

رمزنگاری شبکه حسگر بی سیم

مؤلفین:

آلاله ارجمند

دکتر علی نژاد

آفتاب گیتی

موسسه انتشاراتی آفتاب گیتی



سرشناسه	:	ارجمند، آلاله، ۱۳۶۲-
عنوان و نام پدیدآور	:	رمزنگاری شبکه حسگر بی سیم/تهیه و تألیف آلاله ارجمند، ندا علی نژاد.
مشخصات نشر	:	تهران: آفتاب گیتی، ۱۳۹۹.
مشخصات ظاهری	:	۱۳۸ص: مصور، جدول، نمودار.
شابک	:	۹۷۸-۶۲۲-۲۴۵۳۸۹-۳
وضعیت فهرست نویسی	:	فیبا
یادداشت	:	کتابنامه.
موضوع	:	شبکه های حسگر بی سیم -- تدابیر ایمنی
موضوع	:	Wireless sensor networks -- Security measures
شماره آید	:	علینژاد، ندا، ۱۳۶۸ -
رده بندی کنگره	:	TK۷۸۷۲
رده بندی دیویی	:	۶۸۲۲/۰۰۴
شماره کتابشناسی	:	۷۳۰۳۸

آفتاب گیتی
ناشر

عنوان: رمزنگاری شبکه حسگر بی سیم

مؤلفین: آلاله ارجمند، ندا علی نژاد

صفحه آرای و تنظیم: نوژن گرافیک

نشر و پخش: موسسه انتشاراتی آفتاب گیتی

نوبت چاپ: اول، ۱۳۹۹

شمارگان: ۱۰۰۰ نسخه

چاپ: پاسارگاد

قیمت: ۲۵۰۰۰۰ ریال

شابک: ۹۷۸-۶۲۲-۲۴۵-۳۸۹-۳

کلیه حقوق برای ناشر محفوظ است.

آدرس: تهران میدان انقلاب ضلع جنوب شرقی- نبش خیابان ۱۲ فروردین-

ساختمان ولیعصر- پلاک ۱۳۱۴- طبقه سوم. واحد ۹

www.aftabegiti.com نشر و پخش همراه: ۰۹۱۲۳۳۴۲۳۶۲-۰۲۱۶۶۹۶۹۸۳۷

فهرست مطالب

فصل ۱. معرفی شبکه حسگر بی سیم

۱	مقدمه	۱-۱
۲	تعریف شبکه حسگر بی سیم	۱-۲
۳	ساختار کلی شبکه های حسگر	۱-۳
۴	ساختار خودکار	۱-۳-۱
۵	ساختار نیمه خودکار	۱-۳-۲
۵	ساختار متمرکز	۱-۳-۳
۶	ویژگی ها	۱-۳-۴
۷	کاربردها	۱-۳-۵
۸	ویژگی های شبکه های حسگر	۱-۳-۶
۹	ساختار ارتباطی شبکه های حسگر	۱-۳-۷
۱۴	پشته پروتکلی	۱-۴
۱۶	موضوعات مطرح	۱-۵
۲۳	معماری ارتباطی در شبکه های حسگر	۱-۶

فصل ۲. امنیت در شبکه حسگر بی سیم

۲۵	مقدمه	۲-۱
۲۵	جنبه های اصلی امنیتی شبکه حسگر بی سیم	۲-۲
۲۶	موانع امنیتی حسگر	۲-۲-۱
۲۹	نیازمندی های امنیتی - اهداف امنیتی	۲-۲-۲
۳۵	حملات در شبکه حسگر بی سیم	۲-۲-۳

- ۳-۲. حملات شبکه های حسگر بی سیم و تکنیک های تدافعی ممکن ۳۶
- ۳-۲-۱. راه حل های تشخیص حمله سیبل و حذف آنها به سه دسته ۳۹
- ۴-۲. تحلیل حمله ۴۶
- ۵-۲. معماری ها و پروتکل های مسیریابی ۴۷
- ۶-۲. مدیریت کلید ۴۹
- ۷-۲. همزمان سازس امن ۵۰
- ۸-۲. کشف محل امن ۵۱
- ۹-۲. نکات امنیتی بی سیم ۵۳
- ۱۰-۲. ارائه دل مدیریت امنیت برای شبکه حسگر بی سیم شامل: ۵۵
- ۱۱-۲. اجرای خورشم رمزنگاری RSA برای شبکه های حسگر بی سیم ۵۷
- ۱-۱۱-۲. رمز یک کلید ۵۸
- ۲-۱۱-۲. رمزنگاری ۶۰

فصل ۳. مسیریابی

- ۶۳
- ۱-۳. دلایل اهمیت به مسیریابی در شبکه حسگر بی سیم ۶۳
- ۲-۳. چالش های مسیریابی ۶۳
- ۱-۲-۳. میانگین میزان توان مصرفی در هر گره ۶۴
- ۳-۳. یک روش پیشنهادی در مسیریابی ۶۶
- ۴-۳. خوشه بندی و امنیت در شبکه حسگر بی سیم ۶۷
- ۱-۴-۳. خوشه بندی در شبکه حسگر بی سیم ۶۸
- ۲-۴-۳. اهداف و چالش های طرح خوشه بندی در شبکه حسگر بی سیم ۷۰
- ۱-۲-۴-۳. پارامترهای خوشه بندی ۷۳
- ۲-۲-۴-۳. طبقه بندی پروتکل های خوشه بندی ۷۵
- ۳-۴-۲-۲-۱. سلسله مراتب خوشه بندی تطبیق پذیری کم
- انرژی (LEACH) ۷۸
- ۲-۲-۲-۴-۳. الگوریتم HEED ۸۱
- ۳-۲-۲-۴-۳. پروتکل PEGASIS ۸۳

۸۵	۵-۳. پروتکل های مسیریابی
۸۵	۱-۵-۳. پارامترهای پروتکل های مسیریابی
۸۸	۲-۵-۳. انواع پروتکل های مسیریابی
۸۸	۱-۲-۵-۳. مسیریابی تخت
۸۸	۲-۲-۵-۳. پروتکل سیل آسا
۸۹	۳-۲-۵-۳. پروتکل شایعه پراکنی
۸۹	۴-۲-۵-۳. پروتکل SPIN
۹۲	۵-۲-۵-۳. انتشارمستقیم
۹۴	۶-۲-۵-۳. مسیریابی سلسله مراتبی
۹۶	۷-۲-۵-۳. پروتکل مسیریابی مبتنی بر مکان
۹۷	فصل ۴. مکانیزم های امنیتی
۹۷	۱-۴. خواب گره Sleep attack
۹۹	۲-۴. انکار حمله خواب
۱۰۰	۱-۲-۴. پروتکل های MAC
۱۰۲	۲-۲-۴. روش پیشنهادی
۱۰۶	۳-۴. کارایی الگوریتم های رمزنگاری بر روی شبکه حسگر بی سیم
۱۰۹	۱-۳-۴. رمز های بلوک به صورت زنجیره ای
۱۱۱	۲-۳-۴. ارزیابی عملکرد الگوریتم
۱۱۹	فصل ۵. جمع بندی و نتیجه گیری
۱۲۰	منابع و مآخذ