



دانشگاه زنجان

دانشکده مهندسی

گروه برق

پایان نامه کارشناسی

گرایش: کنترل

عنوان:

چالش‌های امنیتی موجود در شبکه‌های

رادیو شناختگر

استاد راهنما:

دکتر محمد مصطفوی

نگارش:

مهدی اسکندری

شهریور 95

فهرست مطالب

1.....	مقدمه
2.....	1- فصل اول
2.....	1.1 مقدمه
4.....	1.2 ویژگی های یک رادیوشناختگر
6.....	1.3 رادیو مبتنی بر نرم افزار
7.....	1.4 استاندارد IEEE802.22
8.....	1.5 معماری شبکه رادیوشناختگر
10.....	1.6 تقسیم بندی طیف فرکانسی
11.....	1.7 معرفی شبکه های رادیوشناختگر
15.....	1.8 معرفی سامانه های رادیویی هوشمند
17.....	1.9 سامانه های اشتراک طیفی پویا
20.....	1.10 مفاهیم سامانه های رادیویی هوشمند
23.....	1.11 حسگری طیفی
24.....	-2 فصل دوم
24.....	2.1 مقدمه
24.....	2.2 تهدیدهای امنیتی شبکه های بی سیم
25.....	2.3 تهدیدهای امنیتی شبکه رادیوشناختگر
26.....	2.4 طبقه بندی انواع حملات
27.....	2.4.1 تقلید رفتار کاربر اولیه (PUEA)

2.4.2	حمله به توابع هدف	32
2.4.3	حمله به لایه MAC	35
2.4.4	تحریف داده های مربوط به طیف سنجی (SSDF)	37
2.4.5	حمله به کانال کنترل مشترک (CCC)	38
2.4.6	حمله CROSS-LAYER	40
2.4.7	حمله به رادیو نرم افزاری (SDR)	42
3-	جمع بندی و نتیجه گیری	44
4-	منابع	45

فهرست نمودارها

- نمودار 1-1 طیف فرکانسی در کانزاس آمریکا..... 3
- نمودار 1-2 سیر تکامل یک رادیوشناختگر تا امروز..... 7
- نمودار 1-3 استفاده از فرکانس‌های مختلف طیفی در طول زمان..... 16
- نمودار 1-4 توزیع توان در فرکانس‌های مختلف طیفی..... 16
- نمودار 1-5 دو روش عمده برای بهره‌وری از طیف فرکانسی الف) اشتراک طیفی از طریق ارسال زمینه‌ای سیگنال‌ها. ب) اشتراک طیفی از طریق روی هم گذاری سیگنال‌ها..... 19
- نمودار 1-6 حفرة‌های طیفی در باندهای فرکانسی و زمان‌ها و توان‌های مختلف..... 21
- نمودار 1-2 دو شکل از یک تابع هدف (a) براساس پارامترهای خاص (b) بعد از حمله از سوی مهاجم 35

مقدمه

طیف فرکانسی یک منبع محدود و ارزشمند است. نحوه 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 طیف‌سنجی و شناسایی طیف‌های بدون استفاده، پارامترهای خود را نظیر مدولاسیون، توان، فرکانس و غیره متناسب با 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 تحقیقات 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 نظر گرفتن این که طیف‌سنجی 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 جمع‌بندی و نتیجه‌گیری مطالب آورده خواهد شد.

1- فصل اول

معرفی شبکه رادیو شناختگر

1.1 مقدمه

با توجه به رشد روزافزون مخابرات بی سیم پیش بینی می شود 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 آمریکا¹ (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 ایستا² می گوید. از جمله مزیت های این روش کاهش تداخل، سادگی

ساخت و پیاده سازی و افزایش کیفیت خدمات رسانی می باشد.

با در نظر گرفتن یکسان نبودن نیاز کاربران به طیف فرکانسی و پهنای باند اختصاص یافته به آن ها،

قسمت قابل توجهی از طیف فرکانسی بدون استفاده باقی مانده و بخش های دیگر نیز فقط در زمان های خاص،

دارای ترافیک چشمگیری هستند. لازم به ذکر است که در بخش هایی از طیف فرکانسی، تراکم کاربرها بسیار

زیاد است.

علاوه بر طیف های خریداری شده توسط کاربران که طیف مجوزدار³ نامیده می شود، قسمت هایی از

طیف فرکانسی به کاربران بدون مجوز اختصاص یافته است. کاربرها می توانند بدون هیچ مجوزی و در

توان های پایین از این بخش استفاده کنند. استانداردهایی چون Wi-Fi، Wi-MAX، Bluetooth در باند ISM

⁴ حضور دارند. محدوده ی فرکانسی این باند بین 2.4 تا 2.5 گیگاهرتز بوده و یکی از شلوغ ترین باندهای

فرکانسی است. به این باندها، باندهای بدون مجوز⁵ می گویند. 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

کاربری که مالک طیف است و اولیت استفاده از طیف با او می‌باشد، کاربر مجوزدار² یا کاربر اولیه³، و به کاربری که طیف را مشاهده می‌کند تا فرصت طیفی پیدا کند، کاربر بدون مجوز⁴ یا کاربر ثانویه⁵ 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	No interference	Negotiate Waveforms	"Aware" Capabilities	Learn the Environment	Goal Driven Environment	"Aware" Environment	Receiver	Transmitter	Can sense Environment	Autonomous	Adapts (Intelligently)
FCC											
Haykin											
IEEE 1900.1											
IEEE USA											
ITU-R											
Mitola											
NTIA											
SDRF CRWG											
SDRF SIG											
VT CRWG											

سیستم رادیوشناختگر شامل سه بخش اصلی می باشد 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. طیف سنجی یکی از ویژگی های اصلی رادیوشناختگر است که شامل بخش های ذیل است:

- تخمین مجموع تداخل در محیط های رادیویی
- شناسایی حفره های فرکانسی
- تخمین اطلاعات و وضعیت کانال مانند SNR

• پیش بینی ظرفیت کانال

2. مدیریت/شناخت: یک شبکه رادیوشناختگر، طیف های فرکانسی اعم از مجوزدار و بدون مجوز را در

محدوده ی وسیع شناسایی می کند. بعد از آن بهترین باند را انتخاب کرده و جهت استفاده از آن با دیگر کاربران همکاری می کند. سپس به محض آشکار شدن کاربر اولیه باید باند ترک شود. بنابراین به منظور پیاده سازی مراحل فوق، سیستم رادیوشناختگر نیازهی بخشی جدید جهت مدیریت و شناخت دارد.

مدیریت نیز یکی از ویژگی های 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 نتیجه گیری

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 تعیین امنیت این شبکه‌ها توجه چندانی نشده است در حالی که داشتن یک

ارتباط امن جزو اساسی‌ترین نیازهای یک سیستم است. بنابراین در ادامه پروژه به بررسی مسأله‌ی 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 روزه‌های 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.