

مقدمه‌ای بر شبکه‌های موردی

(با رویکرد امنیت)

مؤلفین:

مهران آقایی

مصطفی اخوان صفار

محمد محسن صدر

(اعضای هیات علمی دانشگاه پیام نور)

سرشناسه	: آقای، مهران، ۱۳۶۳
عنوان و نام پدیدآور	: مقدمه ای بر شبکه های موردی / مولفین مهران آقای، مصطفی اخوان صفار، محمد محسن صدر (اعضای هیات علمی دانشگاه پیام نور)
مشخصات نشر	: مشهد: انتشارات خط اول، ۱۳۹۵
مشخصات ظاهری	: ۲۴۰ ص:، مصور، جدول، نمودار
شابک	: 978-600-96894-2-2
وضعیت فهرست نویسی	: فیا
یادداشت	: واژه نامه
یادداشت	: کتابنامه
موضوع	: شبکه های موردی
موضوع	: Ad hoc networks (Computer networks)
شناسه افزوده	: اخوان صفار، مصطفی، ۱۳۶۱
شناسه افزوده	: صدر، محمد محسن ۱۳۵۷
رده بندی کنگره	: TK۷/۵۱-۵/۲۷ ۱۳۹۵
رده بندی دیویی	: ۰۰۴-۸
شماره کتابشناسی ملی	: ۴۵۰۵۹۸۸



تلفن: ۰۵۱۳۷۵۲۹۹۹۳

www.khate-aval.com

info@khate-aval.com

نام ناشر: انتشارات خط اول

نام کتاب: مقدمه ای بر شبکه های موردی (با رویکرد امنیت)

نویسندگان: مهران آقای، مصطفی اخوان صفار، محمد محسن صدر

صفحه آرا: نفیسه اسماعیلی

شمارگان: ۱۰۰۰ جلد

نوبت چاپ: اول / زمستان ۱۳۹۵

چاپخانه: معین

قیمت: ۱۲۰۰۰ تومان

شابک: ۹۷۸-۶۰۰-۹۶۸۹۴-۲-۲

نمایندگی فروش: مشهد- خیابان سعدی- بازارچه کتاب- شماره ۲۵- کتابفروشی درخشش

تلفن: ۰۵۱۳۲۲۵۱۹۲۳

این اثر مشمول قانون حمایت مولفان و مصنفان و هنرمندان است و هرگونه کپی برداری و نشر از تمام یا قسمتی از این اثر بدون اجازه مولف (ناشر) منع شرعی و قانونی داشته و مورد پیگرد قانونی قرار خواهد گرفت.

مقدمه مؤلف

کتاب حاضر، حاصل بیش از ۸ سال تحقیق و مطالعه بر روی شبکه‌های موردی می‌باشد. این کتاب براساس تحقیقات صورت گرفته از مقالات و کتاب‌ها و مطالعه موردی صورت گرفته مؤلف و شبیه سازی شبکه، ای مختلف و بررسی شبکه‌ها از جنبه‌های مختلف می‌باشد. این کتاب در چهار فصل به تشریح شبکه وردی، الگوریتم‌های مسیریابی، مخاطرات و امنیت آن، انرژی و پیاده سازی کاربردی شبکه‌های موردی می‌پردازد.

پیاده سازی حملات و رشک در وضعیت‌های مختلف و شبیه سازی آن به کمک شبیه ساز قدرتمند آپ نت کمک بزرگی برای دانشجویان در مقاطع تحصیلات تکمیلی می‌باشد.

افراد زیادی برای آماده سازی این کتاب زحمت کشیده اند و به طور ویژه خانم مهندس حکیمی فر، از همه آنها تشکر می‌نمایم. همچنین از تمامی هم اساتید گرانقدرمان در دانشگاه علم و صنعت ایران تشکر و قدردانی می‌کنیم.

در پایان از شما خواننده گرامی تقاضا می‌کنم در صورت مشاهده هر گونه اشکال و یا داشتن هر گونه پیشنهاد و یا انتقاد اینجانب را مطلع سازید.

ان آقائی - مصطفی اخوان صفار

آذرماه ۱۳۹۵

m.aghaei@pnu.ac.ir
akhavansaffar@pnu.ac.ir

فهرست مطالب

۵	 مقدمه مؤلف
۲۳	 فصل اول: معرفی شبکه‌های موردی
۲۳	 ۱. معرفی شبکه موردی
۲۳	 ۱.۱. مقدمه
۲۴	 ۱.۲. شبکه‌های سیستم
۲۵	 ۱.۲.۱. شبکه بدون سیم
۲۵	 ۱.۳. شبکه‌های موردی سیم
۲۶	 ۱.۴. چرا شبکه‌های موردی؟
۲۷	 ۱.۵. کاربردهای شبکه موردی
۲۷	 ۱.۵.۱. شبکه‌های شخصی
۲۷	 ۱.۵.۲. محیط‌های نظامی
۲۷	 ۱.۵.۳. محیط‌های غیرنظامی
۲۷	 ۱.۵.۴. عملکردهای فوری
۲۸	 ۱.۵.۵. محیط‌های علمی
۲۸	 ۱.۶. ویژگی‌های شبکه‌های سیم موردی
۲۹	 ۱.۷. چالش‌های موجود در شبکه‌های سیم موردی
۳۰	 ۱.۷.۱. مدیریت انرژی
۳۰	 ۱.۷.۲. مقیاس‌پذیری شبکه
۳۰	 ۱.۷.۳. مسیریابی
۳۱	 ۱.۷.۴. کنترل ترافیک
۳۱	 ۱.۷.۵. امنیت

۳۱	۱.۸ وضعیت مسیریابی در شبکه موردی سیار
۳۲	۱.۹ مدل‌های حرکتی در شبکه‌های موردی
۳۳	۱.۹.۱ مدل حرکتی پروتین
۳۴	۱.۹.۲ مدل ستونی
۳۵	۱.۹.۳ مدل تعقیب
۳۶	۱.۹.۴ مدل راه‌رفتن تصادفی
۳۷	۱.۹.۵ مدل حرکت تصادفی نقطه راه
۳۸	۱.۹.۶ مدل تصادفی گگوس-مارکف
۳۸	۱.۹.۷ مدل بردار حرکتی
۴۰	۱.۹.۸ مسیرهای جغرافیایی
۴۰	۱.۹.۸.۱ مکان‌های دور
۴۰	۱.۹.۸.۲ اجتماع
۴۱	۱.۹.۸.۳ مدل حرکتی تصادفی هم‌ا

۴۳	فصل دوم: مسیریابی در شبکه ادهاک
۴۳	۲.۱ معرفی
۴۳	۲.۲ مقدمه
۴۴	۲.۳ دسته‌بندی پروتکل‌های مسیریابی
۴۴	۲.۳.۱ آگاهی
۴۵	۲.۳.۲ تک‌پخش
۴۵	۲.۳.۳ چندپخش
۴۶	۲.۴ مسیریابی
۴۷	۲.۴.۱ پروتکل‌های مسیریابی بردار فاصله
۴۸	۲.۴.۲ پروتکل‌های مسیریابی مبتنی بر حالت اتصال
۴۸	۲.۴.۳ پروتکل‌های تک سطحی مبتنی بر جدول
۴۹	۲.۴.۴ پروتکل مسیریابی DSDV
۴۹	۲.۴.۵ پروتکل OLSR

۵۰	 پروتکل های تک سطحی مبتنی بر تقاضا
۵۱	 AODV پروتکل
۵۱	 SAODV پروتکل
۵۳	 ۲.۴.۸.۱ خصوصیات امنیتی
۵۴	 ۲.۴.۸.۲ پیاده سازی
۵۵	 ۲.۴.۸.۳ توسعه تک امضایی RREQ
۵۷	 ۲.۴.۸.۴ توسعه تک امضایی RREP
۵۷	 ۲.۴.۸.۵ توسعه دو امضایی RREQ
۵۹	 ۲.۴.۸.۶ توسعه دو امضایی RREP
۶۰	 ۲.۴.۸.۷ توسعه امضاء RRER
۶۰	 ۲.۴.۸.۸ توسعه امضاء RREP-ACK
۶۱	 ۲.۴.۸.۹ امنیت AODV
۶۱	 امضاءهای SAODV
۶۳	 ۲.۴.۸.۱۰ زنجیره های داده ساز SAODV
۶۴	 ۲.۴.۸.۱۱ سازگاریهای مورد نیاز با IEEE 802.11
۶۵	 ۲.۴.۸.۱۲ ملاحظات امنیتی
۶۶	 ۲.۴.۸.۱۳ بررسی کاربرد پروتکل مسیریابی امنیتی SAODV در قیاس با AODV
۶۶	 ۲.۴.۸.۱۳.۱ AODV
۶۷	 ۲.۴.۸.۱۳.۲ AODV و امنیت
۶۷	 ۲.۴.۸.۱۳.۳ AODV: حمله "فرد میانی" (۱) - شکل ۲-۸
۶۸	 ۲.۴.۸.۱۳.۴ AODV: حمله "فرد میانی" (۲) - شکل ۲-۹
۶۸	 SAODV
۶۹	 SAODV سازگار
۷۰	 ۲.۵ مدیر کلید A-SAODV
۷۱	 نمایش تجربی A-SAODV
۷۱	 ۲.۵.۱ معضلات AODV و راه حل ها
۷۴	 ۲.۶ پروتکل DSR

۷۵	۲.۶.۱ جزئیات عملکرد DSR
۷۵	۲.۶.۲ مشخصات مهم پروتکل DSR
۷۶	۲.۶.۳ کشف مسیر
۸۰	۲.۶.۳.۱ نگهداری از مسیر
۸۰	۲.۶.۳.۲ خلاصه
۸۱	۲.۷ پروتکل‌های تک سطحی ترکیبی
۸۱	۲.۷.۱ پروتکل مسیریابی ZRP
۸۱	۲.۷.۱.۱ پروتکل‌های سلسله مراتبی ترکیبی
۸۲	۲.۷.۱.۲ پروتکل مسیریابی CBRP
۸۴	۲.۷.۱.۳ الگوریتم تشکین خوشه پروتکل CBRP
۸۵	۲.۷.۱.۴ مثال: رنج کشف مسیر در پروتکل CBRP
۸۷	۲.۷.۱.۵ مقایسه بین پروتکل‌های تک سطحی و سلسله مراتبی
۸۹	۲.۷.۱.۶ مسیریابی بردار فاصله
۹۰	۲.۷.۱.۷ مسیریابی حالت اتصال
۹۰	۲.۷.۱.۸ مسیریابی مبدأ
۹۱	۲.۷.۲ اهداف مسیریابی
۹۲	۲.۷.۳ معیارهای تعیین مسیر بهینه
۹۲	۲.۷.۴ معیارهای مهم مسیریابی در شبکه‌های ادماک
۹۷	فصل سوم: امنیت در شبکه‌های موردی
۹۸	۳.۱ تهدیدات
۹۸	۳.۱.۱ دشمن آمانور
۹۸	۳.۱.۲ دشمن حرفه‌ای
۹۸	۳.۱.۳ دشمن با پشتوانه مالی
۹۸	۳.۲ آسیب پذیری
۱۰۰	۳.۳ حملات مسیریابی
۱۰۰	۳.۳.۱ حملات غیرفعال

۱۰۰	۳.۳.۲ حملات فعال
۱۰۱	۳.۳.۲.۱ فقدان خواب
۱۰۱	۳.۳.۲.۲ فاش سازی موقعیت
۱۰۱	۳.۳.۲.۳ اسنراق سمع
۱۰۱	۳.۳.۲.۴ آنالیز ترافیک
۱۰۲	۳.۳.۲.۵ حمله ممانعت از سرویس
۱۰۲	۳.۳.۳ توضیحات کلی درباره حملات ممکن بر روی مسیریابی‌ها در شبکه موردی
۱۰۲	۳.۳.۳ حمله حفره تاریک
۱۰۲	۳.۳.۳ جعل هویت
۱۰۳	۳.۳.۳.۱ دستکاری بسته‌های مسیریابی در هنگام عبور
۱۰۳	۳.۳.۳.۲ رریخ بسته‌ها
۱۰۳	۳.۳.۳.۳ حفره تاریک
۱۰۴	۳.۳.۳.۴ حمله سواخ رمی
۱۰۴	۳.۳.۳.۵ حمله هجومی
۱۰۵	۳.۴ راه‌حل‌های امنیتی در شبکه‌های کامپیوتری
۱۰۹	۳.۵ تشخیص نفوذ
۱۰۹	۳.۵.۱ پیش‌گیری از نفوذ
۱۱۰	۳.۵.۲ راه‌حل‌های امنیتی در شبکه‌های Ad hoc
۱۱۲	۳.۵.۳ مسیریابی امن
۱۱۳	۳.۶ سیستم‌های تشخیص نفوذ در شبکه موردی
۱۱۴	۳.۶.۱ سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری
۱۱۵	۳.۶.۲ سیستم‌های تشخیص نفوذ مبتنی بر امضا یا دانش
۱۱۵	۳.۶.۳ تشخیص رفتارهای ناهنجار بر مبنای مشخصه‌ها
۱۱۶	۳.۶.۴ کنترل فرآیندهای استاتیکی برای تشخیص حملات کامپیوتری
۱۱۶	۳.۶.۵ روش پاسخ‌گویی آنی به حملات مسیریابی
۱۱۷	۳.۶.۶ تشخیص نفوذ در شبکه‌های موردی
۱۱۸	۳.۶.۷ استفاده از سنگ نگهبان و مسیر سنج

۱۱۸	۳.۶.۸ سابقه تحقیق در رابطه با سیستم‌های تشخیص نفوذ.....
۱۲۰	۳.۷ طراحی یک سیستم تشخیص نفوذ پیشنهادی و دلخواه بر اساس پارامترهای شبکه و انتخاب ویژگی.....
۱۲۱	۳.۷.۱ بخش اول: واحد شنود.....
۱۲۳	۳.۷.۲ بخش دوم واحد تشخیص نفوذ.....
۱۲۳	۳.۷.۳ تئوری تحلیل مولفه‌های اصلی.....

فصل چهارم: شبیه‌سازی..... ۱۲۵

۱۲۵	۴.۱ مقایسه‌ای بر نرم افزارهای شبیه ساز شبکه.....
۱۲۵	۴.۱.۱ شبیه ساز شبکه NS.....
۱۲۵	۴.۱.۱.۱ مقایسه.....
۱۲۵	۴.۱.۱.۲ مقایسه.....
۱۲۹	۴.۱.۱.۳ مقایسه شبیه سازی به ساز NS.....
۱۲۹	۴.۱.۱.۴ Otel زبانی برای کاربر.....
۱۳۳	۴.۱.۱.۵ مثال ساده از شبیه سازی.....
۱۳۹	۴.۱.۱.۶ زمانبند رویداد.....
۱۴۱	۴.۱.۱.۷ اجرای شبکه.....
۱۴۶	۴-۸-۵ بسته.....
۱۴۷	۴.۱.۱.۸ بعد از شبیه سازی.....
۱۵۰	۴.۱.۱.۹ توسعه NS.....
۱۵۲	۴.۱.۱.۱۰ اتصال Otel.....
۱۵۴	۴.۱.۱.۱۱ صدور دره‌های C++ به Otel.....
۱۵۵	۴.۱.۱.۱۲ صدور متغیرهای رده C++ به OTCL.....
۱۵۶	۴.۱.۱.۱۳ صدور فرمان‌های کنترلی شیء C++ به OTCL.....
۱۵۶	۴.۱.۱.۱۴ اجرای یک فرمان Otel از درون برنامه C++.....
۱۵۷	۴.۱.۲ آرایه چند مثال.....
۱۵۷	۴.۱.۲.۱ شبکه محلی (LAN).....
۱۵۸	۴.۱.۲.۲ بخش چندتایی (Multicast).....

۱۶۰	 Web ۴.۱.۲.۳ سرویس دهنده
۱۶۲	 ۴.۱.۳ نرم افزار شبیه ساز OPNET
۱۶۲	 ۴.۱.۳.۱ مقدمه
۱۶۴	 ۴.۱.۳.۲ کاربردهای OPNET
۱۶۵	 ۴.۱.۳.۳ ادیتور OPNET و لایه های موجود در آن
۱۶۵	 ۴.۱.۳.۳.۱ لایه شبکه
۱۶۶	 ۴.۱.۳.۳.۲ لایه گره
۱۶۷	 ۴.۱.۳.۳.۳ لایه فرایند
۱۶۸	 ۴.۱.۳.۴ ساختار سلسله مراتبی در شبیه ساز OPNET
۱۶۹	 ۴.۱.۳.۴.۱ (Network editor یا Project editor) ویرایشگر شبکه
۱۷۳	 ۴.۱.۳.۴.۲ Object palette پنجره
۱۷۴	 ۴.۱.۳.۴.۳ رسم و انتخاب شبکه در محیط ویرایشگر شبکه
۱۷۵	 ۴.۱.۳.۴.۵ مشخص کردن پارامترهای مورد نظر برای اجرای شبیه سازی
۱۷۶	 ۴.۱.۳.۵ ویرایشگر Node
۱۷۸	 ۴.۱.۳.۵.۱ انواع مازول ها در ویرایشگر Node
۱۸۰	 ۴.۱.۳.۵.۲ منوهای مختلف در ویرایشگر Node
۱۸۲	 ۴.۱.۳.۵.۳ ویرایشگر Process
۱۸۳	 ۴.۱.۳.۵.۴ حالات موجود در دیاگرام STD
۱۸۴	 ۴.۱.۳.۵.۶ بررسی منوهای موجود در ویرایشگر Process
۱۸۴	 ۴.۱.۳.۵.۷ توابع تعریف شده در Porto-C
۱۸۵	 ۴.۱.۳.۵.۸ برخی از مهمترین گروه های KP
۱۸۶	 ۴.۱.۳.۵.۹ ویرایشگر انتشار آنتن (Antenna Pattern Editor)
۱۸۸	 ۴.۱.۳.۵.۱۰ ویرایشگر فرمت بسته (Packet Format Editor)
۱۸۸	 ۴-۵-۱ عملیات ویرایشگر فرمت پکت
۱۸۹	 ۴.۱.۴ مشاهده و تحلیل نتایج شبیه سازی
۱۹۰	 ۴.۲ شبیه سازی سیستم تشخیص نفوذ
۱۹۱	 ۴.۲.۱ نرم افزار Opnet

۱۹۳	 پیاده‌سازی ۴.۲.۲
۱۹۵	 نحوه پایش مشخصه‌ها ۴.۲.۳
۱۹۹	 ۴.۲.۳.۱ آزمایش اول، آزمون شبکه در حالت عادی است
۱۹۹	 ۴.۲.۳.۲ آزمایش دوم، پیاده‌سازی حمله DoS نوع اول
۱۹۹	 ۴.۲.۳.۳ آزمایش سوم، پیاده‌سازی حمله DoS نوع دوم
۲۰۰	 ۴.۲.۳.۴ آزمایش چهارم، پیاده‌سازی حمله DDoS
۲۰۰	 ۴.۲.۳.۵ آزمایش پنجم، پیاده‌سازی حملهای با طول بسته زمانی زیاد
۲۰۰	 ۴.۲.۱ آزمایش ششم، پیاده‌سازی یکی از ضعف‌های سیستم
۲۰۱	 ۴.۲.۱ تحلیل آزمایش‌های این بخش
۲۰۱	 ۴.۲.۳.۱ سناریو ۱ پیاده‌سازی شبکه در ۸ حالت عادی
۲۰۲	 ۴.۲.۳.۲ سناریو ۲ پیاده‌سازی حمله DOS نوع دوم در وضعیت‌های متفاوت شبکه
۲۰۳	 ۴.۲.۳.۳ سناریو ۳ پیاده‌سازی حمله DOS نوع دوم در وضعیت‌های متفاوت شبکه
۲۰۶	 ۴.۲.۳.۴ سناریو چهارم پیاده‌سازی حملات مختلف
۲۰۶	 ۴.۲.۴ طراحی سیستم تشخیص نفوذ بر اساس خوشه‌بندی و طبقه‌بندی
۲۰۷	 ۴.۲.۵ خوشه‌بندی
۲۰۸	 ۴.۲.۶ طبقه‌بندی
۲۰۹	 ۴.۲.۷ K-امین نزدیکترین همسایه
۲۱۰	 ۴.۲.۸ پردازش داده‌ها توسط الگوریتمهای طبقه‌بندی و خوشه‌بندی
۲۱۱	 ۴.۲.۹ پیش پردازش
۲۱۲	 ۴.۲.۱۰ ماتریس ضرایب
۲۱۳	 ۴.۲.۱۰.۱ نرخ True Positive
۲۱۳	 ۴.۲.۱۰.۲ نرخ False Positive
۲۱۹	 ۴.۲.۱۱ ارزیابی خروجی K-امین نزدیکترین همسایه و K-تا میانگین
۲۲۰	 ۴.۲.۱۲ سناریو اول
۲۲۲	 ۴.۲.۱۳ سناریو دوم
۲۲۳	 ۴.۲.۱۴ سناریو سوم
۲۲۶	 ۴.۲.۱۵ سناریو چهارم

۲۲۷	 ۴.۲.۱۶ ستاریو پنجم
۲۳۰	 ۴.۲.۱۷ خلاصه
۲۳۳	 مراجع

www.ketab.ir