

احراز هویت در شبکه های رادیو شناختگر مبتنی بر شبکه

میلاد حیدری پور

انتشارات راه دکتوری (همکار سنجش و دانش)

۵۰۰ نسخه

۱۳۹۵-اول

۹۷۸-۶۰۰-۸۶۴۱-۷۱-۱

مؤلف:

ناشر:

تیراژ:

نوبت چاپ:

شابک:

کلیه حقوق مادی و معنوی این اثر برای مؤلف محفوظ می باشد



فصلنامه علمی-تخصصی
فصلنامه علمی-تخصصی

- سرشناسه
عنوان و نام پدیدآور
مشخصات نشر
مشخصات ظاهری
شابک
وضعیت فهرست نویسی
موضوع
موضوع
موضوع
رده بندی کنگره
رده بندی دیویی
شماره کتابشناسی ملی
- : حیدری پور، میلاد، ۱۳۶۷ -
: احراز هویت در شبکه های رادیو شناختگر مبتنی بر شبکه / مولف میلاد حیدری پور .
: تهران: انتشارات راه دگتری: سفینش و دانش، ۱۳۹۶ .
: ۶۳ ص.
: ۱۸۰۰۰۰:۹۷۸-۶۰۰-۸۶۴۱-۷۱-۱ رزاق
: قیما
: شبکه های رادیو شناختی
Cognitive radio networks :
: شبکه های رادیو شناختی - تدابیر ایمنی
Cognitive radio networks -- Security measures :
TK۵۱۰۳/۴۸۱۵/ج۹ ص ۲۹۶ :
: ۶۲۱، ۴۴ :
: ۵۹۹۹ :
: ۵۹۹۹ :

فهرست مطالب

فهرست مطالب	عنوان	صفحه
۱	چکیده	۱
۲	مقدمه	۲
۵	فصل اول	۵
۵	کلیات	۵
۶	۱-۱ بیان مسئله	۶
۶	۲-۱ سوال	۶
۷	۳-۱ متغیرها	۷
۷	۵-۱ اهداف	۷
۷	۶-۱ اهمیت و ضرورت	۷
۷	۷-۱ روش	۷
۸	۸-۱ روش گرد آوری اطلاعات	۸
۸	۹-۱ ابزار گرد آوری اطلاعات	۸
۸	۱۰-۱ شیوه تجزیه و تحلیل اطلاعات	۸
۸	۱۲-۱ تعریف مفاهیم	۸
۸	۱-۱۲-۱ رادیو شناختی	۸
۸	۲-۱۲-۱ شبکه	۸
۹	۳-۱۲-۱ احراز هویت	۹
۹	۱۴-۱ محدودیت ها و موانع	۹
۹	۱۵-۱ سازمان دهی	۹
۱۰	فصل دوم:	۱۰
۱۰	پیشینه	۱۰
۱۲	اصول:	۱۲
۱۲	۱-۲-۲-۳ ویژگی های رادیوی شناختی:	۱۲
۱۲	۲-۲-۲-۳ عملکردهای رادیو شناختی:	۱۲
۱۳	۳-۲-۲-۳ کاربردها و ساختار شبکه:	۱۳

۱۴	۳-۲-۳ حسگری طیف و آنالیز:
۱۴	۱-۳-۲-۳ دمای تداخل:
۱۵	۲-۲-۳-۲ حسگری طیف:
۱۸	۲-۳-۲-۳ حسگری مبتنی بر فیلتر:
۱۸	۴-۳-۲-۳ حسگری سریع:
۱۸	۵-۳-۲-۳ حسگری مبتنی بر یلگیری / توجیه:
۱۸	۶-۳-۲-۳ حسگری و مدل‌یابی مبتنی بر اندازه‌ها:
۱۹	۷-۳-۲-۳ حسگری همکارانه:
۲۱	۴-۲-۳ تخصیص و تقسیم طیف دینامیک:
۲۲	۱-۲-۳-۱ کنترل دسترسی متوسط در شبکه‌های رادیویی شناختی:
۲۳	۲-۲-۳-۲ از زدن طیف:
۲۳	۱-۲-۳-۲ رله شناختی:
۲۴	۴-۲-۳-۴ حسگری صرفاً دسترسی:
۲۴	۵-۴-۲-۳ کنترل تیره در یک شبکه CR:
۲۵	۶-۴-۲-۳ مدیریت کنترل آنال:
۲۵	۷-۴-۲-۳ تقسیم طیف ترابری:
۲۵	۸-۴-۲-۳ بازی تقسیم طیف:
۲۶	۹-۴-۲-۳ مسیر یابی در یک شبکه C:
۲۶	۱۰-۴-۲-۳ شبیه‌سازی و اجرای همگامی:
۲۷	۱۱-۴-۲-۳ ایمنی در شبکه‌های CR:
۲۷	۵-۲-۳-۵ سکوها و استانداردهای رادیویی شناختی:
۲۸	۲ بررسی امنیت شبکه‌های رادیو شناختگر
۲۸	۱-۲-۳-۳ تهدیدات امنیتی شبکه‌های بی‌سیم
۲۸	۲-۲-۳-۳ تهدیدهای امنیتی شبکه‌های رادیو شناختگر
۲۹	۳-۲-۳-۳ طبقه بندی انواع حملات
۳۰	الف) تقلید رفتار کاربر اولیه (PUEA)
۳۰	ب) تحریف داده‌های مربوط به طبقه‌بندی (SSDF)
۳۱	ج) حمله به لایه MAC
۳۲	د) حمله به کانال مشترک (CCC)
۳۳	ه) حمله CROSS-LAYER
۳۳	ی) حمله به رادیو نرم افزار تعریف شده (SDR) 15
۳۳	۳-۳-۳ راه‌های مقابله با حملات شناخته شده
۳۳	۱-۳-۳-۳ مقابله با تقلید رفتار کاربر اولیه
۳۴	۲-۳-۳-۳ مقابله با تحریف داده‌های مربوط به طیف سنجی

۳۵	۳-۳-۳-۳	مقایله با حمله با لایه MAC
۳۵	۴-۳-۳-۳	مقایله با حمله به CCC
۳۶	۵-۳-۳-۳	مقایله با حمله Cross-Layer
۳۶	۶-۳-۳-۳	مقایله با حمله به SDR
۳۶	۲-	چالش‌های امنیتی در شبکه‌های رادیو شناختگر
۳۷	۱-۲	احراز هویت
۳۷	۱	شناسایی
۳۸	۲-۱-۳	احراز هویت
۳۸	۱-۲-۱-۳	نوع اول
۳۸	۲-۲-۱-۳	نوع دوم
۳۸	۳-۲-۱-۳	نوع سوم
۳۸	۳-۱-۳	احراز هویت با عاملی
۳۹	۴-۱-۳	روش‌های شناسایی و احراز هویت
۳۹	۱-۴-۱-۳	احراز هویت با رمز عبور
۳۹	۲-۴-۱-۳	احراز هویت با مدل بیومتریک
۳۹	۳-۴-۱-۳	احراز هویت با token
۴۰	۴-۴-۱-۳	احراز هویت با Ticket
۴۰	۵-۴-۱-۳	
۴۱	۲-۲	نگاهی گذرا به نظریه شبکه
۴۸	۳-	طرح پیشنهادی
۴۸	۱-۳	توصیف ریاضیات طرح پیشنهادی و نمادها
۴۸	۲-۳	جبر طرح پیشنهادی
۵۰	۳-۳	الگوریتم پیشنهادی برای تولید کلیدهای اعتبارسنجی
۵۱	۴-۳	روش احراز هویت در طرح پیشنهادی
۵۱	۵-۳	اثبات صحت الگوریتم پیشنهادی
۵۳	۶-۳	امنیت الگوریتم پیشنهادی

چکیده

با توسعه سریع دستگاه ها و کاربردهای وایرلس جدید در دهه اخیر شاهد رشد تقاضا برای طیف رادیویی وایرلس بوده است. البته سیاست تخصیص طیف ثابت یک مشکل برای استفاده موثرتر طیف می شود که تحت آن بخشی از طیف دارای گواهی به شدت مورد استفاده کمتر قرار می گیرد. کاربرد ناکارآمد منابع طیف محدود، سازمان های قانون گذار طیف را ملزم به بررسی سیاست شان و جستجوی فناوری ارتباطات جدید می نماید که می تواند از طیف وایرلس به یک شیوه انعطاف پذیر و هوشمندانه تر بهره برداری نماید. مفهوم رادیویی شناختی برای پرداخت به مساله کارایی طیف پیشنهاد می شود و در سال های اخیر مورد توجه زیادی قرار گرفته است. پیشرفت های معنادار زیادی در پند سال گذشته در زمینه رادیوهای شناختی وجود داشته اند.

در این مجموعه روشی متفاوت و جدید برای احراز هویت در سطح شبکه ی رادیو شناختگر ارائه خواهیم کرد که از چندین منظر نسبت به روش های موجود برتری دارد: نخست آن که از امکانات موجود در سطح لایه ی فیزیکی و MAC بهره خواهد گرفت و به منابع مستقل دسترسی ندارد. دوم آن که عملیات پیشنهادی در سطح سخت افزار و با پیچیدگی محاسباتی کمتری نسبت به روش های مرسوم کار می کند و سرعت چشم گیر و قابل ملاحظه ای دارد. سوم آن که الگوی پیشنهادی با شرایط حاکم بر محیط رادیویی و تهدیدهای امنیتی محیطی به خوبی مطابقت دارد. روش پیشنهادی برخلاف روش های مرسوم، امنیت خود را از مساله ی SVP در متنبه (attacker) به دست آورده است.

واژه گان کلیدی: رادیو شناختگر، احراز هویت، شبکه، SVP

کاربرد منابع طیف رادیویی و تنظیم اشعارات رادیویی از سوی سازمان های قانونگذار ملی نظیر کمیسیون ارتباطات فدرال FCC هماهنگ می شوند. FCC طیف را به دارندگان گواهی دار که به آنها کاربران اولیه نیز گفته می شود بر یک پایه بلند مدت برای نواحی جغرافیایی بزرگ تخصیص می دهد. البته بخش اعظمی از طیف تخصیص داده شده مانند شکل ۱ کم استفاده باقی می ماند. کاربرد ناکارآمد طیف محدود، توسعه روش های دسترسی طیف پویا را لازم می نماید در این روش ها کاربرانی که گواهی های طیف ندارند تحت عنوان کاربران ثانویه اجازه استفاده از طیف گواهی دار بلااستفاده موقتی پیدا می کنند.

در سال های اخیر FCC کاربردهای جامع و انعطاف پذیرتر طیف موجود را از طریق استفاده از فناوری رادیوی شناختی مدنظر قرار داده است. رادیوی شناختی، فناوری توانمند ساز کلیدی است که امکان استفاده از شبکه های ارتباطی نسل بعد موسوم به شبکه های دسترسی طیف پویا DSA برای استفاده کارآمدتر طیف به یک شیوه فرصت طلبانه بدون مداخله در کاربران اولیه می دهد. این فناوری به عنوان یک رادیو تعریف می شود که می تواند پارامترهای فرستنده اش را طبق تعاملات با محیطی که در آن عمل می کند تغییر دهد. این با دستگاه های رادیوی متعارف فرق دارد از این لحاظ که یک رادیوی شناختی می توان کاربران را با قابلیت شناختی و قابلیت پیگیر بندی مجدد تجهیز نماید. قابلیت شناختی به توانایی برای حس و جمع آوری اطلاعات از محیط اطراف، استفاده می شود از جمله اطلاعات در مورد فرکانس انتقال، پهنای باند، نیرو، مدولاسیون و ... با این قابلیت، کاربران ثانویه می توانند بهترین طیف موجود را شناسایی کنند. قابلیت پیگیر بندی مجدد به توانایی برای تطبیق و سازش سریع پارامترهای عملکردی طبق اطلاعات حس شده به منظور دستیابی به عملکرد مطلوب اطلاق می شود. با بهره برداری از طیف به یک شیوه فرصت طلبانه، رادیوی شناختی به کاربران ثانویه امکان حس این را می دهد که کدام بخش از طیف در دسترس می باشد. انتخاب بهترین کانال موجود، هماهنگ سازی دسترسی طیف با کاربران دیگر و تخلیه کانال زمانی که یک کاربر اولیه، دعای استفاده صحیح از طیف دارد می دهد. با ملاحظه استفاده جامع و انعطاف پذیرتر منابع طیف به ویژه زمانی که کاربران ثانویه کاربران اولیه همزیستی دارد الگوهای تخصیص طیف سنتی و پروتکل های دسترسی طیف دیگر قابل کاربرد نمی باشند. این امری که کاربران اولیه برای استفاده از طیف در اولویت می باشند هنگامی که کاربران ثانویه با کاربران اولیه همزیست می باشند آنها باید مانیورینگ به موقع باند پهن طیف گواهی مورد استفاده را انجام دهند. وقتی به کاربران ثانویه اجازه انتقال همزمان داده ها با یک کاربر اولیه داده می شود حد دمای تداخل نباید زیر پا گذاشته شود.

اگر کاربران ثانویه تنها اجازه انتقال در زمانی دارند که کاربران اولیه از طیف استفاده نمی کنند آنها باید از حضور مجدد اولیه از طریق روش های آشکارسازی مختلف از قبیل آشکارسازی انرژی، آشکارسازی ویژگی، آشکارسازی منسجم و فیلتر تطبیقی آگاه باشند. به دلیل عدم قطعیت نویز، ایجاد سایه و اثر چند مسیری، عملکرد آشکارسازی حس کاربر واحد

نسبتاً محدود می باشد. حسگرهای همکارانه در بهبود بخشیدن دقت آشکارسازی با بهره بردن از تنوع کاربری و فضایی مؤثر محسوب شده است. به منظور استفاده کامل از منابع طیف، تخصیص طیف پویای کارآمد و الگوهای تقسیم بسیار مهم می باشند. پروتکل های کنترل دسترسی طیف جدید و مدیریت کانال باید به گونه ای طراحی شوند که با محیط طیف پویا مطابقت داشته باشند ضمن آنکه از برخورد با یک کاربر اولیه نیز اجتناب می کنند. وقتی یک کاربر اولیه در یک باند گواهی دار مجدداً ظاهر می شود یک مکانیسم کنارگذاری طیف خوب برای تأمین انتقال فرکانس صاف با نهفتگی پایین برای کاربران ثانویه لازم می باشد. در شبکه های وایرلس شناختی چند برآمدگی، برآمدگی های شناختی واسطه باید به طور هوشمند از رله اطلاعات و مسیریابی از طریق استفاده از مجموعه ای از کانال های متغیر پویا پشتیبانی نمایند. به منظور مدیریت تداخل در کاربران اولیه تداخل دو جانبه در میان خود آنها، نیروی انتقال کاربران ثانویه باید با دقت کنترل شود و رقابیشان برای منابع طیف نیز باید در نظر گرفته شود. پیشرفت های معنادار زیادی در چند سال گذشته در زمینه راه های شناختی وجود داشته اند. این مجموعه به بررسی پیشرفت های اخیر طی تحقیقی در رابطه با رادیوهای شناختی می پردازد. به دلایل محدودیت باندهای فرکانسی در دسترس، نحوه ی تخصیص طیف فرکانسی بین کاربران به یکی از مهمترین مشاغل در توسعه ی شبکه های بی سیم تبدیل شده است. در حال حاضر سیاست اختصاص طیف فرکانسی در شبکه های رادیو، سیاستی جزئی و ایستا است. گسترش کاربردها و خدمات بی سیم در سال های اخیر سبب شده تا کمبود سطوح فرکانس رادیو، که بتواند پاسخگوی نیاز روزافزون آنها باشد، همواره به عامل اصلی نگرانی در گسترش بسترهای ارتباطی تبدیل شود [1].

بررسی های انجام شده حاکی از آن است که کاربران آه به کاردارای مجوز ارسال بر روی طیف هستند، هرگز از باندهای فرکانسی تخصیص یافته به صورت مفید و مؤثر، استفاده نمی کنند. بنابراین استفاده ناکارآمد از باندهای فرکانسی مجاز سبب بروز مشکل کمبود طیف فرکانسی شده است [2].

فناوری رادیوشناختگر با تکیه بر الگوریتم های هوشمند در تلاش است تا کاربران ثانوی و بدون مجوز بتوانند از باندهای فرکانسی در تملک به دیگران به شکلی پویا و بدون مزاحمت و اختلال برای صاحبان اصلی، به شکل فرصت طلبانه استفاده کنند.

امیتولاه در اوایل دهه ۱۹۹۰ اندیشه ی «رادیوی مبتنی بر نرم افزار» (SDR) را مطرح ساخت و سپس با استفاده از این نظریه در سال ۱۹۹۸ برای اولین بار مفهوم رادیوشناختگر را ارائه نمود [۱]. رادیوشناختگر یک سیستم مخابراتی هوشمند است که قادر به شناس محیط خارجی، یادگیری و اتخاذ تصمیم هوشمند برای تنظیم پارامترهای انتقال بر اساس وضعیت فعلی محیط است به قسمی که به صورت کارآمد و بدون تداخل با سیگنال های مالک اصلی طیف، بهره وری باندهای فرکانسی را به بالاترین سطح ممکن می رساند [۳،۴].

هر یک از اجزای شبکه های رادیوشناختگر می توانند از محیط پیرامون خود یاد بگیرند و خودشان را با محیط وفق دهند. این قابلیت برای پیاده سازی روش هایی خلاق و هوشمند در مدیریت طیف قابلیتی ارزشمند و اساسی است [5].

مدیریت باندهای فرکانسی بلااستفاده و بهره‌گیری از این باندها برای اهداف و مقاصد دیگری همانند ارائه اینترنت سرعت بالا در مناطق روستایی و امکان ایجاد برنامه‌های کاربردی با نرخ انتقال داده‌ی بالا مانند ویدئو کنفرانس‌ها و تسریع در به روزرسانی شبکه‌های ارتباطی که منجر به کاهش هزینه‌های ساخت می‌شود، از مزایای دیگر رادیوشناختگر است [۲].

شبکه‌های رادیوشناختگر به دلیل ویژگی‌های خاص و محیطی که در بطن آن فعالیت می‌کنند با چالش‌های جدیدی روبرو هستند و برای غلبه بر چهار عملکرد (تابع) استفاده می‌کنند که شامل سنجش طیف، مدیریت طیف، تسهیم طیف و جا به جایی در طیف است [۶].

در این مجموعه روشی متفاوت و جدید برای احراز هویت در سطح شبکه‌ی رادیوشناختگر ارائه خواهیم کرد که از چندین منظر نسبت به روش‌های موجود برتر است: نخست آنکه از امکانات موجود در سطح لایه‌ی فیزیکی و MAC بهره خواهد گرفت و تابع مستقل نیاز ندارد. دوم آنکه عملیات پیشنهادی در سطح سخت افزار و با پیچیدگی محاسباتی کمتری نسبت به روش‌های مرسوم کار می‌کند و سرعت چشمگیر و قابل ملاحظه‌ای دارد. سوم آنکه الگوی پیشنهادی با شرایط حاکم بر محیط رادیویی و راداری‌های چنین محیطی به خوبی مطابقت دارد.