

コグニティブ無線における一次利用者模擬攻撃に対する 協力型検知方式

周 士博† 堀 良彰‡ 櫻井 幸一‡

†九州大学大学院システム情報科学府

819-0395 福岡県福岡市西区元岡744

shih-po@itslab.csce.kyushu-u.ac.jp

‡九州大学大学院システム情報科学研究院

819-0395 福岡県福岡市西区元岡744

hori@inf.kyushu-u.ac.jp, sakurai@csce.kyushu-u.ac.jp

あらまし 近年、無線 LAN の利用者が急速な増加とともに、周波数不足という問題が発生している。コグニティブ無線は動的スペクトラムアクセスによりこの問題を解決できるような技術であるが、PUE (Primary User Emulation) 攻撃というサービス妨害(DoS: Denial of Service) 攻撃がある。対策として WSPRT(Wald's Sequential Probability Ratio Test)を用いた検知モデルが提案されている。この対策は攻撃者らの存在場所により見逃し(False Alarm)率が 4 割程度になる恐れがある。本稿では、複数の二次利用者(Secondary User)が WSPRT を用いた検知を行い、それぞれの検知結果を共有するという協力検知方式を提案する。提案手法に関する実験を行い、攻撃者が集中して分布している場合、単独の利用者による WSPRT を用いた検知方式より見逃し率を低減できることを示す。

Multi-users Cooperative Detection for Primary User Emulation Attack in Cognitive Radio Networks

Shih-Po Chou† Yoshiaki Hori‡ Kouichi Sakurai‡

†Graduate School of information Science and Electrical Engineering, Kyushu University

744 Motoooka, Nishi-ku, Fukuoka 819-0395, JAPAN

shih-po@itslab.csce.kyushu-u.ac.jp

‡Faculty of Information Science and Electrical Engineering, Kyushu University

744 Motoooka, Nishi-ku, Fukuoka 819-0395, JAPAN

hori@inf.kyushu-u.ac.jp, sakurai@csce.kyushu-u.ac.jp

Abstract Recently, more and more people become to use the wireless networks. A problem that the increase of available radio spectrum resources cannot follow user increases. CRNs can help secondary users to find the white spectrum by using dynamic spectrum access (DSA) technology. However, the security of cognitive radio network cannot be ensured. Primary user emulation attack (PUEA) is known as one type of denial of service (DoS) attack in CRNs. We proposed a cooperative detection method for PUEA base on the Wald's sequential probability ratio test (WSPRT). And we show the result of our cooperative detection method with multi-users.

1 はじめに

最近、無線ネットワークの利用者は増える傾向にある。しかし、電波間の干渉や法律などの制限があるため、周波数帯域を大幅に増加させることは困難である。従来の無線ネットワークのスペクトラムの使用率は頻度によって大きな差が見られ、最小では15%しか使用されないものの、最大では85%のスペクトラムが使用されている[1]。そのため無線ネットワークが普及するとともに、通信時に使用できる周波数が不足することになる。コグニティブ無線技術はその問題を解決するため、開発が進められている。

しかし、様々な長所があるコグニティブ無線にも無線ネットワークと同じようなセキュリティに関する脆弱性がある。例えば、PUE 攻撃(Primary user emulation attacks)という攻撃である[2][3]。

本稿では、PUE 攻撃への対策として NPCHT(Neyman-Person Composite Hypothesis Test)と WSPRT(Wald's Sequential Probability Ratio Test)を用いた2つの既存手法を紹介する[4][5]。これらは受信した電波のエネルギーを分析することだけでなく、利用者と基地局の位置情報も利用するものである。しかし、攻撃者らが二次利用者の近くに集中していると、見逃し率が高くなる。本稿では、シミュレーションによって、見逃し率が攻撃者の存在位置により4割程度になる恐れがあることを示す。さらに、その見逃し率を抑えるため、二次利用者間で情報を共有する WSPRT に基づく協力型の検知方式を提案する。また、その方式の優位性を実験によって示す。

2 コグニティブ無線

コグニティブ無線とは、Dynamic Spectrum Access(DSA)により、ライセンスを持つ一次

利用者(Primary User)の未使用周波数帯を検知し、二次利用者(Secondary user)が通信をする際に最適な未使用周波数帯に切り替えることで、周波数帯域を有効に利用できる技術である。一次利用者とは優先的に特定の周波数帯を使用できるユーザである(例:TVタワーなど)。二次利用者とは一次利用者のような権限を持っていないユーザである。DSAの検知手法としてエネルギー検知、特徴検知とマッチフィルタ検知の3つが提案されている[6]。その中でも特に、エネルギー検知が利用されている。その理由は、一次利用者からのエネルギーだけを分析することで、一次利用者の通信に影響を与えずに未使用周波数帯を検知できるためである。将来、無線LANの利用者が現在より多くなることは間違いなく、有限の周波数帯域を有効に利用することが大切になる。コグニティブ無線はこの周波数不足の問題を軽減できる技術だと考えられる。

3 一次利用者模擬 (PUE) 攻撃

コグニティブ無線において、二次利用者は電波のエネルギーによって、スペクトラムが一次利用者に使われているかどうかを確認することができる。攻撃者はその特徴を利用し、一次利用者と類似しているシグナルを発信することで、他の二次利用者に一次利用者が存在していると認識させ、他のスペクトラムを探させることができる。このような攻撃を一次利用者模擬 (Primary User Emulation, PUE) 攻撃という。もしPUE 攻撃を利用する攻撃者が複数存在してしまうと、スペクトラム検知頻度が高くなり、通信遅延やDoSなどの恐れがある。その結果、多くのスペクトラムの使用が中断される可能性がある。コグニティブ無線を実用化するためには、PUE 攻撃を解決する必要がある。

4 既存対策

4.1 Neyman-Person Composite Hypothesis Test (NPCHT) :

NPCHT を用いた検知手法は PUE 攻撃への対策として提案されている。現時点での通信が正常か攻撃かを区別するため、事前に期待する誤検知率によって定められる閾値(α)を設定する。

この手法では、基地局からのエネルギー $P_r^{(p)}$ は、基地局の送信パワー P_t 、二次利用者との距離 d_p 、アンテナ利得 G_p により、

$$P_r^{(p)} = P_t d_p^{-2} G_p^2 \quad (1)$$

で計算できる。基地局からのエネルギー $P_r^{(p)}$ の確率密度関数は、

$$p^{(P_r)}(\gamma) = \frac{1}{A\sigma_p\sqrt{2\pi\gamma}} \exp\left\{-\frac{(10\log_{10}\gamma - \mu_p)^2}{2\sigma_p^2}\right\} \quad (2)$$

である。

そして、攻撃者数が M 個のとき、全攻撃者からのエネルギー $P_r^{(m)}$ は、各攻撃者の送信パワー P_m 、二次利用者との距離 d_j 、アンテナ利得 G_j により、

$$P_r^{(m)} = \sum_{j=1}^M P_m d_j^{-4} G_j^2 \quad (3)$$

と計算できる。全攻撃者からのエネルギー $P_r^{(m)}$ の確率密度関数は

$$p^{(m)}(\chi) = \frac{1}{A\sigma_\chi\sqrt{2\pi\chi}} \exp\left\{-\frac{(10\log_{10}\chi - \mu_\chi)^2}{2\sigma_\chi^2}\right\} \quad (4)$$

となり、(3)と(4)の確率密度関数の比

$$\Lambda = \frac{p^{(m)}(x)}{p^{(P_r)}(x)} \quad (5)$$

を計算する。

$$\begin{cases} \Lambda \leq \alpha & D_1 : \text{通信が正常である} \\ \Lambda \geq \alpha & D_2 : \text{PUE 攻撃である} \end{cases}$$

上記のように設定した閾値と比べることで、二次利用者は現時点の通信が正常なのか、または PUE 攻撃なのかを区別できる。

表 1 は誤検知率に関する閾値を 0.2、表 2 はこの閾値を 0.1 とし、攻撃者の存在範囲

を変更したときの、誤検知率と見逃し率を示す。表 1 と表 2 を比較すると、誤検知率は設定した閾値とほぼ同じである。しかし、見逃し率は攻撃者の存在範囲が 30m~150m の場合、8 割程度になる可能性がある。

表 1. 閾値 $\alpha = 0.2$ の際に、攻撃者の存在範囲と確率(False Alarm, Miss)の関係

攻撃者存在範囲	30m~ 90m	30m~ 150m	30m~ 210m	30m~ 270m
False Alarm	0.72	0.79	0.66	0.35
Miss	0.203	0.204	0.202	0.202

False Alarm : 見逃し。 Miss : 誤検知。

表 2. 閾値 $\alpha = 0.1$ の際に、攻撃者の存在範囲と確率(False Alarm, Miss)の関係

攻撃者存在範囲	30m~ 90m	30m~ 150m	30m~ 210m	30m~ 270m
False Alarm	0.85	0.88	0.81	0.52
Miss	0.101	0.103	0.104	0.101

4.2 Wald's Sequential Probability Ratio Test (WSPRT) :

WSPRT を用いた検知手法は現時点での通信が、正常か攻撃かを区別するため、期待する誤検知率と見逃し率によって定められる閾値(α_1, α_2)を事前に設定する。誤検知とは実際に正常な通信が行われているにもかかわらず、攻撃であると検知することである。逆に、見逃しとは実際に PUE 攻撃が行われているにもかかわらず、正常であると検知することである。この二つの閾値(α_1, α_2)により、通信状況を判断するための閾値(T_1, T_2)を得られる。

WSPRT を用いた検知手法では、基地局からの電界強度 $P_r^{(p)}$ と M 個の攻撃者からの電

界強度 $P_r^{(m)}$ を計算する。そして、基地局からの電界強度 $P_r^{(p)}$ の確率密度関数と全攻撃者からの電界強度 $P_r^{(m)}$ の確率密度関数から得られる $P_r^{(p)}$ と $P_r^{(m)}$ により、尤度比 Λ を計算する。 X_i は時点 i で感知した電界強度である。ある連続した時間軸上で n 回の試験を行った決定値を計算する。

$$\Lambda_n = \prod_{i=1}^n \frac{p^{(m)}(x_i)}{p^{(p)}(x_i)} \quad (6)$$

以下のように通信の状況を分析できる。

$$\left\{ \begin{array}{ll} \Lambda_n \leq T_1 = \frac{\alpha_1}{1 - \alpha_2} & D_1 : \text{通信が正常である} \\ \Lambda_n \geq T_2 = \frac{1 - \alpha_1}{\alpha_2} & D_2 : \text{PUE 攻撃である} \\ \text{他の状況} & D_3 : \text{区別できない} \end{array} \right.$$

表 3. 閾値($\alpha_1 = 0.2$, $\alpha_2 = 0.2$)の際に、攻撃者の存在範囲と確率(False Alarm, Miss)の関係

攻撃者 存在範囲	30m~ 90m	30m~ 150m	30m~ 210m	30m~ 270m
False Alarm	0.31	0.44	0.27	0.16
Miss	0.183	0.180	0.173	0.148

表 4. 閾値($\alpha_1 = 0.1$, $\alpha_2 = 0.2$)の際に、攻撃者の存在範囲と確率(False Alarm, Miss)の関係

攻撃者 存在範囲	30m~ 90m	30m~ 150m	30m~ 210m	30m~ 270m
False Alarm	0.37	0.39	0.31	0.18
Miss	0.174	0.163	0.158	0.121

表 3 は誤検知率と見逃し率に関する閾値を(0.2, 0.2)、表 4 はこれらの閾値を(0.1, 0.2)とし、攻撃者の存在範囲を変更したときの、誤検知率と見逃し率を示す。表 3 と表 4 では誤検知率が閾値より小さくなり、見逃し率も NPCHT を用いた検知手法の結果より良くなる。

攻撃者の分布が分散しているならば、Jin らの WSPRT を用いた検知方式が有効である。しかし、全攻撃者が二次利用者の周りに集中して分布している場合、見逃し率が 4 割程度になる。

5 提案とその評価

5.1 提案手法

我々は既存研究の問題に対し、複数の二次利用者らが協力して検知を行う方式を提案する。前提として全ての二次利用者は WSPRT を用いた検知手法を実装する。

まず、各々の二次利用者は SNR(Signal-to-Noise Ratio)値を計算する。二次利用者の周りに攻撃者の数が少なければ、攻撃者からの干渉も少なくなり、SNR 値が高くなる。逆に、攻撃者の数が多ければ、干渉が大きくなり、SNR 値が低くなる。

次に、WSPRT を用いた手法により、それぞれの通信状況の検知を行う。検知の結果と先に計算した SNR 値をまとめ、レポートを作成する。

最後に、作成したレポートを交換する。それぞれの SNR 値を比べ、最も高い SNR 値を持つ二次利用者を選択し、そのレポートを参照し、通信の状況が正常か PUE 攻撃かを判断する。

5.2 実験と評価

我々の提案手法が Jin らの WSPRT を用いた検知方式の問題点を有効に改善できるかどうか MATLAB を用いたシミュレーションにより示す。表 5 はそれぞれのシミュレーションの共通パラメータを示す。

実験 1 と実験 2 は、二次利用者が 2 人の場合の協力型の検知方式のシミュレーションを行う。2 人の座標を SU1(0, 0), SU2(500, 0) に設定する。

表 5. シミュレーションの共通パラメータ

TV タワー	1 個
TV タワーが電波を送信する確率	0.5
攻撃者数	25 人
攻撃者が電波を送信する確率	1
攻撃者の分布範囲	300m×300m
誤検知の閾値(α_1)	0.2
見逃しの閾値(α_2)	0.2

実験 1 :

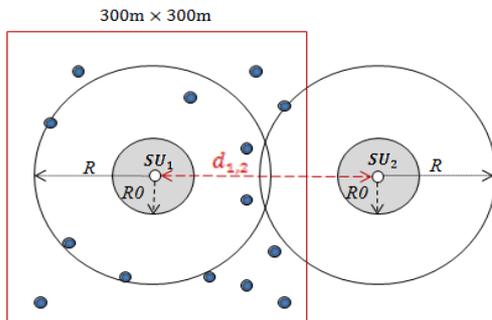


図 1. 実験 1 で想定している状況

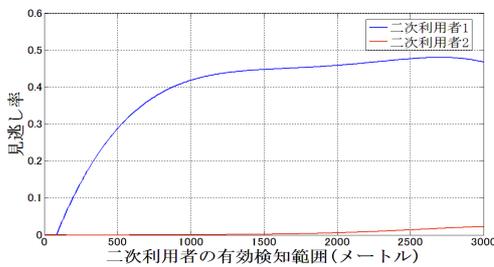


図 2. 実験 1 における 2 人の有効検知範囲と見逃し率の関係

実験 1 では二次利用者を SU1 と SU2 の 2 人として、SU1 の周りに攻撃者が分布すると仮定する。図 1 は実験 1 における攻撃者と二次利用者の分布を示す。この状況は SU1 の検知に対する影響が最も大きい。図 2 は図 1 の環境での二次利用者の有効検知範囲と見逃し率との関係の結果を示す。この図より、SU1 での見逃し率が 5 割弱になってしまったが、SU2 では 2 割未満になった。

実験 2 :

実験 2 では二次利用者を SU1 と SU2 の 2 人として、攻撃者が 2 人の中点を中心として分布すると仮定する。図 3 は実験 2 における攻撃者と二次利用者の分布を示す。この状況は 2 人の検知に対する影響がほぼ同程度である。図 4 は図 3 の環境での二次利用者の有効検知範囲と見逃し率との関係の結果を示す。この図より、SU1 と SU2 での見逃し率が 3 割程度になった。

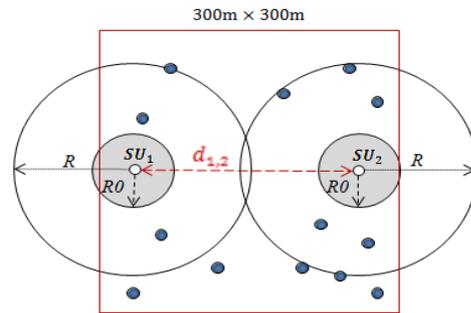


図 3. 実験 2 で想定している状況

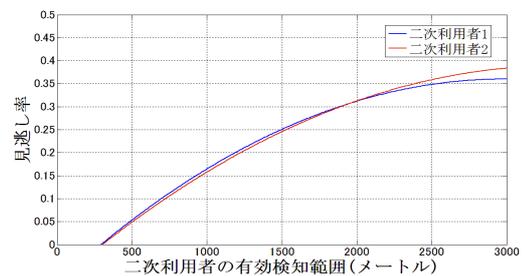


図 4. 実験 2 における 2 人の有効検知範囲と見逃し率の関係

以上のシミュレーションより、二次利用者が 2 人の場合、攻撃者を 2 人の中点を中心として分布している状況、2 人ともに同じような影響を与えるため、我々の協力検知方式における最悪な状況であると考えられる。

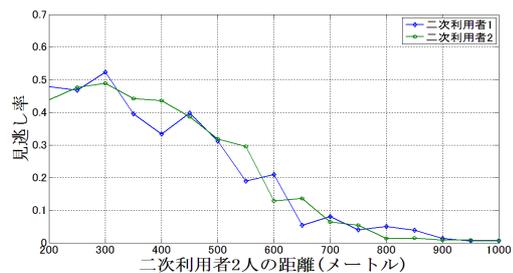


図 5. 二人の距離と見逃し率の関係

図5は2人の二次利用者の相対距離と見逃し率の関係を示す。2人の距離が600m以上にすると、見逃し率が設定した閾値より低くなる。WSPRTを用いた検知手法を利用する際に、適当な二次利用者を2人(距離が600m以上)選択することで、正しい検知の結果が得られる。

実験3:

実験3では、二次利用者が3人の場合の協力型の検知方式のシミュレーションを行う。三人の二次利用者の座標をSU1(100, 300), SU2(0, 0), SU3(500, 0)に設定する。攻撃者は3人のフェルマー点を中心とした範囲の中にランダムに分布しているとする。フェルマー点とは、三角形の3つの頂点からの距離の合計が最小になる点である。関連研究から、攻撃者が二次利用者の周りに集中していると、二次利用者への影響が最も大きく、最悪の状況で見逃し率が4割程度以上になることが分かっている。

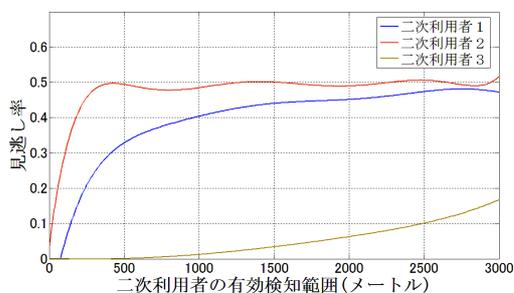


図6. 有効検知範囲と見逃し率の関係

図6は実験3における二次利用者の有効検知範囲と見逃し率の関係を示す。図6より、攻撃者からの影響はSU2が最も大きく、見逃し率が5割弱になってしまった。逆に、SU3の見逃し率が2割未満という検知状況になった。二次利用者らはSNR値が低いSU3のレポートを参照することで、見逃し率を最大3割程度改善できる。

6 まとめと今後の課題

本研究では、PUE攻撃を有効に検知するため、JinらのWSPRTを用いた検知手法に基づく協力型検知方式を提案した。協力型検知方式が単独でのWSPRTを用いた検知手法の問題点を改善できることを確認したが、今後は様々な状況でのシミュレーションをする必要がある。

参考文献

- [1] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey," Elsevier Computer Networks Journal, Vol. 50, pp.2127-2159, Sept. 2006.
- [2] Ruiliang Chen, Jung-Min Park, and Jeffrey H. Reed. "Defense against Primary User Emulation Attacks in Cognitive Radio Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 26, NO. 1, pages 25-37, JANUARY 2008
- [3] O. Le'on, J. Hern'andez-Serrano and M. Soriano. "Securing cognitive radio networks" INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS, volume 23, issue 5, pp633-652, 2010.
- [4] Z. Jin, S. Anand and K. P. Subbalakshmi. "Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing" ACM SIGMOBILE Mobile Computing and Communications Review Volume 13 Issue 2, pages 77-85, April 2009.
- [5] Z. Jin, S. Anand and K. P. Subbalakshmi. "An analytical model for primary user emulation attacks in cognitive radio networks." IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks, pages 1-6, OCTOBER 2008.
- [6] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty. "A Survey on Spectrum Management in Cognitive Radio Networks" IEEE Communications Magazine, Volume 46 Issue4, pages 40-48, April 2008.