه قرار می‌گیرند. نتایج بدست آمده نشان دهنده کارایی مناسب پروتکل‌های طراحی شده، به ویژه پروتکل HKey، نسبت به سایر پروتکل‌های موجود است.

کلمات کلیدی: ۱- مدیریت کلید ۲- شبکه‌های حسگر ۳- چند جمله‌ای متقارن ۴- توزیع کلید تصادفی ۵- امنیت کامل



## فصل اول

### مقدمه

#### ۱-۱ مقدمه

با پیشرفت حاصل شده در دهه اخیر در زمینه شبکه‌های بی‌سیم استفاده از این شبکه‌ها به شدت رو به گسترش است. در این شبکه‌ها عموماً گره‌ها از کانال مشترک برای تبادل اطلاعات استفاده می‌نمایند. این خصوصیت باعث می‌شود تا دسترسی به اطلاعات دیگران به طور غیر مجاز امکان پذیر شده و زمینه بروز حملات مختلف فراهم گردد. از این رو امنیت اطلاعات در شبکه‌های بی‌سیم با چالش‌های جدی مواجه است که نیازمند بررسی و ارائه راه کارهایی برای بهبود سطح امنیت در این شبکه‌ها است.

در یک دسته بندی کلی شبکه‌های بی‌سیم را می‌توان به دو دسته شبکه‌های ساختارمند و بدون ساختار تقسیم کرد [۱]. در شبکه‌های ساختارمند به راه‌اندازی ساختار اولیه برای ایجاد شبکه نیاز است. یکی از معروفترین شبکه‌های ساختارمند شبکه‌های سلولی هستند. در شبکه‌های سلولی، محیط تحت پوشش به سلول‌هایی تقسیم‌بندی می‌شود و در هر سلول از یک ایستگاه مرکزی برای برقراری ارتباط کاربران با یکدیگر استفاده می‌گردد. در شبکه‌های بدون ساختار نیازی به ایجاد ساختار از پیش تعیین شده وجود ندارد. شبکه‌های اقتضایی<sup>۱</sup> و حسگر نمونه‌هایی از شبکه‌های

---

<sup>۱</sup> ad-hoc network

بدون ساختار هستند که به شدت مورد توجه قرار گرفته‌اند. این شبکه‌ها با اجتماع تعدادی گره بی‌سیم با هزینه کم راه‌اندازی می‌شوند [۲، ۳، ۴]. این ویژگی باعث شده است که این شبکه‌ها در حوزه‌های مختلف به ویژه دفاعی، زیست محیطی و علمی کاربردهای زیادی پیدا کنند [۵، ۶، ۷]. با توجه به آنکه شبکه‌های حسگر در آینده در کاربردهای مختلف مورد استفاده قرار می‌گیرند، در این رساله مباحث پیرامون مدیریت کلید در این شبکه‌ها مورد تحقیق و بررسی قرار خواهد گرفت. شبکه‌های حسگر بر اساس نوع سخت‌افزار مورد استفاده به دو دسته همگن<sup>۱</sup> و ناهمگن<sup>۲</sup> تقسیم‌بندی می‌شوند [۸]. در شبکه‌های که از حسگرهای همگن استفاده می‌شود قابلیت سخت‌افزار گره‌ها شبیه بهم است. اما در گره‌های ناهمگن سخت‌افزار گره‌ها مشابه نیستند و دارای قابلیت‌های مختلف می‌باشند. در یک دسته بندی دیگر که بر اساس نقش گره‌های حسگر در شبکه انجام می‌شوند، شبکه‌های حسگر به دو دسته مسطح<sup>۳</sup> و سلسه مراتبی<sup>۴</sup> تقسیم‌بندی می‌شوند [۹، ۱۰، ۱۱]. در شبکه‌های حسگر مسطح نقش گره‌های حسگر در شبکه مشابه هستند اما در شبکه‌های سلسه مراتبی گره‌ها با توجه به قابلیت‌ها و امکاناتشان وظایف و نقشهای متفاوتی دارند. در این رساله شبکه‌های حسگر مسطح مورد توجه و تحقیق قرار گرفته‌اند. از این رو در ادامه منظور از شبکه‌های حسگر، شبکه‌های حسگر مسطح است.

در این فصل ابتدا شبکه‌های حسگر معرفی خواهد شد و پس از آن مؤلفه‌های امنیتی و مکانیزم‌های امنیتی مورد نیاز مرور خواهد شد. در پایان فصل نیز ساختار ادامه گزارش خواهد آمد.

## ۲-۱ شبکه‌های حسگر بی‌سیم

پیشرفت‌های اخیر در زمینه الکترونیک و مخابرات بی‌سیم، توانایی طراحی و ساخت حسگرهایی با توان مصرفی پایین، اندازه کوچک، قیمت مناسب و کاربردهای گوناگون را به وجود آورده است. این حسگرهای کوچک که توانایی انجام اعمالی چون دریافت اطلاعات مختلف محیطی (بر اساس نوع حسگر)، پردازش اطلاعات و ارسال آن‌ها را دارند، موجب پیدایش ایده‌ای برای ایجاد و گسترش شبکه‌های موسوم به شبکه‌های بی‌سیم حسگر شده‌اند. شبکه‌های حسگر در واقع زیر مجموعه‌ای از شبکه‌های اقتضایی محسوب می‌شوند که در آن‌ها توان پردازشی و رادیویی گره‌های حسگر بسیار پایین می‌باشد [۱۲].

<sup>1</sup> homogeneous

<sup>2</sup> heterogeneous

<sup>3</sup> flat

<sup>4</sup> hierarchical

یک شبکه حسگر متشکل از تعداد زیادی گره‌های حسگر است که در یک محیط به طور گسترده پخش شده و به جمع‌آوری اطلاعات از محیط می‌پردازند. لزوماً مکان قرار گرفتن گره‌های حسگر، از قبل تعیین شده و مشخص نیست. چنین خصوصیتی این امکان را فراهم می‌آورد که بتوانیم آن‌ها را در مکان‌های خطرناک و یا غیرقابل دسترس رها کنیم. این بدان معنی است که پروتکل‌ها و الگوریتم‌های شبکه‌های حسگر باید دارای توانایی‌های خودسازماندهی باشند [۱۳].

هر گره حسگر بر روی سخت‌افزار خود دارای یک پردازشگر می‌باشد و به جای فرستادن تمامی اطلاعات خام به مرکز یا به گره دیگر که مسئول پردازش و نتیجه‌گیری اطلاعات است، ابتدا خود یک سری پردازش‌های اولیه و ساده را بر روی اطلاعات انجام می‌دهد و سپس نتایج و یا در صورت لزوم داده‌ها را ارسال می‌کند. از طرف دیگر ممکن است یک گره حسگر به صورت کارانداز<sup>۱</sup> عمل کند و یک عمل خاصی مانند قطع و وصل یک کلید را انجام دهد. بنابراین تبادل اطلاعات در شبکه‌های حسگر / کارانداز به صورت دوطرفه صورت می‌گیرد.

با اینکه هر حسگر به تنهایی توانایی ناچیزی دارد، ترکیب صدها حسگر کوچک امکانات جدیدی را برای کل شبکه عرضه می‌کند. در واقع قدرت شبکه‌های بی‌سیم حسگر در توانایی به‌کارگیری تعداد زیادی گره کوچک است که قادرند به شکل خودکار سازماندهی شوند و در موارد متعددی چون مسیریابی هم‌زمان، نظارت بر شرایط محیطی، نظارت بر سلامت ساختارها یا تجهیزات یک سیستم به کار گرفته شوند.

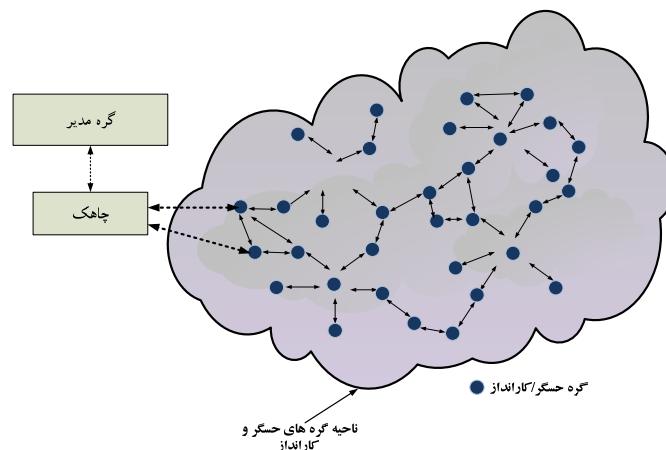
در ابتدای راه اندازی شبکه حسگر، گره‌های حسگر به صورت نامنظم در یک منطقه پراکنده می‌شوند. هر کدام از این گره‌های پخش شده دارای توانایی جمع‌کردن اطلاعات و ارسال آن‌ها به پایانه‌ای موسوم به چاهک<sup>۲</sup> هستند. این اطلاعات از یک مسیر چند گامی<sup>۳</sup> که زیرساخت مشخصی ندارد (همانند شبکه اقتضایی) به چاهک فرستاده می‌شوند و چاهک می‌تواند توسط ارتباط ماهواره یا اینترنت با گره مدیر ارتباط برقرار کند. از سوی دیگر یک چاهک یا مدیر ممکن است اطلاعات خاصی را برای گره‌های حسگر یا کارانداز ارسال نماید [۱۴].

طراحی یک شبکه حسگر تحت تأثیر عوامل متعددی می‌باشد. این عوامل عبارتند از: تحمل خرابی، قابلیت گسترش، هزینه تولید، محیط کار، توپولوژی شبکه حسگر، محدودیت‌های سخت‌افزاری، محیط انتقال و مصرف توان. در شکل ۱-۱ ساختار کلی شبکه حسگر مشاهده می‌شود.

<sup>1</sup> actuator

<sup>2</sup> sink

<sup>3</sup> multi-hop



شکل ۱-۱: ساختار کلی شبکه حسگر

### ۳-۱ مروری بر مفاهیم کلی امنیت

بدون شک زندگی امروز بشر از مقوله ارتباطات تفکیک ناپذیر است. ارتباطات به حدی فاصله‌های دور را به هم نزدیک کرده است که از دنیای بزرگ ما به نام دهکده جهانی یاد می‌شود. ارتباطات آنقدر با زندگی روزمره ما عجین شده است که نمی‌توانیم حتی زندگی بدون آنرا تصور کنیم. در حالیکه تا قرن‌ها پیش مبادله خبر به روزها زمان نیاز داشت، اینکار اکنون تقریباً آنی انجام می‌شود. مخابرات، اینترنت و وسایل ارتباط جمعی نمونه‌هایی از ارتباطات امروزه ما هستند که تبادل اطلاعات و انجام امور روزمره ما را با سهولت بیشتر و هزینه کمتر ممکن ساخته است. از طرف دیگر گسترش ارتباطات شبکه‌ای و نفوذ آن به دوردست‌ترین نقاط جهان باعث شده است زمینه سوء استفاده افراد سودجو هم فراهم شود. در حالیکه هم‌اکنون انجام معاملات کلان اقتصادی و تبادل اطلاعات حیاتی در کوتاهترین زمان به راحتی و با هزینه ناچیز روی شبکه‌های کامپیوتری و اینترنت قابل انجام است، اما انجام این امور بدون در نظر گرفتن تمام جنبه‌های امنیتی، ممکن است باعث ضررهای جبران ناپذیری گردد. از همین جا لزوم امنیت شبکه و ایجاد ارتباط امن احساس می‌شود. برای آشنایی دقیق‌تر با ابعاد امنیت، در این بخش مفاهیم کلی امنیت مرور خواهند شد.

#### ۱-۳-۱ مؤلفه‌های امنیتی

برای تبیین مفهوم امنیت باید به مؤلفه‌های برقراری امنیت در شبکه‌های کامپیوتری پرداخت. این مؤلفه‌ها شامل محرمانگی<sup>۱</sup>، صحت<sup>۲</sup> و دسترس پذیری<sup>۱</sup> است [۱۵، ۱۶، ۱۷، ۱۸] که در ادامه معرفی می‌شوند.

<sup>۱</sup> confidentiality

<sup>۲</sup> integrity