دانشکده مهندسی
گروه برق

پایان‌نامه کارشناسی

گرایش: کنترل

عنوان:

چالش‌های امنیتی موجود در شبکه‌های رادیوشناختگر

استاد راهنما:

دکتر محمد مصطفوی

نگارش:

مهدی اسکندری

شهریور95

چکیده

با در نظر گرفتن استفاده از تکنولوژی بی‌سیم در چند سال اخیر، نگرانی کمبود طیف فرکانسی یکی از دغدغه‌های دولت‌ها، سازمان‌ها و کاربران شده است. رادیوشناختگر، یک شاخه‌ی نوظهور در دنیای مخابرات بی‌سیم است که با بهره‌وری از آن، چهنای باند موجود به بهینه‌ترین صورت استفاده می‌شود و در نتیجه افراد بیشتری قادر به دسترسی به طیف فرکانسی خواهند بود. یکی از مسائل اصلی و ضروری در زمینه‌ی طراحی این رادیو، تأمین امنیت آن است. این مهم نسبت به دیگر قسمت‌های موجود در ساختار رادیوشناختگر، کمتر مورد توجه قرار گرفته است. در این پروژه مرویر کلی بر امنیت شبکه‌های رادیوشناختگر خواهیم داشت و سپس به بررسی انواع حملات، تهدیدات و راه‌های مقابله با آن‌ها خواهیم پرداخت.

کلمات کلیدی: رادیو نرم‌افزاری، رادیوشناختگر، کاربر اولیه، کاربر ثانویه، تهدیدات امنیتی، حملات امنیتی

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

فهرست نمودارها

مقدمه

طیف فرکانسی یک منبع محدود و ارزشمند است. نحوه‌ی دسترسی به طیف فرکانسی در شبکه‌های مخابراتی کنونی به صورت استاتیکی است. با توجه به تقاضای روبه‌رشد کاربران برای استفاده از مخابرات بی‌سیم، این روش تخصیص طیف در آینده نه چندان دور با مشکل مواجه خواهد شد. در حال حاضر، هر کاربر متقاضی طیف فرکانسی، با مراجعه به نهاد مربوطه مجوز استفاده از آن را خریداری می‌کند.

تحقیقات اخیر نشان می‌دهد استفاده نادرست از طیف‌های مجوزدار، باعث به هدر رفتن منابع طیفی می‌شود. این امر توجه محققین را به سمت استفاده دینامیکی از طیف پیش برد. به این ترتیب در ساعاتی طیف‌های خریداری بلااستفاده هستند، دیگر کاربران با رعایت قوانین خاص قادر به استفاده از آن بازه طیفی خواهند بود. به شبکه‌هایی که از این روش استفاده می‌کنند، شبکه‌های رادیوشناختگر می‌گویند. این رادیو به عنوان یک رادیو هوشمند شناخته می‌شود چراکه قادر است محیط پیرامون خود را مشاهده کند و بعد از طیف سنجی و شناسایی طیف‌های بدون استفاده، پارامترهای خود را نظیر مدولاسیون، توان، فرکانس و غیره متناسب را محیط جدید تغییر دهد تا در نهایت بتواند از طیف فرکانسی استفاده کند.

بعد از مطرح شدن این ایده، تحقیقات درباره‌ی چگونگی طراحی این رادیو، به طور گسترده شکل گرفته است. از جمله زمینه‌های تحقیقاتی در شبکه‌های رادیوشناختگر می‌توان به تخصیص طیف، تخصیص توان، جلوگیری از تداخل و غیره اشاره نمود. با این که تأمین امنیت در طراحی هر نوع شبکه‌ای جزو نیازهای اولیه شبکه محسوب می‌شود، اما در تحثیثات انجام شده پیرامون شبکه‌های رادیوشناختگر و نیازهای آن‌ها، به برقراری امنیت و مسائل مربوط به آن توجه چندانی نشده است.

با در نظر گرفتن اهمیت موضوع تأمین امنیت در طراحی شبکه‌های رادیوشناختگر، در این پروژه سعی بر آن شده که به این مهم به طور کامل پرداخته شود.

در فصل یک ابتدا به معرفی رادیوشناختگر و ویژگی‌های آن خواهیم پرداخت.با در نظرگرفتن این که طیف سنجی مهم‌ترین بخش چرخه یک رادیوشناختگر است، قسمتی از فصل یک به آن موضوع هم اختصاص داده شده است. موضوع فصل دوم بررسی مسائل امنیتی و انواع تهدیدها و حملات می‌باشد. در نهایت در فصل سوم جمع بندی و نتیجه گیری مطالب آورده خواهد شد.

1- فصل اول

معرفی شبکه رادیوشناختگر

1.1 مقدمه

با توجه به رشد روزافزون مخابرات بی‌سیم پیش بینی می‌شود در آینده با کمبود طیف فرکانسی مواجه شویم. طیف فرکانسی یک منبع محدود و با ارزش است و باید به صورت اصولی مدیریت شود. به طور مثال کمیته فدرال آمریکا[1](FCC) وظیفه تخصیص پهنای باند تجاری را برعهده دارد. هر کاربر برای ارسال و دریافت اطلاعات روی یک باند مشخص باید به سازمان مربوطه مراجعه و مجوز استفاده از آن را خریداری کند. به این روش تخصیص فرکانس ایستا[2] می‌گوید. از جمله مزیت‌های این روش کاهش تداخل، سادگی ساخت و پیاده‌سازی و افزایش کیفیت خدمات رسانی می‌باشد.

با در نظر گرفتن یکسان نبودن نیاز کاربران به طیف فرکانسی و پهنای باند اختصاص یافته به آن‌ها، قسمت قابل توجهی از طیف فرکانسی بدون استفاده باقی مانده و بخش‌های دیگر نیز فقط در زمان‌های خاص، دارای ترافیک چشمگیری هستند. لازم به ذکر است که در بخش‌هایی از طیف فرکانسی، تراکم کاربرها بسیار زیاد است.

علاوه بر طیف‌های خریداری شده توسط کاربران که طیف مجوزدار[3] نامیده می‌شود، قسمت‌هایی از طیف فرکانسی به کاربران بدون مجوز اختصاص یافته است. کاربرها می‌توانند بدون هیچ مجوزی و در توان‌های پایین از این بخش استفاده کنند. استانداردهایی چون Bluetooth، Wi-MAX و Wi-Fi در باند ISM[4] حضور دارند. محدوده‌ی فرکانسی این باند بین 2.4 تا 2.5 گیگاهرتز بوده و یکی از شلوغ ترین باندهای فرکانسی است. به این باندها، باندهای بدون مجوز[5] می‌گویند. تعداد وسایل ارتباطی که در این بازه فعالیت

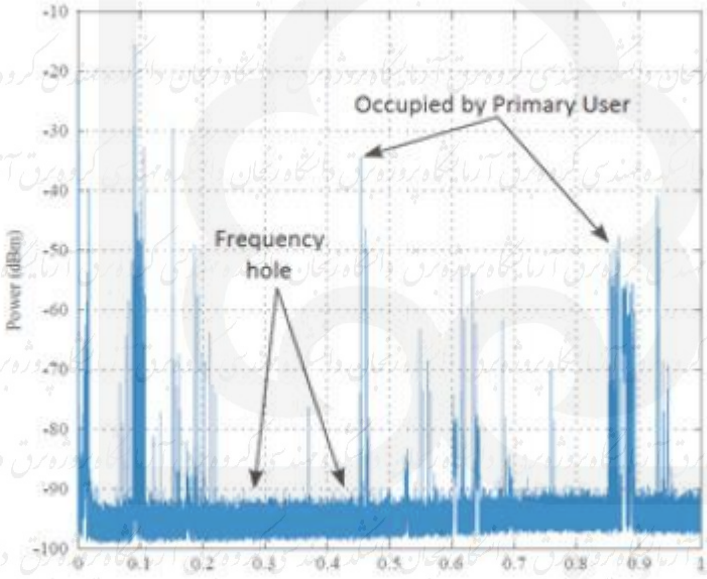
[1] Federal Communications Commission
[2] Static spectrum access
[3] Licensed band
[4] Industrial, Scientific and Medical
[5] Unlicensed band

می‌کنند، هر روز رو به افزایش هستند. بنابراین تداخل بین سیستم‌ها زیاد شده و این موضوع باعث کاهش کارایی سیستم می‌شود.

کمیته فدرال آمریکا در سال 2002 گزارشی را با هدف بهبود بخشیدن استفاده از طیف فرکانسی ارائه کرد. نتیجه این گزارش حاکی از آن بود که تخصیص طیف به روش ایستا، بهینه نیست؛ چراکه درصد چشمگیری از کاربران در تمام ساعت شبانه روز از طیف در دسترس به طور کامل استفاده نمی‌کنند و فرصت های طیفی به میزان قابل توجهی بیهوده هدر می‌رود.

نمودار 1-1 طیف اندازه گیری توسط دانشگاه کانزاس در یک بعد از ظهر را نشان می‌دهد. به قسمت‌هایی از طیف فرکانسی که مالک طیف حضور ندارد و طیف بدون استفاده باقی مانده است، اصطلاحا حفره فرکانسی[1] می‌گویند.

نمودار 1-1 طیف فرکانسی در کانزاس آمریکا



آقای میتولا در سال 1999 ایده استفاده از این طیف به صورت پویا را ارائه کرد. اساس این طرح قابلیت سنجش طیف است و به نحوی که در مواقع خالی بودن طیف امکان استفاده از آن برای کابران دیگر مهیا شده

[1] Frequency Hole

و در نتیجه بهبود چشمگیری در بهره وری حاصل گردد.در این رادیو که رادیو شناختگر[1](CR) نامیده می‌شود، کاربری که مالک طیف است و اولیت استفاده از طیف با او می‌باشد، کاربر مجوزدار[2] یا کاربر اولیه[3]، و به کاربری که طیف را مشاهده می‌کند تا فرصت طیفی پیدا کند، کاربر بدون مجوز[4] یا کاربر ثانویه[5] می‌گویند. هنگامی که کاربر اولیه از طیف استفاده می‌کند، نباید برای او مزاحمت و یا تداخل ایجاد کند و به محض حضور کاربر اولیه باید طیف را ترک کند.

این رادیو می‌تواند به صورت هوشمند بسنجد که کدام باندهای فرکانسی خالی و کدام باندها اشتغال هستند و بعد از آن پارامترهای عملکردی خود نظیر مدولاسیون، توان و غیره را بر طبق مشاهدات طیفی خود تغییر دهد تا بتواند از حفره طیفی استفاده کند.

1.2 ویژگی‌های یک رادیوشناختگر

ویژگی‌های اصلی یک رادیوشناختگر عبارت‌اند از: آگاهی، هوشمندی، تطبیق پذیری و قابلیت اطمینان و بازدهی.

تاکنون تعاریف مختلفی بر مبنای ویژگی‌های رادیوشناختی ارائه شده است که هر یک از آن‌ها روی تعداد خاصی از ویژگی‌ها تأکید دارند. در جدول 1-1 تمام تعاریف بیان شده توسط سازمان‌ها، نویسندگان و محققان جمع آوری شده است.

[1] Cognitive Radio
[2] Licensed user
[3] Primary user
[4] Unlicensed user
[5] Secondary user

جدول 1-1 تمامی تعاریف ارائه شده برای رادیوشناختگر

Definer	Adapts (Intelligently)	Autonomous	Can sense Environment	Transmitter	Receiver	"Aware" Environment	Goal Driven	Learn the Environment	"Aware" Capabilities	Negotiate Waveforms	No interference
FCC	•	•	•	•							
Haykin	•	•	•	•	•	•	•	•			
IEEE 1900.1	•	•	•	•	•						
IEEE USA	•	•	•	•	•	•					•
ITU-R	•	•	•	•	•	•					
Mitola	•	•	•	•	•	•	•	•	•	•	
NTIA	•	•	•	•	•	•	•				
SDRF CRWG	•	•	•	•	•		•				
SDRF SIG	•	•	•	•	•	•	•	•	•		
VT CRWG	•	•	•	•	•	•	•	•	•		

سیستم رادیوشناختگر شامل سه بخش اصلی می‌باشد که عبارتند از:

1. حس کردن طیف فرکانسی: مهمترین تفاوت بین رادیو مبتنی بر شناخت و رادیوهای قدیمی، در نحوه دسترسی به طیف فرکانسی است. طیف‌سنجی یکی از ویژگی‌های اصلی رادیوشناختگر است که شامل بخش‌های ذیل است:
   - تخمین مجموع تداخل در محیط‌های رادیویی
   - شناسایی حفره‌های فرکانسی
   - تخمین اطلاعات و وضعیت کانال مانند SNR
   - پیش بینی ظرفیت کانال
2. مدیریت/شناخت: یک شبکه رادیوشناختگر، طیف‌های فرکانسی اعم از مجوزدار و بدون مجوز را در محدوده‌ی وسیع شناسایی می‌کند. بعد از آن بهترین باند را انتخاب کرده و جهت استفاده از آن با دیگر کاربران همکاری می‌کند. سپس به محض آشکار شدن کاربر اولیه باید باند ترک شود. بنابراین به منظور پیاده‌سازی مراحل فوق، سیستم رادیوشناختگر نیازبه بخشی جدید جهت مدیریت و شناخت دارد. مدیریت نیز یکی از ویژگی‌های اصلی است که شامل بخش های ذیل است:[1]

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

3- جمع بندی و نتیجه‌گیری

با توجه به محدودیت‌های پهنای باند، استفاده از تکنولوژی‌های سنتی بی‌سیم قادر به پاسخگویی نیاز کاربران نیست. در این پروژه یک تکنولوژی جدید به نام رادیوشناختگر معرفی و مفاهیم اولیه آن بیان شد. در تحقیقات انجام شده، به مسأله‌ی تعمین امنیت این شبکه‌ها توجه چندانی نشده است در حالی که داشتن یک ارتباط امن جزو اساسی ترین نیازهای یک سیستم است. بنابراین در ادامه پروژه به بررسی مسائل امنیتی موجود در رادیوشناختگر پرداختیم. با توجه به ساختار متفاوت این رادیو، علاوه بر حملات مرسوم در مخابرات بی‌سیم، حملات جدیدی نیز آن را تهدید می‌کنند. که مختص خود شبکه هستند. در این پروژه سعی شد برخی‌های حملات شاخص و روزنه‌های امنیتی رادیوشناختگر مورد بررسی قرار بگیرد و سپس راه‌های مقابله با این حمله‌ها بین شدند.

4- منابع

[1] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE journal on selected areas in communications*, vol. 23, pp. 201-220, 2005.

[2] F. K. Jondral, "From Maxwell's equations to cognitive radio," in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, 2008, pp. 1-5.

[3] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE communications surveys & tutorials*, vol. 11, pp.2009 ,130-116 .

[4] J. Mitola, "Cognitive radio---an integrated agent architecture for software defined radio," 2000.

[5] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer networks*, vol. 50, pp. 2127-2159, 2006.

[6] M. Mchenry, "Spectrum white space measurements New America Foundation Broadband Forum," ed: June, 2003.

[7] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proceedings of the IEEE*, vol. 100, pp. 3172-3186, 2012.

[8] J. L. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, 2008, pp. 1-7.

[9] R. Dubey, S. Sharma, and L. Chouhan, "Secure and trusted algorithm for cognitive radio network," in *2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN)*, 2012, pp. 1-7.

[10] L. Tang and J. Wu, "Research and analysis on cognitive radio network security," *Wireless Sensor Network*, vol. 4, p. 120, 2012.

[11] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks," *網際網路技術學刊*, vol. 12, pp. 181-198, 2011.

[12] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on selected areas in communications*, vol. 26, pp. 25-37, 2008.

[13] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Ráez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *2009*

IEEE 28th International Performance Computing and Communications Conference, 2009, pp. 208-215.

[14] D. Hlavacek and J. M. Chang, "A layered approach to cognitive radio network security: A survey," *Computer Networks*, vol. 75, pp. 414-436, 2014.

[15] K. K. Chauhan and A. K. S. Sanger, "Survey of Security threats and attacks in cognitive radio networks," in *Electronics and Communication Systems (ICECS), 2014 International Conference on*, 2014, pp. 1-5.

[16] O. León, J. Hernández‐Serrano, and M. Soriano, "Securing cognitive radio networks," *international journal of communication systems*, vol. 23, pp. 633-652, 2010.

[17] C. Cormio and K. R. Chowdhury, "A survey on MAC protocols for cognitive radio networks," *Ad Hoc Networks*, vol. 7, pp. 1315-1329, 2009.

[18] B. F. Lo, "A survey of common control channel design in cognitive radio networks," *Physical Communication*, vol. 4, pp. 26-39, 2011.

[19] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 15, pp. 428-445, 2013.

[20] W. Wang, Y. Sun, H. Li, and Z. Han, "Cross-layer attack and defense in cognitive radio networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, 2010, pp. 1-6.

[21] A. Amanna and J. H. Reed, "Survey of cognitive radio architectures," in *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)*, 2010, pp. 292-297.

[22] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead," *IEEE Communications Surveys & Tutorials*, vol. 14, pp. 355-379, 2012.