Al-Mukhtar Journal of Sciences 36 (2): 129-134, 2021

Cognitive Radio Networks Based on Users' Reputation Scheme

Mahmoud A. Ammar[1*] and Salahedin A. Rehan[2]

[1]*Department of Computer Engineering, University of Zawia, Zawia, Libya*
[2]*Department of Electrical and Electronic Engineering, University of Zawia, Zawia, Libya*

Received: 02 February 2021/ Accepted: 04 April 2021
Doi: https://doi.org/10.54172/mjsc.v36i2.35

Abstract: Cognitive Radio (CR) can be defined as a technology that allows users to change the transmission parameters as required to increase the spectrum efficiency. Because of this mechanism, some threats emerge. Two major threats are found in CR. The first is the Primary User Emulation Attack (PUEA), where the attacker is able to transmit at a forbidden time slot effectively, emulating the signals of the primary user. This makes all the system users believe that the spectrum is occupied by a good primary user. The second threat is known as the spectrum sensing data falsification attack (SSDF). In this case, the attackers send false observation information, intentionally or unintentionally, to the fusion center (FC), causing it to make the wrong decision. In this study, the scheme presented was based on a users' reputation for secure spectrum access in cognitive radio networks. Each Secondary User (SU) performs local sensing and then forwards the sensing results to the main fusion center FC. The FC makes the final decision about the presence of the primary user based on the proposed approach. The schemes substantially reduce the effect of cognitive users with low reputation values while improving the impact of cognitive users with the high reputation values on the final decision. It has been verified that the proposed approach can improve the sensing performance under the impact of a different number of reliable and unreliable users in a CR network. Results based on simulation show that the proposed scheme outperforms the traditional majority scheme despite a high number of malicious users.

Keywords: Cognitive Radio CR; Users' Trust; Primary User; Primary User Emulation Attack (PUEA); Cooperative Spectrum Sensing.

INTRODUCTION

Spectrum sensing and spectrum sharing are important functionalities of CR, which enables the secondary users to monitor the frequency spectrum and detect vacant channels to use (Yadav et al., 2012). A procedure in the CR known as cooperation spectrum sensing involves many users that sense this spectrum and send reports to a base station known as a fusion center FC. The FC is able to process and manipulate those reports to make a final decision about the absence or presence of primary users. This kind of cooperation gives a chance to some adversary nodes that aim to falsify the results of the sensing (Pawelczak et al., 2006).

The disadvantages of cooperation spectrum sensing that compromise and limit the cooperation outcome are the control channel bandwidth, consumption of the energy, and reporting delay. Malicious users presented in the cooperation system will decrease the overall system performance (Cabrić et al., 2005; Zhao, 2007).

There are some previous contributions related to this work. For example, a method known as clustering and soften hard combination is

***Corresponding Author:** Mahmoud Ali Ammar m.ammar@zu.edu.ly, Department of Computer Engineering, University of Zawia, Zawia, Libya

presented to perform a significant trade-off between the overhead saving and performance increase. The cluster cooperative spectrum sensing has some disadvantages, such as in the case when the SUs that have good location correlation are grouped into the same cluster in order to decrease the consumption of the energy for data transition to the cluster-head CH. So, it is very likely that many SU within a cluster can be affected by shadowing or attacker's distribution. Hence CH may take incorrect group decisions about the primary's user availability and then send it to the fusion center misleading the final decision (Cabric et al., 2004; Yucek & Arslan, 2009). This paper uses both the terms 'trust' and 'reputation' to refer to the same meaning.

The mentioned problems are discussed in this paper and tackled by considering a reputation value for each user in the network, where the final decision is taken at the FC to increase the performance of the network. Based on this mechanism, the security of the cognitive network is improved by increasing the sensing performance.

COOPERATIVE SPECTRUM SENSING CHALLENGES

The challenge in cooperative spectrum sensing is to combine the detections of many nodes that might have different sensing times and different sensing results to make accurate detection of the spectrum. This leads to the development of a powerful sharing algorithm for cooperative spectrum sensing crucial to increase the detection performance in cognitive radio networks. A strong and smooth CR communication that combats malicious behaviors of users, trust management is important for SUs to assess the trustworthiness of users (Tkachenko et al., 2006; Yucek & Arslan, 2009).

R_i (reputation values) are performed by the FC and these values represent the trustworthiness for the i^{th} CR user based on local sensing difference D_i, sensing location factor P_i, and control channel condition Ci. This targets to reduce the impact of malicious CR users on the final fusion decision and improve the performance of cooperative spectrum sensing in CR networks. These values reduce the effect of cognitive users with low reputation values while increasing the impact of cognitive users with the high reputation values on the final decision.

CR SIMULATED NETWORK STRUCTURE

The scenario of the simulated CR network is presented in Figure 1. The network consists of:

- A number of good cognitive users (secondary users).
- A number of malicious users (attackers).
- A Fusion Center FC. The main task of the FC is to use the reports sent from the good and malicious users to decide on whether the primary user is present or not (Dutta & Arora, 2018).

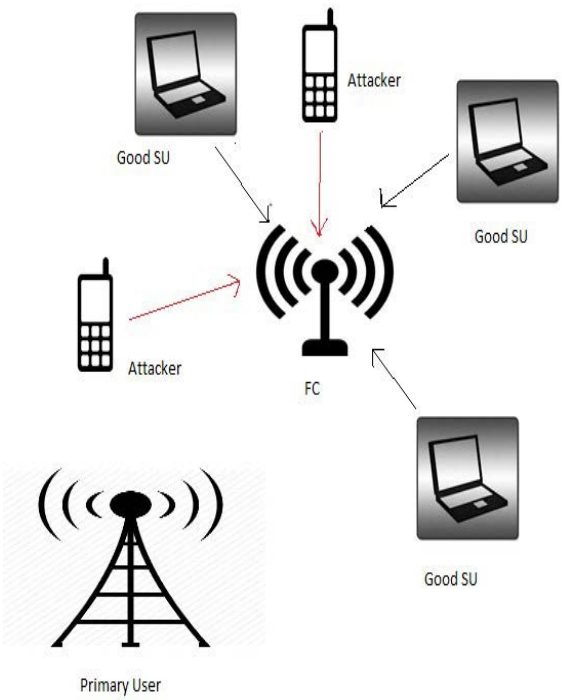

Figure (1). Cognitive radio simulated model

ISSN: online 2617-2186 print 2617-2178

USERS' REPUTATION PROCEDURE

The reputation scheme makes a final decision about the presence of malicious users based on both the users' reputation values and the number of users, rather than the number of users alone. The algorithm in this scheme considers that highly trusted users contribute more to the final decision in order to make more accurate sensing. This approach presents a flexible reputation model for distributed cooperative spectrum sensing against malicious users by benefiting from the users' reputation that describes the behavioral characteristics of both malicious and good users. The algorithm is shown below. Each user has a different weight (reputation) depending on the type of CU. Good CUs are assigned with higher weights. Users with a reputation value over a predefined threshold are considered reliable users (good users).

Two hypotheses are presented in this work. If the primary user is present (H_1) or not present (H_0).
Some variables used in this algorithm are as follows:
L_{di} =Local decision of user i
N = The number of Secondary Users

MODEL ALGORITHM BASED ON USERS' REPUTATION SCHEME

The following algorithm represents the main steps of the proposed approach:
Begin
R_i = Reputation of user i, λ Threshold of trustworthiness
L_{di} = Local decision of user i
if L_{di} = 1 spectrum is occupied
if L_{di} = -1 spectrum is unoccupied
R_i , i=1: to N
For i =1: to N do
If R_i >= λ then
User i is a reliable SU
Add user i to reliable SU list
Else User i is a malicious user
Add user i to Malicious users' list
End if
End for
For i=1: to N do
Take a final decision according to the equation below

$$decision = \begin{cases} H_1 \ \ if \ \sum_{i=1}^{N} L_{di} \ \ R_i > 0 \\ H_0 \ \ if \qquad otherwise \end{cases}$$

End for

RESULTS AND DISCUSSION

MATLAB Program is used to simulate and test the proposed algorithm. First, it is important to compare our proposed scheme with the traditional majority scheme that takes the final decision based on a majority vote. Figure 2 shows the maximum number of malicious users the CR network can tolerate to make a correct decision based on the traditional scheme.

It's clear that in the traditional majority scheme, the maximum number of malicious users does not exceed 50% of all users. Thus, it is vital to design a procedure that can tolerate more malicious users in the network to make better decisions regarding the presence of the primary user.

Additionally, results based on our proposed scheme are presented. Let the reputation value of good SUs be denoted by α, and let the reputation value for malicious users be denoted by β. M is the total number of users, and finally, K is the number of malicious users.

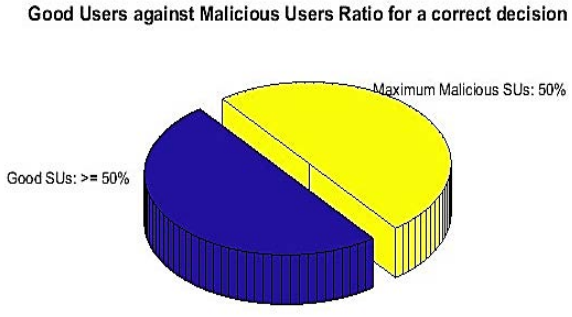

Figure (2). Users' ratio based on conventional role

ISSN: online 2617-2186 print 2617-2178

Figure 3 shows the relationship between M and K. α and β in this case are chosen to evaluate the network under low-value parameters (α=0.6 and β=0.2). It's crucial to check how many malicious users the network can tolerate. For example, from figure 3, if the total number of users M is 29, it's found that the maximum number of malicious users the system can tolerate to make a correct decision is 22, which means there are only 7 good users who were able to make a correct sense.

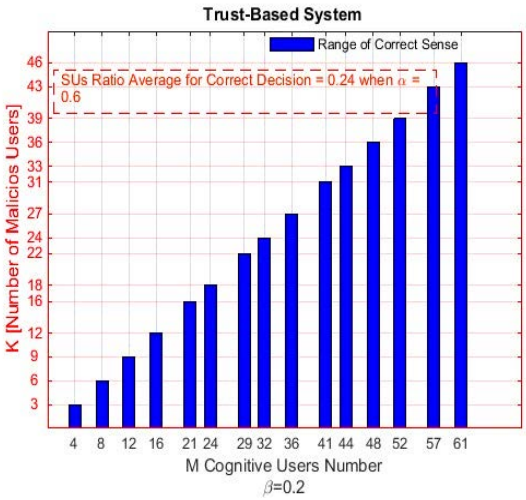

Figure (2)، Users number when α=0.6 and β=0.2

It is clear from figure 3 that the ratio of good SUs the system needs to make a correct sense is at least 24% of all users. This means that the system can tolerate about 76% of malicious users. Figure 4 shows the good users' ratio when α=0.6 and β=0.2 based on the proposed algorithm.

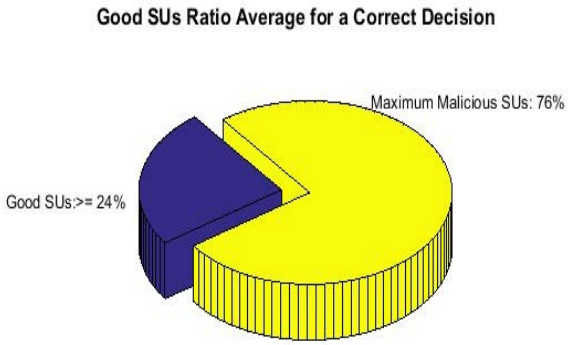

Figure (4). Users' ratio based on proposed trust approach

CONCLUSION

This paper has studied and focused on the users' trust mechanism because the users' trustworthiness is a crucial factor in the CR detection system. CRNs have a unique security problem that is not faced by a conventional wireless network. The main objective of any preventive security mechanism is to reduce and eliminate the impact of some operations performed by adversary users.

The proposed scheme outperforms the traditional majority scheme in terms of malicious user toleration. In fact, the traditional majority scheme can tolerate only about 50% of all users to make a correct decision while in the reputation-based scheme the system can tolerate about 76% of malicious users to make a correct final decision.

ACKNOWLEDGEMENTS

First and foremost, we would like to thank our departmental staff at the engineering faculty for the insightful guidance, advice, and encouragement over the years. Our sincere gratitude to all academics and colleagues within our research group.

We are also so grateful to all those people who have supported us and had contributions in making this work possible. My utmost thanks to the engineering faculty staff and Zawia University in general for the valuable suggestions and support.

Finally, we wholeheartedly thank our great families and friends for their understanding, encouragement, and support.

REFERENCES

Cabric, D., Mishra, S. M., & Brodersen, R. W. (2004). Implementation issues in spectrum sensing for cognitive radios. Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.,

ISSN: online 2617-2186 print 2617-2178

Cabrić, D., Mishra, S. M., Willkomm, D., Brodersen, R., & Wolisz, A. (2005). A cognitive radio approach for usage of virtual unlicensed spectrum. 14th IST mobile and wireless communications summit,

Dutta, S., & Arora, K. (2018). Review On Cognitive Radio.

Pawelczak, P., Janssen, G. J. & ،Prasad, R. V. (2006). WLC10-4: Performance measures of dynamic spectrum access networks. IEEE Globecom 2006,

Tkachenko, A., Cabric, D., & Brodersen, R. (2006). Experimental study of spectrum sensing based on energy detection and network cooperation. Proc. 1st Int. Workshop on Technol. and Policy of Spectrum Sensing TAPAS 2006,

Yadav, P., Chatterjee, S., & Bhattacharya, P. P. (2012). A survey on dynamic spectrum access techniques in cognitive radio. *International Journal of Next-Generation Networks* .27 ،(4)4 ،

Yucek, T., & Arslan, H. (2009). A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE communications surveys & tutorials*, *11*(1), 116-130.

Zhao, Q. (2007). Sadler, BM: A survey of dynamic spectrum access. *IEEE Signal Process. Mag*, *24*(3), 79-89.

ISSN: online 2617-2186 print 2617-2178

شبكات الراديو المعرفية المعتمدة على ثقة المستخدمين

محمود علي عمار[1*] وصلاح الدين عبد الرزاق ريحان[2]

[1]قسم الحاسوب، كلية الهندسة، جامعة الزاوية، ليبيا

[2]قسم الهندسة الكهربية والإلكترونية، كلية الهندسة، جامعة الزاوية، ليبيا

تاريخ الاستلام: 02 فبراير 2021 / تاريخ القبول: 04 أبريل 2021

Doi:https://doi.org/10.54172/mjsc.v36i2.35

المستخلص: يمكن تعريف شبكات الراديو المعرفية الذكية المعروفة بـ Cognitive Radio (CR) بأنها تقنية تسمح للمستخدمين بتغيير بيانات الإرسال على النحو المطلوب لزيادة كفاءة التردد. هذه الآلية تنتج بعض التهديدات الأمنية، هناك هجومان رئيسيان فيCR ، الأول هو هجمات محاكاة المستخدم الأساسية Primary User Emulation Attack (PUEA) حيث يكون المهاجم غير الآمن، والمسمى بغير الشرعي قادرًا على الإرسال في فترات زمنية محظورة بحيث يحاكي بشكل فعال إشارات المستخدم الأساسي الشرعي مما يجعل جميع المستخدمين في النظام يعتقدون أن التردد مشغول من قبل مستخدم أساسي شرعي. والهجوم الثاني المعروف بهجمات تزوير بيانات استشعار التردد Spectrum Sensing Falsification Attack (SSDF) حيث يرسل المهاجمون معلومات استشعارية خاطئة قد تكون عن قصد، أو عن غير قصد إلى مركز الاندماج الرئيسي Fusion Center (FC) وهذا يجعل FC يتخذ قرارا خاطئا.في هذا العمل ، تم تقديم مخطط يستند إلى سمعة المستخدمين للوصول الآمن إلى التردد في شبكات الراديو المعرفية. يقوم كل مستخدم ثانوي (Secondary User SU) باستشعار محلي، ثم يقوم بإعادة توجيه نتائج الاستشعار إلى مركز الاندماج الرئيسيFC ، لذلك يتخذ FC القرار النهائي بشكل جماعي بشأن إذا ما كان التردد مشغولا من قبل مستخدم شرعي، أو غير شرعي. تقلل هذه المخططات المقترحة في هذا العمل بشكل كبير من تأثير المستخدمين الإدراكيين ذوي قيمة السمعة المنخفضة، مع تحسين تأثير المستخدمين الإدراكيين ذوي القيمة العالية للسمعة على القرار النهائي. تم التحقق من أن هذا النهج المقترح يمكن أن يحسن أداء الشبكة تحت تأثير عدد مختلف من المستخدمين الموثوق بهم وغير الموثوق بهم في شبكة .CR تظهر النتائج المستندة إلى المحاكاة أن المخطط المقترح يتفوق على مخطط الأغلبية التقليدي على الرغم من وجود عدد كبير من المستخدمين الضارين في الشبكة.

الكلمات المفتاحية: الراديو المعرفي، ثقة المستخدمين، المستخدم الأساسي، هجوم محاكاة المستخدم الأساسي، الاستشعار عن التردد التعاوني.

*[1] محمود على عمار m.ammar@zu.edu.ly، قسم الحاسوب ، كلية الهندسة ، جامعة الزاوية ، ليبيا