Proceedings of the 4th International Conference on Computing and Data Science (CONF-CDS 2022)
DOI: 10.54254/2755-2721/2/20220616

Cognitive radio: SSDF attack and security

Liangyu Song[1,5,†], Shuqi Shen[2,†], Yujie Cao[3] and Xiaoming Lyu[4]

[1]School of Communications and Information Engineering, Nanjing University of Posts and Telecommunication, Nanjing, 210003, China,
[2]School of Information Engineering, Wuhan University of Technology, Wuhan, 430070, China
[3]Department of Electrical and Computer engineering, University of Washington, Seattle, 98195, USA
[4]Ningbo Xiaoshi High School, Ningbo, 315000, China

[5]b19010221@njupt.edu.cn
[†]These two authors contribute equally to the work.

Abstract: Cooperative spectrum sensing can improve the performance of system detection, but when there are some malicious users in sensors, they will launch spectrum sensing data falsification attack, this is to say they send false sensing result, which will have a great influence on the final decision of fusion center and the primary user. Given that, this paper proposes a basic cooperative spectrum sensing algorithm based on reputation to defend malicious users and then improve that algorithm, advance a new algorithm-reputation weighted cooperative spectrum sensing algorithm.Verified by simulation, our algorithm has achieved the expected effect. The first algorithm can effectively resist attacks especially when the attack probability of malicious users is high. When malicious users are more intelligent, their attack probabilities are different from each other and are uncertain. At this time, the second algorithm can better improve the performance of the final decision of fusion center.

Keywords: SSDF attack, cooperative spectrum sensing algorithm based on reputation, reputation weighted, data fusion, detection probability.

1. Introduction

Cognitive radio (CR), an intelligent wireless communication system with the ability of cognition and reconfiguration, has been facing new security threats. Adversaries could exploit several vulnerabilities of the technology and degrade its performance. In our research, Spectrum Sensing Data Falsification (SSDF) attack, where malicious users (MU) falsify their spectrum sensing data before sending to the fusion center (FC) to reduce the performance of the collaborating network, is examined.

Currently, there're limited research works on the security problem brought by SSDF attack, and there are limitations for each existing approaches. For instance, the approach in is not valid in the presence of multiple attackers [1], while the algorithm in loses superiority when the attackers are mostly independent [2].

Based on these papers, we put forward a reputation-based algorithm and an improved reputation-weighted algorithm to defend against SSDF attacks, and the basic goal for us is to decrease the false

DOI: 10.54254/2755-2721/2/20220616

alarm probability (Q_f) and increase the detection probability (Q_d) as much as possible.

2. System model

Here, we consider a ad hoc network with single center and N cognitive users. And M of them are malicious and they are going to attack the fusion center at a specific time. As shown in fig. 1.

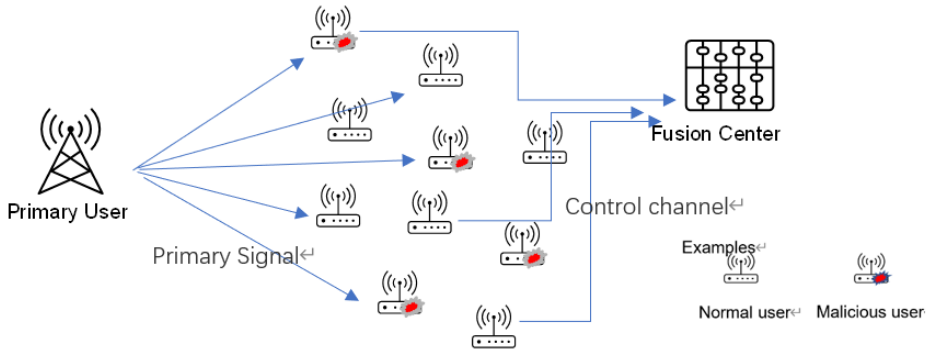

Figure 1. Security model of SSDF.

In this system, time is divided into many small intervals and at the end of each interval, the CR nodes report their sensing results to the FC. It is assumed that the sensing results of each CR are independent of each other and the reported results are single bit decisions.

Each CR node uses energy detection or pilot detection.

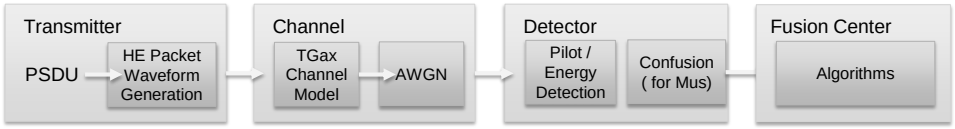

Figure 2. Simulation flow of SSDF attack.

Here is the flow of our simulation. You can see two kinds of users are made in one block so its four blocks.

And in this flow A PSDU，or PLCP Service Data Unit， is created and encoded to create a single packet waveform.

1. The waveform is passed through an indoor TGax channel model.
2. Then add white Gaussian noise
3. The packet is detected
4. Send it directly to fusion center or for the malicious user they add confusion
5. Fusion center make the decision

2.1. Primary user model

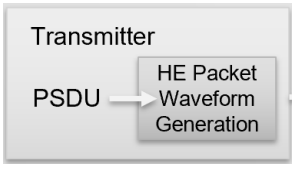

Figure 3. Structure of Transmitter.

The main users here follow the 802.11ax standard [3]. In each simulation, the main users will randomly send many data packets with a payload of 1000 bytes in 20 MHz channel bandwidth.

2.2. Channel model

The channel here adopts the combination of TGax [4] and AWGN. When the primary user sends a signal, it will pass through these two filters, and when the primary user does not send a signal, the channel is

DOI: 10.54254/2755-2721/2/20220616

AWGN channel [5].

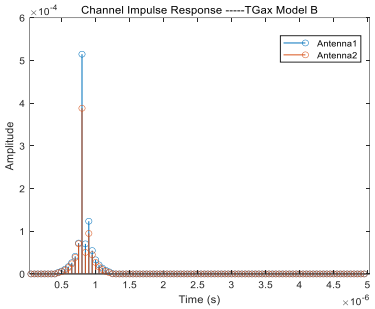

Figure 4. Channel impulse response.

2.3. Channel parameters

Breakpoint distance： 5m
RMS delay spread： 15ns
Maximum delay： 80ns
Rician K-factor： 0dB
Number of taps： 9
Number of clusters： 2

- * When the distance set greater than 5 meters, the channel can be considered as a NLOS channel.

2.4. Cognitive radios model

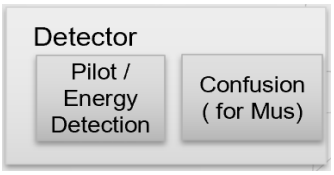

Figure 5. Structure of Detector.

In the receiver, the double sliding window detection mechanism is adopted. In the CR node [6], two detection schemes can be used. Energy detection is more rapid, but suffers from high detection error warnings and low detection probability. pilot detection is accurate and more adaptable to low signal-to-noise ratios, but the detection time is long and the time delay for reporting to FC is greater [7].

* Cabric, D. , A. Tkachenko , and R. W. Brodersen . Spectrum Sensing Measurements of Pilot, Energy, and Collaborative Detection. IEEE, 2007.

2.5. Malicious users model

Assume that there are 20 users, of which 40% are malicious. They confuse the results in many ways [8].

1) Independent attacks

Here, the malicious users would not communicate with each other and will apply the attack directly to FC.

1.1) random reporting results

The user detected the probability of detection is P_d and it will randomly report the cannel's status at P_{report}.

1.2) reverse reporting

The user detected the probability of detection is P_d and it will oppositely report the cannel's status.

2) cooperative attacks

Here, the malicious user will communicate with each other and report the same data to FC.

DOI: 10.54254/2755-2721/2/20220616

2.1) against most results.

If more than a half of the malicious CRs detected the primary user, it will report the opposite result to FC. This can be regarded as an improvement of the second independent attack.

2.2) L out of M attack

This is an attack with certain randomness. When one or more of these users decide to attack, they will take malicious behavior, which can be regarded as an improvement of the first cooperative malicious attack.

3. Algorithm and implement

In the given system model,we consider two attack scenario. In his first scenario the attack probability of each malicious user is equal and really high. For this attack scenario, we propose the algorithm based on reputation. In the second scenario, we consider the attack probability of each malicious user is not necessarily equal and attack probability in every sensing is random. We improve the first algorithm and propose reputation-weighted cooperative spectrum sensing algorithm.

3.1. Algorithm based on reputation

1)Reputation calculation

In order to distinguish honest users from malicious users, we introduce reputation. In each cycle detection, we compare the final decision of the fusion center with the local detection data of each sensor. The more times they are equal, the higher the user's reputation. Obviously, honest users always report real detection data and have higher reputation; malicious users often report false detection data so that have very low reputation.

The reputation value of each sensor is defined as:

$$reputation[i] = \frac{correct\_response[i]}{response[i]} \tag{1}$$

Where correct_response[i] is the times of reporting correct sensing result, if fusion center's final decision is equal to the sensor i 's sensing result, we consider the sensing result is correct. Response[i] is the times of sensor i participating in the cooperative spectrum sensing, we consider that some sensors may not participate in cooperative spectrum sensing occasionally.

2)Reputation threshold calculation

The reputation threshold Φ is the key parameter for fusion center to distinguish honest users from malicious users, which is calculated by the following equation:

$$\phi = \frac{1}{CR\_size-2}\sum_{i=2}^{CR\_size-1} reputation[i] \tag{2}$$

Where CR_size is the number of sensors.

Here we use the trimmed mean of all sensors' reputation value. Trimmed mean is the average of the remaining values after removing the maximum value and minimum value in a set of data. This method removes the extreme values that affect the stability in a set of data, so it can have good robustness and is not easy to be affected by extreme factors.

3)The final decision

In this scenario, fusion center firstly distinguishes between malicious users and honest users by comparing their reputation value and threshold:

$$\begin{cases} Honest\ user\ , reputation[i] \geq \phi \\ Malicious\ user\ , reputation[i]\ < \phi \end{cases} \tag{3}$$

After determining whether the user is a malicious user, fusion center discards all sensing result from malicious users. Here, fusion center uses the "majority fusion rule" to process the honest users' sensing

DOI: 10.54254/2755-2721/2/20220616

result and make the final decision, which can be described by the following formula:

$$final\ decision \begin{cases} 1, \sum_i^{HU\_size} Sensing\_result[i] \geq \frac{HU\_size}{2} \\ 0, \sum_i^{HU\_size} Sensing\_result[i] < \frac{HU\_size}{2} \end{cases} \quad (4)$$

4)Implement

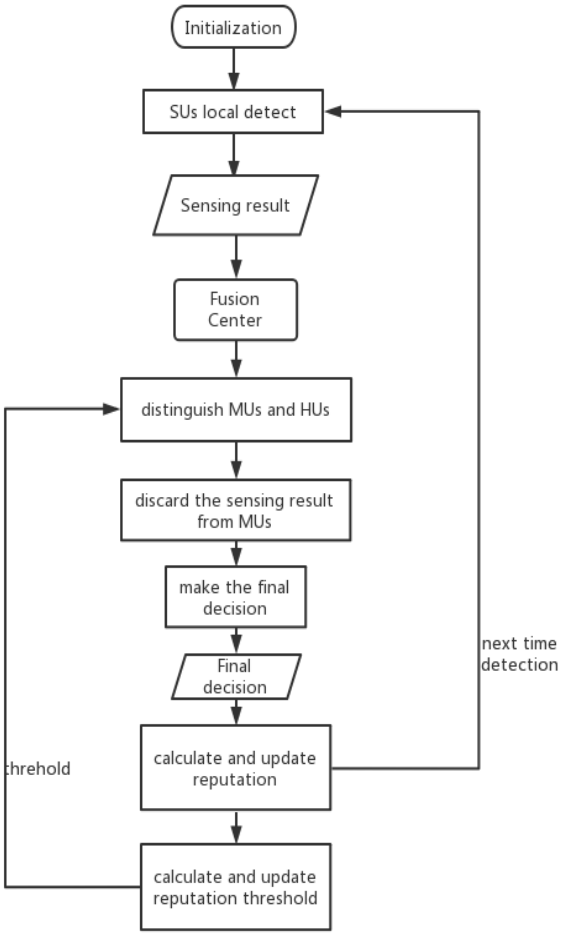

Figure 6. Flow chart of algorithm I.

Step 1: Initialization. We initialize some arrays to store the historical and updated value in each cycle detection.

Step 2: Local detection. Every sensor use pilot detection to obtain their own local detection result.

Step 3: Sending sensing result to fusion center. In this scenario, we suppose that the probability of attack is 85%(pa=0.85),and attack type is opposite reporting malicious attack, this is to say malicious users have the probability of 85% to tamper with their sensing results which are going to be sent to fusion center.

Step 4: Distinguish malicious users. Fusion center obtain the reputation value of each sensor and use formula (3) to distinguish them.

Step 5: Confusion and making the final decision by formula (4).

Step 6: Updating reputation value of each sensor and reputation threshold for the next cycle cooperative spectrum sensing.

Step 7: Repeat step2 to step7.

DOI: 10.54254/2755-2721/2/20220616

3.2. Reputation-weighted algorithm

In this scenario, the probability of attack is random and each malicious user's attack probability is not equal. So, there may be malicious users with low attack probability. In this circumstance, it is not wise for fusion center to discard all malicious users, because those with low attack probability can help cooperative spectrum sensing. More cognitive sensors can improve the detection probability of the system. In the following algorithm proposed, instead of discarding all malicious users, fusion center give corresponding weight factor according to their reputation during data confusion.

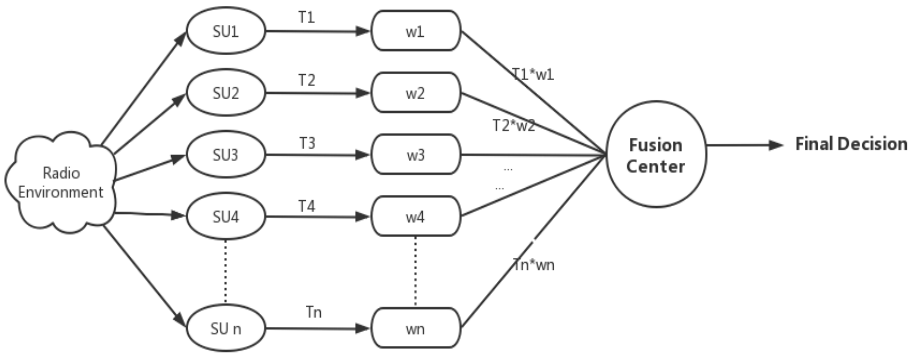

Figure7. Weight-based cooperative spectrum sensing model.

Where SU is secondary user,Ti is local detection data,wi is the weight factor for each secondary user.

1)Weight factor calculation

The weight factor is the key of this algorithm. We use the following formula to calculate the reputation to get the weight factor.

$$w[i] = \frac{reputation[i]}{\sqrt{\sum_{i=1}^{CR\_size} reputation[i]^2}} \tag{5}$$

meeting the condition that ||w||=1

The denominator of this formula sums the squares of all sensors' reputation and then extract a root,this is to find the modulus of the reputation vector.

The weight factor of each node is the value of their own reputation divided by the reputation vector modulus. Finally we can meet the condition that modulus of weight factor vector is equal to one, it makes sense when meeting this condition.

2)Data confusion and the final decision

In this algorithm, fusion center no longer needs to identify malicious user and discard them. Fusion center adopts the method of linear weighting for data fusion, it uses the calculated weight factor corresponding to each sensor W_i to linearly weight the local detection statistics T_i of each sensor, T_i is multiplied by the wi and then accumulates them, then we can get the fusion center detection statistic $\bar{T}$shown in the following formula:

$$\bar{T} = \sum_{i=1}^{CR\_size} W[i]T[i] \tag{6}$$

The final decision can be decided as:

$$fianl\ desision \begin{cases} PU\ is\ present, \bar{T} \geq \lambda \\ PU\ is\ absent, \bar{T} < \lambda \end{cases} \tag{7}$$

DOI: 10.54254/2755-2721/2/20220616

3)Implement

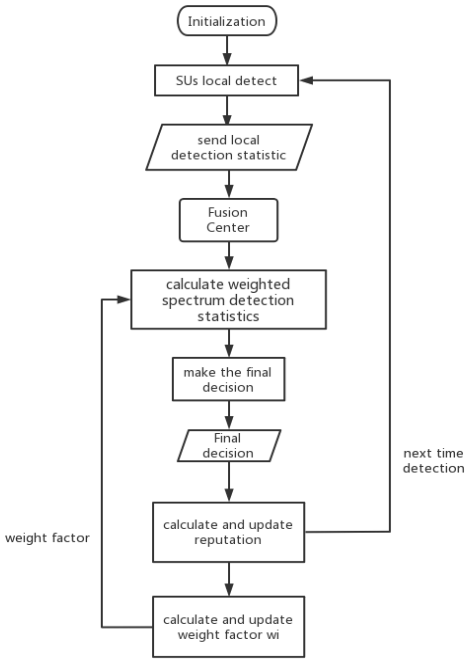

Figure 8. Flow chart of algorithm II.

Step 1: Initialization. We initialize some arrays to store the historical and updated value in each cycle detection.

Step 2: Local detection. Every sensor use energy detection to obtain their own local detection result. Step 3: Sending local detection statistic T_i to fusion center. In this scenario, we suppose that the probability of attack is random .

Step 4: Confusion. Fusion center obtain the weight factor value of each sensor and use formula to get the final detection statistic $\overline{T}$.

Step 5: Making the final decision by formula(7).

Step 6: Updating reputation value of each sensor and weight factor value for the next cycle cooperative spectrum sensing.

Step 7: Repeat step2 to step7.

4. Experiments and results

In the system model part, we successfully created a system which contains primary users, malicious users, Channel, Cognitive radios and fusion center models. After these models are generated, we can apply algorithms

4.1. The effectievness of the first algorithm

In the Algorithm and Implementation part, we set up Radio environment and the result shows that compare to the normal cooperative Spectrum Awareness algorithm (without reputation). When we have massive Mu and large probability of attack (ratio=0.4, pa= 85%), Cooperative Spectrum Sensing Algorithm based on reputation, our first algorithm, performed better.

DOI: 10.54254/2755-2721/2/20220616

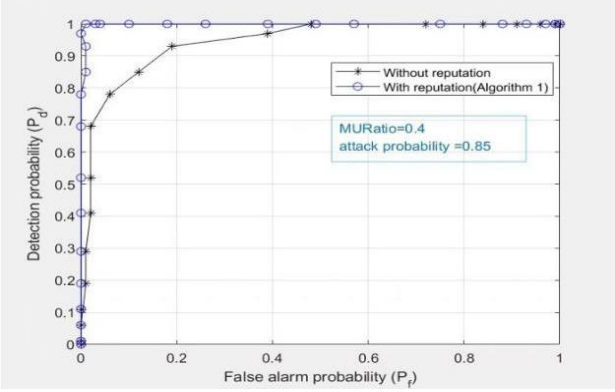

Figure 9. Comparison of results with and without the first reputation algorithm (attack probability is high,at 85%).

However, our algorithm is not perfect:

When the probability of attack is low (pa = 40% in our test) or the attack user is not that massive (ratio = 0.2 in our test), our first algorithm is not much different from the the normal cooperative Spectrum, and may be worse theoretically, because more sensors may improve Pd if MU are not screened out.

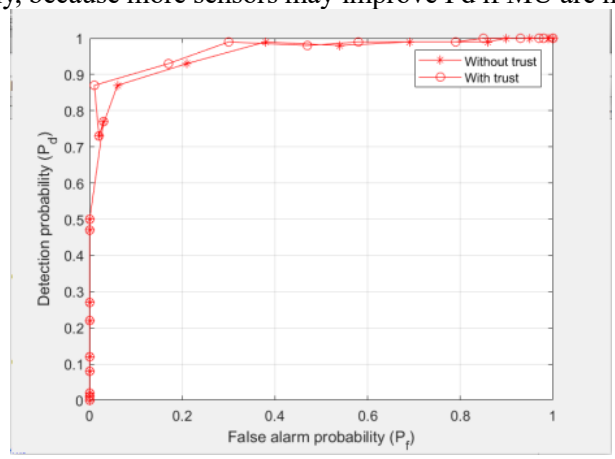

Figure 10. Comparison of results with and without the first reputation algorithm (attack probability is low, at 40%).

4.2. A way to improve

To solve this problem, we improved our first algorithm and enhanced it to the Reputation-weighted cooperative spectrum sensing algorithm, our second algorithm.

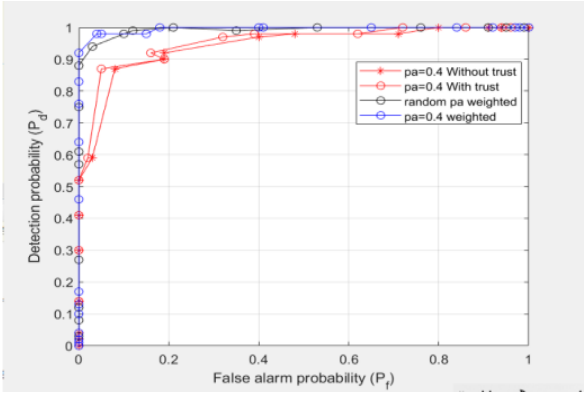

Figure 11. Comparison of results with and without the first reputation algorithm and reputation-weighted algorithm.

DOI: 10.54254/2755-2721/2/20220616

In the graph above we can notice that our second algorithm performed better in the comparison to other methods when the attack probability is relatively low (40%).

And in the graph below we can see that in a more harmful situation, which the posibility of attack is random, our algorithm which is trust-weighted has a greater advantage than those simply with or without trust.

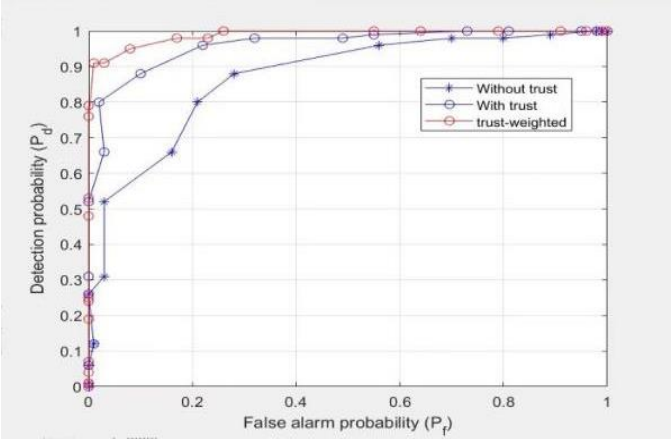

Figure 12. Comparison of two algorithms when the attack probability is random.

4.3. Current problems

Even though the Reputation-weighted cooperative spectrum sensing algorithm has shown obvious advantages, it still has some problems that cannot be neglected. As can be seen from the figure below, when the number of malicious users is small, the advantages of our new method are not obvious. Meanwhile, we only tested its ability to deal with non-cooperative attacks, and its defense ability against cooperative attacks is unknown.

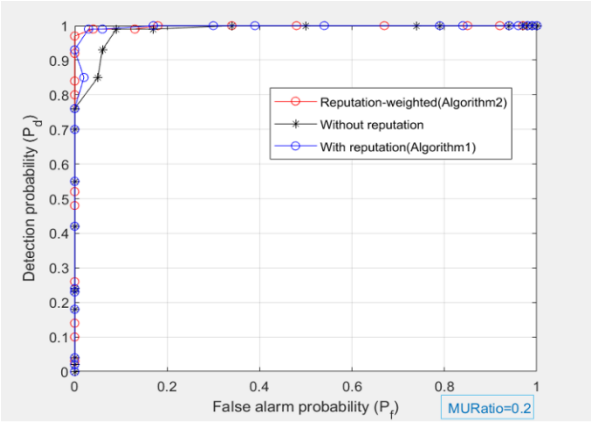

Figure 13. Comparison of two algorithms when the number of malicious users is small.

5. Conclusion

In this report, we propose a trust-based method and a reputation-weighted method to defense the SSDF attacks. The core idea of the algorithm is that we can selectively accept malicious users instead of shutting them out altogether. Our approach is tested in the presence of independent SSDF attacks. We compared the performance of our algorithm with the normal cooperative Spectrum Awareness algorithm. From the simulation results, our algorithm shows better results when facing the massive and aggressive attacks. However, when the number of malicious users is low, our algorithm did not show the superiority. We're going to refine our work on the current algorithms for non-cooperative attacks and produce an algorithm that can deal with cooperative attacks.

DOI: 10.54254/2755-2721/2/20220616

Acknowledgement

Authors of the Project Report (In alphabetical order):

Lyu Xiaoming/Iris contributed to the state-of-art research and summary. The first part of the report: introduction to the SSDF attack and the our approach.

Shenshu Qi/Luna contributed the research and compilation of algorithms against two kinds of attackers, simulate and compare the algorithm results. The third part of the report: algorithm and implement.

Songliang Yu/Andrew contributed to the experimental architecture, user model and channel model. The second part of the report: the compilation of system model and the control and coordination of project progress.

Yujie Cao/ Oliver contributed to the result analysis and conclusion. The forth part and fifth part of the report: Experiments and results, and conclusion and future work.

References

[1] Li, Husheng, and Zhu Han. "Catching attacker (s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach." 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN). IEEE, 2010.

[2] Li, Li, Fangwei Li, and Jiang Zhu. "A method to defense against cooperative SSDF attacks in Cognitive Radio Networks." 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013). IEEE, 2013.

[3] IEEE Std 802.11ax™-2021 (Amendment to IEEE Std 802.11-2020). “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 1: Enhancements for High Efficiency WLAN.” IEEE Standard for Information technology — Telecommunications and information exchange between systems. Local and metropolitan area networks — Specific requirements.

[4] Jianhan, L., Ron, P. et al. TGax Channel Model. IEEE 802.11-14/0882r4, September 2014.

[5] Kermoal, J. P., L. Schumacher, K. I. Pedersen, P. E. Mogensen, and F. Frederiksen. “A Stochastic MIMO Radio Channel Model with Experimental Validation.” IEEE Journal on Selected Areas in Communications. Vol. 20, No. 6, August 2002, pp. 1211–1226.

[6] Terry, J., and J. Heiskala. OFDM Wireless LANs: A Theoretical and Practical Guide. Indianapolis, IN: Sams, 2002.

[7] D. Cabric, A. Tkachenko and R. W. Brodersen, "Spectrum Sensing Measurements of Pilot, Energy, and Collaborative Detection," MILCOM 2006 - 2006 IEEE Military Communications conference, 2006, pp. 1-7, doi:10.1109/MILCOM.2006.301994.

[8] Li, Li, Fangwei Li, and Jiang Zhu. "A method to defense against cooperative SSDF attacks in Cognitive Radio Networks." 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013). IEEE, 2013.