

مرجع کامل

تکنولوژی بلوتوث و امنیت در آن

شامل مباحث

ساختار رادیویی

معماری بلوتوث

مکانیسم‌های امنیتی

انواع حملات و ضعف‌های امنیتی

راه‌های مقابله با حملات و افزایش امنیت

پایاده سازی پروتکل‌های امنیتی در اینترنت بلوتوث

آموزش روش‌های شبیه سازی شبکه بلوتوث

مؤلف:

مصطفی اخوان صفار

(عضو هیأت علمی دانشگاه پیام نور)

سرشناسه	:	اخوان صفار، مصطفی، ۱۳۶۱-
عنوان و نام پدیدآور	:	مرجع کامل تکنولوژی بلوتوث و امنیت در آن شامل مباحث: ساختار رادیویی.../
مؤلف: مصطفی اخوان صفار.		
مشخصات نشر	:	مشهد: خط اول، ۱۳۹۴
مشخصات ظاهری	:	۳۷۲ ص: مصور (بخش رنگی)، نمودار (بخش رنگی)
شابک	:	978-600-95208-6-2
وضعیت فهرست‌نویسی	:	فیا
یادداشت	:	کتابنامه: ص. [۳۷۱] - ۳۷۲.
موضوع	:	تکنولوژی بلوتوث
موضوع	:	ارتباطات بی‌سیم -- تدابیر ایمنی
ردیف کتبی	:	۱۳۹۴ م ۳ الف ۳/۲ TK5۱۰۲
رده‌بندی دیوینی	:	۰۰۴/۶۲
شماره کتابشناسی ملی	:	۴۱۳۴۴۲۴



تلفن: ۰۵۱۳۷۵۲۹۹۹۳

www.khate-aval.com

info@khate-aval.com

نام ناشر: انتشارات خط اول

نام کتاب: مرجع کامل تکنولوژی بلوتوث و امنیت در آن

مؤلف: مصطفی اخوان صفار

صفحه‌آرا: نفیسه اسماعیلی

شمارگان: ۱۰۰۰ جلد

نوبت چاپ: اول / زمستان ۱۳۹۴

چاپخانه: معین

قیمت: ۲۴۵۰۰ تومان

شابک: ۹۷۸-۶۰۰-۹۵۲۰۸-۶-۲

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.

چکیده

بلوتوث نوعی از ارتباطات امواج رادیویی ولی با برد کوتاه است و از پروتکل خاصی برای ارسال اطلاعات خود استفاده می‌کند و به همین دلیل است که شرکت‌های معتبر سازنده دستگاه‌های ارتباطی و کامپیوتری علاقه زیادی دارند تا در از آن استفاده کنند. عوامل بسیاری موجب شده تا شرکت‌ها و موسسات ارتباطی به دنبال استفاده از بلوتوث باشند. یکی از این عوامل محدودیت در انتقال داده از طریق سیم است. در واقع بلوتوث یک ابزار صنعتی برای اتصال از نوع بی سیم به شبکه‌های محلی و جهانی است. از جمله کاربردها می‌توان به موارد زیر اشاره کرد: ایجاد یک شبکه بیسیم برای کامپیوترهای رومیزی با یک پهنای باند که یک استفاده در تجهیزاتی مثل پرینتر، میکروفن، کیبرد، موس، بلوتوث فروش زیادی در تلفنهای سلولی داشته است که آنها را قادر ساخته که به کامپیوترها و PDAs و هندفری‌ها و بسیاری دیگر از دستگاهها متصل شوند و به این ترتیب یک شبکه بیسیم LAN را ایجاد می‌کنند، انتقال فایلها (مثل عکس و mp3 و غیره، بین گوشی‌های موبایل و PDAs و کامپیوترها از طریق OBEX، handset، بلوتوث برای گوشی موبایل و si. air. n. one، دستگاههای اندازه گیری و تست، ابزارهای پزشکی، گیرنده‌های GPS، اتومبیل و استفاده بعنوان هندفری تلفن در آن، کنترل از راه دور تلویزیون بجای اینفرارد، وسایل کمک شنوایی، پلی استیشن و Nintendo Revolution و.. با تمام مزبتهای و استفاده‌های متعدد و روزافزون از این تکنولوژی عدم توجه به اشکالات امنیتی که در آن وجود دارد می‌تواند صدمات جبران ناپذیری را وارد کند. اما کتابی جامع در مورد این تکنولوژی و مباحث امنیتی در آن تا کنون گردآوری نشده است. که هدف از نگارش این کتاب بررسی جامع این تکنولوژی، مسائل امنیتی و حملات موجود در آن می‌باشد. امید است که بتواند بعنوان یک مرجع آموزشی کامل و جامع نیاز دانش پژوهان و پژوهشگران را مرتفع سازد.

فهرست مطالب

۲۷.....	فصل اول: معرفی بلوتوث
۲۸.....	۱-۱ مقدمه
۳۰.....	۲-۱ تاریخچه
۳۱.....	۳-۱ کاربردهای بلوتوث
۳۲.....	۴-۱ خصوصیات بلوتوث
۳۴.....	۵-۱ طیف گسترده
۳۵.....	گسترش
۳۶.....	۶-۱ پرسش‌های فرکانسی
۳۶.....	۷-۱ ماهیت TDD
۳۹.....	فصل دوم: بسته‌ها و کانال‌های ارتباطی
۴۰.....	۱-۲ مشخصات کلی بلوتوث
۴۲.....	۲-۲ کانالهای فیزیکی
۴۳.....	۳-۲ ارتباطهای فیزیکی
۴۳.....	بسته‌های اطلاعات
۴۴.....	کد دسترسی
۴۶.....	۴-۲ preamble
۴۶.....	۵-۲ Sync Word
۴۷.....	۶-۲ Trailer
۴۷.....	۷-۲ فیلد هدر
۴۸.....	۸-۲ نوع بسته‌های اطلاعات
۴۹.....	۹-۲ محموله‌های بلوتوث

۱۰-۲.....فیلدهای صوتی.....۵۰

۱۱-۲.....فیلدهای داده.....۵۰

فصل سوم: معماری بلوتوث.....۵۳

۱-۳.....توپولوژی بلوتوث.....۵۴

۲-۳.....پیکونت.....۵۴

۳-۳.....اسکرت.....۵۵

۴-۳.....ایمپار پروتکل بلوتوث.....۵۶

۵-۱.....سته پروتکل های بلوتوث.....۵۹

۶-۳.....داده های.....۵۹

۷-۳.....پروتکل مدیریت اتصال.....۶۰

۸-۳.....پروتکل انتقال داده های منطقی و پردازش.....۶۰

۹-۳.....پروتکل سرویس.....۶۰

۱۰-۳.....پروتکل جایگزینی سابل.....۶۱

۱۱-۳.....پروتکل کنترل تلفنی.....۶۱

۱۲-۳.....پروتکل های الحاقی.....۶۱

۱۳-۳.....پروفایلها (پروتکل و مدل های قابل استفاده در بلوتوث).....۶۲

۱۴-۳.....ارسال فایل.....۶۳

۱۵-۳.....اتصال اینترنت.....۶۳

۱۶-۳.....همزمانی.....۶۴

۱۷-۳.....دسترسی به LAN.....۶۴

۱۸-۳.....تلفن سه کاره.....۶۵

۱۹-۳.....هدفن دوردست.....۶۶

فصل چهارم: امنیت در بلوتوث.....۶۷

۱-۴.....توضیحات کلی.....۶۸

۲-۴.....اصول رمزنگاری.....۶۹

۷۱.....	۳-۴ کلید اتصال
۷۲.....	۴-۴ کلید مقدار دهی اولیه
۷۳.....	۵-۴ کلید ترکیبی (مرب)
۷۴.....	۶-۴ کلید واحد
۷۵.....	۷-۴ کلید مستر
۷۶.....	۸-۴ کلید رمزگزاری
۷۷.....	۹-۴ تصدیق هویت
۷۸.....	۱۰-۴ رمزنگاری
۸۰.....	۱۱-۴ مدیر امنیت

۸۱..... فصل پنجم: نقطه ضعفهای امنیتی ۱. بلوتوث و معرفی حملات

۸۶.....	۱-۵ طبقه بندی حملات
۸۸.....	۲-۵ آسیب پذیری در پروتکل تصدیق هویت پیرینگ
۸۸.....	۱-۲-۵ زوج سازی
۹۲.....	۲-۲-۵ تصدیق هویت
۹۵.....	۳-۵ حملات ناشی از نقص در طراحی پروتکل بلوتوث
۹۵.....	۱-۳-۵ حمله پین کد
۹۹.....	۲-۳-۵ حملات کلید واحد
۱۰۲.....	۳-۳-۵ حملات کلید مستر
۱۰۲.....	۴-۳-۵ حملات رد سرویس
۱۰۳.....	۵-۳-۵ حملات رمز
۱۰۸.....	۶-۳-۵ شکستن آفلاین پین
۱۱۰.....	۷-۳-۵ حمله Relay
۱۱۲.....	۸-۳-۵ جعل هویت دستگاه
۱۱۴.....	۹-۳-۵ حملات رد سرویس در تصدیق هویت و زوج سازی
۱۱۶.....	۱۰-۳-۵ حمله مرد میانی
۱۱۸.....	۴-۵ حملات ناشی از نقص در پیکره بندی ضعیف پروتکل بلوتوث

- ۱۱۸..... ۱-۴-۵ بلواسنارفینگ
- ۱۲۱..... ۲-۴-۵ حمله بلویاگینگ
- ۱۲۳..... ۳-۴-۵ Bluejacking حمله
- ۱۲۶..... ۴-۴-۵ حمله ربایش جانبی
- ۱۲۶..... ۵-۴-۵ حمله ربایش جانبی معکوس
- ۱۲۷..... ۶-۴-۵ شکستن بین آنلاین
- ۱۲۹..... ۷-۴-۵ شکستن بین آنلاین نسخه ۲
- ۱۳۰..... ۸-۴-۵ شکستن بین آفلاین-آنلاین
- ۱۳۲..... ۹-۴-۵ استراق سمع و جعل هویت
- ۱۳۴..... ۱۰-۴-۵ مکان یابی
- ۱۳۶..... ۱-۴-۵ Hopping along
- ۱۳۷..... ۱۲-۴-۵ حمله
- ۱۳۷..... ۱۳-۴-۵ حملات
- ۱۳۸..... ۱۴-۴-۵ مسئله محلی کردن و نه اشت شبکه
- ۱۳۸..... ۱۵-۴-۵ مد غیر قابل کشف
- ۱۳۹..... ۱۶-۴-۵ تحلیل مولد تصادفی
- ۱۳۹..... ۱۷-۴-۵ مشکل وسایل مسروقه/فروخته شده
- ۱۴۰..... ۱۸-۴-۵ ویروسها و کرمهای بلوتوث
- ۱۴۷..... ۵-۵ دیگر مشکلات امنیتی

فصل ششم: راههای مقابله با حملات

- ۱۴۹..... ۱-۶ مقابله با حملات ناشی از پیاده سازی ضعیف
- ۱۵۰..... ۱-۱-۶ بین کد طولانی
- ۱۵۱..... ۲-۱-۶ محافظت از کلیدهای واحد
- ۱۵۱..... ۳-۱-۶ امنیت لایه کاربرد
- ۱۵۱..... ۴-۱-۶ روشهای محافظت در مقابل حملات شخصی میانی
- ۱۵۲..... ۵-۱-۶ حفاظت فیزیکی

- ۶-۱-۶ استفاده از نام مستعار برای مقابله با حملات مکان یابی CAC..... ۱۵۲
- ۶-۱-۷ رمز..... ۱۵۲
- ۶-۱-۸ مقابله با ویروسها و کرم‌ها در بلوتوث..... ۱۵۲
- ۶-۲ مقابله با حملات ناشی از طراحی پروتکل بلوتوث..... ۱۵۳
- ۶-۳ استفاده از پروتکل‌های رمزنگاری تبادل کلید امن..... ۱۵۴
- ۶-۲-۱ پروتکل تبادل کلید نمایی پسورد ساده..... ۱۵۵
- ۶-۲-۲ پروتکل ایستگاه به ایستگاه (STS)..... ۱۵۶
- ۶-۲-۳ ام‌اند‌ای ایستگاه به ایستگاه..... ۱۵۶
- ۶-۲-۴ اس‌ان کار ایستگاه به ایستگاه..... ۱۵۷
- ۶-۲-۵ تصدیق هویت تنها با STS..... ۱۵۷
- ۶-۲-۶ پروتکل STS-MAC..... ۱۵۸
- ۶-۲-۲ جلویی از حملات با استفاده از STS-MAC و SPEKE..... ۱۵۹
- ۶-۲-۳ جلویی از حمله مرد میانه..... ۱۶۵
- ۶-۲-۱ اضافه کردن یک پنجره سفر در سطح رابط کاربر..... ۱۶۶
- ۶-۲-۲ الزام استفاده از یک کانال اوج در پروتکل زوج سازی بلوتوث..... ۱۶۶
- ۶-۳ استفاده از تکنیک‌های Anti-jamming..... ۱۶۶
- ۶-۴ استفاده از پروتکل‌های تبادل کلید امن..... ۱۶۸

فصل هفتم: پیاده‌سازی برخی مکانیزم‌های امنیتی ارائه شده..... ۱۷۳

- ۷-۱ پیاده سازی از طریق برنامه نویسی..... ۱۷۴
- ۷-۱-۱ تحلیل زمانی اثرپذیری برخی حملات..... ۱۷۷
- ۷-۲-۱ نقطه ضعف‌های انتخاب پین کد..... ۱۸۰
- ۷-۳-۱ حمله شکستن پین آنلاین..... ۱۸۱
- ۷-۴-۱ حمله جعل هویت و relay..... ۱۸۱
- ۷-۲ پیاده سازی نرم افزاری..... ۱۸۲

فصل هشتم: روش‌های شبیه‌سازی شبکه بلوتوث.....	۱۹۱
۸-۱ مقدمه بر شبکه بلوتوث.....	۱۹۲
۸-۲ پروتکل استک بلوتوث.....	۱۹۲
۸-۲-۱ پروتکل باند پایه.....	۱۹۳
۸-۲-۲ پروتکل پروتکل کنترل اتصالات منطقی و پردازش (L2CAP).....	۱۹۳
۸-۲-۳ پروتکل مدیریت اتصال (LMP).....	۱۹۴
۸-۳ فرکانس‌های مورد استفاده در بلوتوث.....	۱۹۴
۸-۴ پرش‌های فرکانسی.....	۱۹۵
۸-۵ بسته‌های اطلاعات.....	۱۹۸
۸-۵-۱ دستور.....	۱۹۹
۸-۵-۲ پیلد preamble.....	۲۰۰
۸-۵-۳ پیلد Sync.....	۲۰۱
۸-۵-۴ پیلد Trailer.....	۲۰۱
۸-۵-۵ پیلد هدر.....	۲۰۱
۸-۵-۶ نوع بسته‌های اطلاعات.....	۲۰۳
۸-۶ محموله‌های بلوتوث.....	۲۰۴
۸-۶-۱ پیلدهای صوتی.....	۲۰۴
۸-۶-۲ پیلدهای داده.....	۲۰۴
۸-۷ کنترل خطا در بلوتوث.....	۲۰۶
۸-۸ شبیه‌سازی شبکه NS.....	۲۰۷
۸-۸-۱ مقدمه.....	۲۰۷
۸-۸-۲ نمای کلی.....	۲۰۷
۸-۸-۳ مبانی کلیدی شبیه‌سازی NS.....	۲۱۱
۸-۸-۳-۱ Otel زبانی برای کاربر.....	۲۱۱
۸-۸-۳-۲ مثالی ساده از شبیه‌سازی.....	۲۱۴
۸-۸-۳ زمانبند رویداد.....	۲۱۹
۸-۸-۴ اجزای شبکه.....	۲۲۲

۲۲۶.....	۸-۸-۵ بسته
۲۲۷.....	۸-۸-۶ بعد از شبیه سازی
۲۲۷.....	۸-۸-۱۰ مثالی از تحلیل ردیابی
۲۳۰.....	۸-۸-۷ توسعه NS
۲۳۰.....	۸-۸-۱۰ در کجا بدنال چه چیزی باشیم؟
۲۳۲.....	۸-۸-۷-۲ اتصال Otcl
۲۳۴.....	۸-۸-۷-۳ صدور دره های C++ به Otcl
۲۳۵.....	۸-۸-۷-۴ صدور متغیرهای رده C++ به OTCL
۲۳۵.....	۸-۸-۵۰ در فرمان های کنترلی شیء C++ به OTCL
۲۳۶.....	۸-۸-۷-۵ اجرای یک فرمان Otcl از درون برنامه C++
۲۳۷.....	۸-۸-۷-۸ ارائه چند مثال
۲۳۷.....	۸-۸-۷-۱ شبکه محلی (LAN)
۲۳۷.....	۸-۸-۷-۲ پخش چندتایی (Multicast)
۲۴۰.....	۸-۸-۷-۳ سرویس دهنده Web
۲۴۲.....	۸-۹-۱ شبیه سازی شبکه بلوتوث با استفاده از BlueHoc
۲۴۳.....	۸-۹-۱ مقدمه
۲۴۳.....	۸-۹-۲ مدل شبیه ساز BlueHoc
۲۴۵.....	۸-۹-۳ شبیه سازی لایه های بلوتوث در BlueHoc
۲۴۶.....	۸-۹-۴ شبیه سازی حالات بلوتوث
۲۴۷.....	۸-۹-۵ انواع بسته های BlueHoc
۲۴۸.....	۸-۹-۶ سرآیند بسته های BlueHoc
۲۴۸.....	۸-۹-۷ شبیه سازی باند پایه در BlueHoc
۲۴۸.....	۸-۹-۸ شبیه سازی زمانبند در BlueHoc
۲۴۸.....	۸-۹-۹ شبیه سازی L2CAP در BlueHoc
۲۴۹.....	۸-۹-۱۰ اضافه نمودن کلاس های C++ در NS برای شبیه سازی بلوتوث
۲۵۱.....	۸-۹-۱۱ شبیه سازی صفحه بندی و کشف دستگاه
۲۵۲.....	۸-۹-۱۲ برقراری ارتباط در BlueHoc

- ۲۵۲..... ۱۳-۹-۸ سیگنالینگ LMP
- ۲۵۲..... ۱۴-۹-۸ برقراری ارتباط L2CAP
- ۲۵۳..... ۱۵-۹-۸ نگاشت QoS
- ۲۵۴..... ۱۶-۹-۸ شبیه سازی پروتکل انطباق و کنترل لینک منطقی در BlueHoc
- ۲۵۵..... ۱۷-۹-۸ استفاده از شبیه ساز TCP/IP در NS
- ۲۵۷..... ۱۸-۹-۸ آموزش دانلود و نصب BlueHoc
- ۲۵۸..... ۱۹-۹-۸ واسط گرافیکی
- ۲۵۹..... ۲۰-۹-۸ پیکره بندی برنامه شبیه ساز
- ۲۶۱..... ۲۱-۹-۸ پشتیبانی از Trace
- ۲۶۵..... ۲۲-۹-۸ نمونه یک شبکه از شبیه سازی و توضیحات
- ۲۶۹..... ۲۳-۹-۸ جریان بسته های مثال فوق
- ۲۷۱..... ۱۰-۸ شبیه سازی و ارتباطات پورت سریال
- ۲۷۱..... ۱-۱۰-۸ مقدمه ای بر برنامه نویسی پورت سریال در C#
- ۲۷۵..... ۲-۱۰-۸ نوشتن برنامه بر روی پورت سریال
- ۲۷۵..... ۳-۱۰-۸ دریافت از پورت سریال
- ۲۷۸..... ۴-۱۰-۸ کتابخانه Franson Bluetooth، برنامه نویسی C#
- ۲۷۹..... ۱-۴-۱۰-۸ انواع کلاس ها
- ۲۸۶..... ۲-۴-۱۰-۸ رویدادهای Delegate
- ۲۸۶..... ۳-۴-۱۰-۸ انواع رویدادهای شمارشی
- ۲۹۰..... ۵-۱۰-۸ طراحی یک اپلیکیشن بلوتوث در تلفن همراه با استفاده از برنامه نویسی پورت سریال
- ۲۹۸..... ۱۱-۸ نرم افزار شبیه ساز OPNET
- ۲۹۸..... ۱-۱۱-۸ مقدمه
- ۲۹۹..... ۲-۱۱-۸ کاربردهای OPNET
- ۳۰۰..... ۳-۱۱-۸ ادیتور OPNET و لایه های موجود در آن
- ۳۰۰..... ۱-۳-۱۱-۸ لایه شبکه
- ۳۰۱..... ۲-۳-۱۱-۸ لایه گره
- ۳۰۲..... ۳-۳-۱۱-۸ لایه فرایند

۳۰۳.....	۴-۱۱-۸ ساختار سلسله مراتبی در شبیه ساز OPNET.....
۳۰۴.....	۱-۴-۱۱-۸ ویرایشگر شبکه (Network editor یا Project editor).....
۳۰۸.....	۱-۱-۴-۱۱-۸ پنجره Object palette.....
۳۰۹.....	۲-۱-۴-۱۱-۸ رسم ساختار شبکه در محیط ویرایشگر شبکه.....
۳۱۰.....	۳-۱-۴-۱۱-۸ مشخص کردن پارامترهای مورد نظر برای اجرای شبیه سازی.....
۳۱۱.....	۲-۴-۱۱-۸ ویرایشگر Node.....
۳۱۳.....	۱-۲-۴-۱۱-۸ انواع ماژول‌ها در ویرایشگر Node.....
۳۱۵.....	۲-۲-۴-۱۱-۸ منوهای مختلف در ویرایشگر Node.....
۳۱۷.....	۳-۱-۱۱-۸ ویرایشگر Process.....
۳۱۸.....	۴-۱-۱۱-۸ حالات موجود در دیاگرام STD.....
۳۱۸.....	۵-۴-۱۱-۸ بر روی منوها موجود در ویرایشگر Process.....
۳۱۹.....	۶-۴-۱۱-۸ توابع تعریف شده در Port.....
۳۲۰.....	۱-۶-۴-۱۱-۸ برخی از مهم ترین گره های KP.....
۳۲۱.....	۳-۴-۱۱-۸ ویرایشگر انتشار آنتن (Antenna Pattern Editor).....
۳۲۲.....	۴-۴-۱۱-۸ ویرایشگر فرمت بسته (Packet Format Editor).....
۳۲۳.....	۱-۵-۴ عملیات ویرایشگر فرمت پکت.....
۳۲۳.....	۵-۴-۱۱-۸ مشاهده و تحلیل نتایج شبیه سازی.....
۳۲۴.....	۵-۱۱-۸ انتخاب ابزار شبیه سازی OPNET/BONEs.....
۳۲۵.....	۶-۱۱-۸ تشریح پیاده سازی.....
۳۲۵.....	۱-۶-۱۱-۸ مکان پیاده سازی کد C.....
۳۲۶.....	۲-۶-۱۱-۸ فاز شروع شبیه سازی.....
۳۲۶.....	۱-۲-۶-۱۱-۸ مقدار دهی مستر.....
۳۲۶.....	۲-۲-۶-۱۱-۸ مقداردهی اسلیو.....
۳۲۷.....	۳-۲-۶-۱۱-۸ مقداردهی اغتشاشگر.....
۳۲۷.....	۳-۶-۱۱-۸ وقفه ها.....
۳۲۷.....	۴-۶-۱۱-۸ بروز رسانی آماری.....
۳۲۸.....	۵-۶-۱۱-۸ بررسی اجمالی توابع مفید در شبیه سازی.....

- ۳۲۸..... ۱-۵-۶-۱۱-۸ توابع مفید مستر
- ۳۳۱..... ۲-۵-۶-۱۱-۸ توابع مفید اسلیو
- ۳۳۳..... ۳-۵-۶-۱۱-۸ توابع مفید اغتشاشگر
- ۳۳۴..... ۶-۶-۱۱-۸ محل قرارگیری دستگاه‌ها در شبیه سازی
- ۳۳۴..... ۷-۶-۱۱-۸ تایمرها
- ۳۳۴..... ۸-۶-۱۱-۸ تخصیص منابع
- ۳۳۵..... ۷-۱۱-۸ شبیه سازی
- ۳۳۵..... ۱-۷-۱۱-۸ پارامترهای مورد نیاز شبیه سازی
- ۳۳۵..... ۲-۷-۱۱-۸ گذردهی
- ۳۳۶..... ۷-۱۱-۸ مان تاخیر
- ۳۳۶..... ۴-۷-۱۱-۸ تخصیص منابع
- ۳۳۶..... ۵-۷-۱۱-۸ (صفات) شبیه سازی مستر
- ۳۳۸..... ۶-۷-۱۱-۸ مای (صفات) شبیه سازی اسلیو
- ۳۴۱..... ۷-۷-۱۱-۸ ویژگی‌های (صفات) شبیه سازی اغتشاشگر
- ۳۴۲..... ۸-۷-۱۱-۸ نتیجه شبیه سازی
- ۳۴۳..... ۱-۸-۷-۱۱-۸ پارامترهای نتیجه مستر
- ۳۴۳..... ۲-۸-۷-۱۱-۸ پارامترهای نتیجه اسلیو
- ۳۴۵..... ۳-۸-۷-۱۱-۸ پارامترهای نتیجه اغتشاشگر
- ۳۴۵..... ۹-۷-۱۱-۸ چگونگی پیکره بندی یک شبیه سازی
- ۳۴۶..... ۱۰-۷-۱۱-۸ سناریوهای شبیه سازی
- ۳۴۷..... ۱۱-۷-۱۱-۸ سناریوی شبیه سازی ۱: انتقال فابل
- ۳۴۷..... ۱-۱۱-۷-۱۱-۸ شرایط پایه ای
- ۳۴۷..... ۲-۱۱-۷-۱۱-۸ تنظیم پارامترهای شبیه سازی
- ۳۴۷..... ۱-۲-۱۱-۷-۱۱-۸ شبیه سازی ۱
- ۳۴۸..... ۲-۲-۱۱-۷-۱۱-۸ شبیه سازی ۲
- ۳۴۸..... ۳-۲-۱۱-۷-۱۱-۸ شبیه سازی ۳
- ۳۴۸..... ۳-۱۱-۷-۱۱-۸ نتایج شبیه سازی

۳۴۸.....	۱-۱۱-۷-۱۱-۸ نتایج شبیه سازی ۱
۳۵۱.....	۲-۱۱-۷-۱۱-۸ نتایج شبیه سازی ۲
۳۵۴.....	۳-۱۱-۷-۱۱-۸ نتایج شبیه سازی ۳
۳۵۶.....	نتیجه گیری
۳۵۶.....	۱۲-۷-۱۱-۸ سناریوی شبیه سازی ۲: Intercom telephony
۳۵۶.....	۱-۱۲-۷-۱۱-۸ شرایط پایه ای
۳۵۷.....	۲-۱۲-۷-۱۱-۸ تنظیم پارامترهای شبیه سازی
۳۵۷.....	۱-۲-۱۲-۷-۱۱-۸ شبیه سازی ۱
۳۵۷.....	۲-۲-۱۲-۷-۱۱-۸ شبیه سازی ۲
۳۵۷.....	۳-۲-۱۲-۷-۱۱-۸ شبیه سازی ۳
۳۵۸.....	۱۲-۷-۱۱-۸ نتایج شبیه سازی
۳۵۸.....	۳-۱۲-۷-۱۱-۸ نتایج شبیه سازی ۱
۳۵۹.....	۲-۳-۱۲-۷-۱۱-۸ نتایج شبیه سازی ۲
۳۶۱.....	۳-۳-۱۲-۷-۱۱-۸ نتایج شبیه سازی ۳
۳۶۲.....	۹-۱۱-۸ دیگر اطلاعات کاربردی پیاده سازی بلوتوث
۳۶۲.....	۹-۱۱-۸ اصوات بلوتوث
۳۶۳.....	۲-۹-۱۱-۸ پیاده سازی انواع بسته جدید
۳۶۳.....	۳-۹-۱۱-۸ گسترش تعداد اسلیوها
۳۶۴.....	۴-۹-۱۱-۸ اضافه کردن پارامترهای آماری
۳۶۴.....	۵-۹-۱۱-۸ آنتن همگرا
۳۶۵.....	۶-۹-۱۱-۸ پرو فایل بلوتوث
۳۶۵.....	۱-۶-۹-۱۱-۸ Generic Access پرو فایل
۳۶۶.....	۲-۶-۹-۱۱-۸ پرو فایل (Service Discovery Application) SDP
۳۶۶.....	۳-۶-۹-۱۱-۸ Cordless Telephony پرو فایل
۳۶۶.....	۴-۶-۹-۱۱-۸ Intercom پرو فایل
۳۶۶.....	۵-۶-۹-۱۱-۸ Serial Port پرو فایل
۳۶۶.....	۶-۶-۹-۱۱-۸ Headset پرو فایل

۳۶۷.....	Dial-up Networking	پرو فایل ۷-۶-۹-۱۱-۸
۳۶۷.....	Fax	پرو فایل ۸-۶-۹-۱۱-۸
۳۶۷.....	LAN Access	پرو فایل ۹-۶-۹-۱۱-۸
۳۶۷.....	Generic Object Exchange	پرو فایل ۱۰-۶-۹-۱۱-۸
۳۶۷.....	Object Push	پرو فایل ۱۱-۶-۹-۱۱-۸
۳۶۸.....	File Transfer	پرو فایل ۱۲-۶-۹-۱۱-۸
۳۶۸.....	Synchronisation	پرو فایل ۱۳-۶-۹-۱۱-۸
۳۶۸.....	برد الکترونیک قابل توسعه بلوتوث اریکسون	۷-۹-۱۱-۸
۳۷۱.....		مراجع

فهرست شکل‌ها

۲۹	شکل ۱-۱: امنیت در بلوتوث
۳۰	شکل ۲-۱: سنگ رونی که نشانه بلوتوث است
۳۲	شکل ۳-۱: آرم تجاری دستگاه‌های بلوتوث
۳۳	شکل ۴-۱: سخت افزار بلوتوث
۳۶	شکل ۵-۱: طیف گسترده
۳۷	شکل ۶-۱: باندهای محافظ در FDI
۳۸	شکل ۷-۱: TDD و زمانبندی
۳۸	شکل ۸-۱: بسته‌های چند شیاری
۴۱	شکل ۱-۲: واحدهای سیستم بلوتوث
۴۱	شکل ۲-۲: واحدهای سیستم بلوتوث
۴۴	شکل ۳-۲: بسته اطلاعات بلوتوث
۴۵	شکل ۴-۲: ساختار کد دسترسی
۴۶	شکل ۵-۲: preamble
۴۷	شکل ۶-۲: Trailer
۴۷	شکل ۷-۲: ساختار فیلد هدر
۵۰	شکل ۸-۲: بخش عنوان فیلد داده
۵۵	شکل ۱-۳: پیکون
۵۶	شکل ۲-۳: اسکرین
۵۷	شکل ۳-۳: پروتکل بلوتوث
۶۲	شکل ۴-۳: ساختار WAP
۶۳	شکل ۵-۳: پروتکل بسته لازم برای انتقال فایل
۶۴	شکل ۶-۳: پروتکل بسته لازم برای همزمان سازی

- شکل ۳-۷: پروتکل پشته لازم برای دسترسی به LAN. ۶۵
- شکل ۳-۸: پروتکل پشته لازم برای تلفن‌های سه کاره. ۶۵
- شکل ۳-۹: پروتکل پشته لازم برای هدست‌های دور. ۶۶
- شکل ۴-۱: الگوریتم E_1 . ۷۰
- شکل ۴-۲: الگوریتم E_{21} و E_{22} . ۷۱
- شکل ۴-۳: الگوریتم E_3 . ۷۱
- شکل ۴-۴: تولید کلید اولیه. ۷۳
- شکل ۴-۴: تبادل کلید مرکب. ۷۴
- شکل ۴-۶: تبادل کلید واحد. ۷۵
- شکل ۴-۷: تولید کلید مشترک. ۷۶
- شکل ۴-۸: تصدیق هویت در بلوتوث. ۷۷
- شکل ۴-۹: رمزگذاری با استفاده از الگوریتم E_0 . ۷۸
- شکل ۴-۱۰: ساختمان داخلی مخور E_0 . ۷۹
- شکل ۵-۱: طبقه بندی حملات امنیتی از نظر فعال و غیر فعال بودن. ۸۶
- شکل ۵-۲: شکل ساده شده پروتکل زوج سازی بلوتوث. ۹۰
- شکل ۵-۳: جزئیات پروتکل زوج سازی بلوتوث. ۹۱
- شکل ۵-۴: شکل کلی پروتکل تصدیق هویت. ۹۳
- شکل ۵-۵: جزئیات پروتکل تصدیق هویت. ۹۴
- شکل ۵-۶: حمله آفلاین به پین کد. ۹۸
- شکل ۵-۷: حمله آنلاین به پین کد. ۹۹
- شکل ۵-۸: حمله کلید واحد. ۱۰۱
- شکل ۵-۹: مسئله روز تولد ۴-بعدی. ۱۰۷
- شکل ۵-۱۰: شکستن پین آفلاین. ۱۰۹
- شکل ۵-۱۱: بازسازی پیامهای تصویق هویت. ۱۱۱
- شکل ۵-۱۲: جعل هویت یک وسیله و عبور از تصدیق هویت. ۱۱۳
- شکل ۵-۱۳: حمله رد سرویس در تصدیق هویت و زوج سازی. ۱۱۵
- شکل ۵-۱۴: مرحله اول حمله مرد میانی. ۱۱۷

- شکل ۵-۱۵: مرحله دوم حمله مرد میانی..... ۱۱۸
- شکل ۵-۱۶: دیگرام حمله شکستن بین آنالین..... ۱۲۸
- شکل ۵-۱۷: دیگرام حمله شکستن بین آنالین نسخه ۲..... ۱۳۰
- شکل ۵-۱۸: شکستن بین آنالین-آنالین..... ۱۳۱
- شکل ۵-۱۹: دریافت یک فابل آلوده Cabir..... ۱۴۲
- شکل ۵-۲۰: تغییر مد بلوتوث در گوشی های Nokia..... ۱۴۳
- شکل ۵-۲۱: شناسایی ویروس توسط گوشی های پیشرفته..... ۱۴۴
- شکل ۵-۲۲: دریافت فایلهای آلوده به ویروس Commwarrior..... ۱۴۵
- شکل ۵-۲۳: نمونه‌ای از اسان قابل‌های آلوده به Commwarrior..... ۱۴۵
- شکل ۶-۱: نحوه تولید MAC..... Error! Bookmark not defined.
- شکل ۶-۲: زوج سازی با پروتکل های تبادل کلید امن..... ۱۶۱
- شکل ۶-۳: تصدیق هویت با پروتکل های تبادل کلید امن..... ۱۶۲
- شکل ۶-۴: جلوگیری از حمله مرد میانی با استفاده از تکنیک های Anti-jamming..... ۱۶۸
- شکل ۶-۵: توقف حمله مرد میانی در فرایند زوج سازی..... ۱۷۰
- شکل ۶-۶: توقف حمله مرد میانی در فرایند تصدیق هویت..... ۱۷۱
- شکل ۷-۱: زوج سازی و تصدیق هویت موفق بین دو گره شبکه..... ۱۷۴
- شکل ۷-۲: نمونه تعریف ویژگی های اسلیو در opnet..... ۱۸۳
- شکل ۷-۳: لایه شبکه در opnet در طراحی پیکونت..... ۱۸۴
- شکل ۷-۴: لایه گره در opnet در طراحی پیکونت..... ۱۸۴
- شکل ۷-۵: لایه فرایند در opnet در طراحی پیکونت..... ۱۸۵
- شکل ۷-۶: نمودار استفاده از کانال توسط ۶ اسلیو..... ۱۸۶
- شکل ۷-۷: نمودار تاخیر اتصال توسط ۶ اسلیو..... ۱۸۶
- شکل ۷-۸: نمایش نمودار نرخ انتقال برای یک اسلیو..... ۱۸۷
- شکل ۷-۹: نمودار استفاده از کانال توسط ۶ اسلیو تعریف شده..... ۱۸۸
- شکل ۷-۱۰: نمودار تاخیر اتصال توسط ۹ اسلیو..... ۱۸۸
- شکل ۷-۱۱: برقراری ارتباط صحیح مستر با اسلیوها..... ۱۸۹
- شکل ۸-۱: لایه های پروتکل بلوتوث..... ۱۹۲

۱۹۶	شکل ۸-۲: باند محافظ در FDD
۱۹۷	شکل ۸-۳: TDD و زمانبندی
۱۹۷	شکل ۸-۴: بسته های چند شیاری
۱۹۸	شکل ۸-۵: بسته اطلاعات بلوتوث
۱۹۹	شکل ۸-۶: ساختار کد دسترسی
۲۰۱	شکل ۸-۷: فیلد preamble
۲۰۱	شکل ۸-۸: فیلد Trailer
۲۰۲	شکل ۸-۹: ساختار فیلد هدر
۲۰۵	شکل ۸-۱۰: بخشی عنوان فیلد داده
۲۰۶	شکل ۸-۱۱: ترتیب بیت ها FEC و بدون FEC
۲۰۸	شکل ۸-۱۲: NS: دنباله های ساده شده برای کاربر
۲۱۰	شکل ۸-۱۳: همزادی + و - و 0
۲۱۰	شکل ۸-۱۴: معماری NS
۲۱۲	شکل ۸-۱۵: مثالی از اسکرپیت Tel
۲۱۳	شکل ۸-۱۶: مثالی از اسکرپیت Tel
۲۱۵	شکل ۸-۱۷: یک توپولوژی ساده شبکه و سناریوی شبیه سازی
۲۱۶	شکل ۸-۱۸: مثالی از اسکرپیت Tel
۲۲۰	شکل ۸-۱۹: زمانبند رویداد گسته
۲۲۲	شکل ۸-۲۰: سلسله مراتب کلاسها
۲۲۳	شکل ۸-۲۱: گروه (Multicast & Unicast)
۲۲۴	شکل ۸-۲۲: اتصال
۲۲۴	شکل ۸-۲۳: وارد کردن Object های ردیابی
۲۲۵	شکل ۸-۲۴: صف مایتورینگ
۲۲۶	شکل ۸-۲۵: مثالی از جریان بسته ها
۲۲۷	شکل ۸-۲۶: قالب بسته NS
۲۲۸	شکل ۸-۲۷: اسکرپیت شبیه سازی NS با فعال بودن ردیابی
۲۲۹	شکل ۸-۲۸: مثالی از قالب ردیابی

۲۳۰	شکل ۸-۲۹: گراف دریافتی (cbr) از گره n3
۲۳۱	شکل ۸-۳۰: ساختار فهرستی NS
۲۳۳	شکل ۸-۳۱: مثالی از اجزای شبکه و Object اتصال در C++
۲۳۳	شکل ۸-۳۲: مثال افزایش محدوده متغیر
۲۳۳	شکل ۸-۳۳: مفسر فرمان Otcl
۲۳۴	شکل ۸-۳۴: اجرای فرمان Otcl از یک C++ Object
۲۳۴	شکل ۸-۳۵: عنصر شبکه در زبان C++ وشی پیوند
۲۳۵	شکل ۸-۳۶: انقیاد متغیر
۲۳۶	شکل ۸-۳۷: مفسر فرمان Otcl
۲۳۶	شکل ۸-۳۸: اجرای فرمان OTcl توسط یک شی C++
۲۳۷	شکل ۸-۳۹: توپولوژی شبیه سازی شبکه حلی
۲۳۸	شکل ۸-۴۰: پنجره NAM از شبیه سازی
۲۴۰	شکل ۸-۴۱: توپولوژی شبیه سازی شبکه سرچشمه Web
۲۴۷	شکل ۸-۴۲: نمودار حالت کنترلرهای بلوتوث
۲۵۰	شکل ۸-۴۳: ساختار یک گره بلوتوث
۲۵۴	شکل ۸-۴۴: برقراری ارتباط و تبادل پیام‌های مربوط به OoS
۲۶۰	شکل ۸-۴۵: نحوه پیکره بندی مستر یا استفاده از واسطه گرافیک
۲۶۹	شکل ۸-۴۶: نمایش جریان داده
۲۷۰	شکل ۸-۴۷: نتیجه اجرای NAM
۲۹۱	شکل ۸-۴۸: فرم setting پیاده سازی شده
۲۹۲	شکل ۸-۴۹: نمای طراحی کلاس Form1
۳۰۱	شکل ۸-۵۰: لایه شبکه در OPNET
۳۰۲	شکل ۸-۵۱: لایه گره در OPNET
۳۰۳	شکل ۸-۵۲: لایه فرایند در OPNET
۳۰۴	شکل ۸-۵۳: ساختار سلسله مراتبی در OPNET
۳۰۵	شکل ۸-۵۴: انتخاب و وارد شدن به محیط ویرایشگر شبکه
۳۰۶	شکل ۸-۵۵: انتخاب ساختار شبکه بر مبنای یک ساختار قبلی

- شکل ۸-۵۶: انتخاب مشخصات جغرافیایی شبکه ۳۰۶
- شکل ۸-۵۷: تکنولوژی ادوات مورد استفاده ۳۰۶
- شکل ۸-۵۸: نمایش تمامی اطلاعات انتخاب شده در مراحل قبلی برای تأیید نهایی ۳۰۷
- شکل ۸-۵۹: محیط ویرایشگر شبکه ۳۰۷
- شکل ۸-۶۰: پنجره Object Palette ۳۰۹
- شکل ۸-۶۱: تعیین پارامترهای مورد نیاز برای اجرای شبیه سازی پارامترهای خصوصی و عمومی ۳۱۱
- شکل ۸-۶۲: محیط ویرایشگر Node ۳۱۲
- شکل ۸-۶۳: انواع اتصال مازول ها ۳۱۳
- شکل ۸-۶۴: مازول پردازشگر ۳۱۳
- شکل ۸-۶۵: مازول سف ۳۱۴
- شکل ۸-۶۶: انواع مازول های فیلتر شده ۳۱۴
- شکل ۸-۶۷: انواع مازول های نگین شده ۳۱۴
- شکل ۸-۶۸: مازول آنتن و نحوه تعامالت آن ها ۳۱۵
- شکل ۸-۶۹: دیاگرام STD ۳۱۷
- شکل ۸-۷۰: حالت های موجود در دیاگرام STD ۳۱۸
- شکل ۸-۷۱: نحوه نام گذاری توابع KP ۳۱۹
- شکل ۸-۷۲: نمایش پارامترهای ویرایشگر انتشار آنتن ۳۲۱
- شکل ۸-۷۳: محیط ویرایشگر انتشار آنتن ۳۲۲
- شکل ۸-۷۴: محیط ویرایشگر Packet Format ۳۲۳
- شکل ۸-۷۵: پنجره مشاهده نتایج ۳۲۴
- شکل ۸-۷۶: نمودار استفاده از کانال با ۶ اسلیو ۳۴۹
- شکل ۸-۷۷: تاخیرهای اتصال زمانی که ۶ اسلیو فعال هستند ۳۵۰
- شکل ۸-۷۸: نرخ انتقال (kbits/s) برای یک اسلیو ۳۵۱
- شکل ۸-۷۹: نمودار استفاده از کانال زمانی که ۱۱ اسلیو فعال می باشد ۳۵۲
- شکل ۸-۹۰: تاخیرهای اتصال زمانی که ۱۱ اسلیو فعال هستند ۳۵۳
- شکل ۸-۹۱: نرخ انتقال (kbits/s) برای یک اسلیو با کاهش انتقال ۳۵۴
- شکل ۸-۹۲: تعداد بسته های گم شده ۳۵۵

- شکل ۸-۹۳: فاصله بین متر و اغتشاشگر (m) ۳۵۶
- شکل ۸-۹۴: تاخیرهای اتصال ۳۵۸
- شکل ۸-۹۵: توزیع تجمعی زمان‌های تاخیر ۳۵۹
- شکل ۸-۹۶: متوسط احتمال بلاکینگ ۳۶۰
- شکل ۸-۹۷: تاخیر اتصال ۳۶۱
- شکل ۸-۹۸: متوسط احتمال بلاکینگ ۳۶۲
- شکل ۸-۹۹: تشعشع از یک آنتن همگرا ۳۶۴
- شکل ۸-۱۰۰: پروفایل‌ها، بلوتوث ۳۶۵
- شکل ۸-۱۰۱: برد الک‌رونیک قابل توسعه بلوتوث اریکسون ۳۶۹

فهرست جداول

۴۶	جدول ۱-۲: انواع LAP
۴۹	جدول ۲-۲: انواع بسته‌های بلوتوث
۵۱	جدول ۲-۳: ساختار L_CH
۵۸	جدول ۳-۳: لایه‌های پروتکل بلوتوث
۸۳	جدول ۱-۱: انواع حملات و علل آن در بلوتوث
۱۴۱	جدول ۲-۵: انواع ویرس‌های موبایل
۱۷۹	جدول ۱-۷: مقایسه زمان تست کلید در حملات پین و رمز
۱۸۵	جدول ۲-۷: پیکره بندی پارامترهای شبیه سازی
۱۸۷	جدول ۳-۷: نمونه پیکره بندی پارامترهای شبیه سازی
۱۹۵	جدول ۱-۸: باندهای فرکانسی برتر در مناطق مختلف
۲۰۰	جدول ۲-۸: انواع LAP
۲۰۳	جدول ۳-۸: انواع بسته‌های بلوتوث
۲۰۵	جدول ۴-۸: ساختار L_CH
۲۰۶	جدول ۵-۸: انواع بسته‌های ACL
۲۰۶	جدول ۶-۸: انواع بسته‌های SCO
۲۴۶	جدول ۷-۸: حالات مختلف بلوتوث
۲۴۹	جدول ۸-۸: حالات مختلف بلوتوث
۳۳۷	جدول ۹-۸: صفات مستر و مقادیر قابل تعریف
۳۴۰	جدول ۱۰-۸: صفات اسلیو و مقادیر قابل تعریف
۳۴۲	جدول ۱۱-۸: صفات اغتشاشگر و مقادیر قابل تعریف
۳۴۷	جدول ۱۲-۸: شبیه سازی ۱: تنظیم پارامترهای شبیه سازی
۳۴۸	جدول ۱۳-۸: شبیه سازی ۲: تنظیم پارامترهای شبیه سازی
۳۵۷	جدول ۱۴-۸: شبیه سازی ۱: تنظیم پارامترهای شبیه سازی