Fuzzy logic based authentication in cognitive radio networks

Israa Nasir Abdulhussien, Safa Abdulridha Abduljaleel
General Directorate of Education in Al-Qadissiyah Governorate/Ministry of Education, Qadissiyah, Iraq

Article Info

Article history:

Received Jul 1, 2021
Revised Dec 26, 2021
Accepted Jan 20, 2022

Keywords:

Authentication
Cluster
Cognitive radio network
Fuzzy logic
Security

ABSTRACT

Security is a critical issue in cognitive radio networks because the cognitive node enters and variably leaves the spectrum, so it is difficult to process communication secretly. We suggested a fuzzy logic-based implicit authentication mechanism to be a solution for the confusion if there were any cognitive node doubts it to be unauthentic, and to improve user privacy in cognitive radio networks. Using a fuzzy logic technique, the proposed scheme computed certification based on proposed feedback. When a cognitive node needs to join the network, it is verified by using fuzzy logic if the node was authenticated or not. Our proposed fuzzy logic's results implicit authentication proved that it was a very successful and applicable scheme on cognitive radio networks, and it will be able to make an effective final decision in the context of incompleteness, ambiguity, and heterogeneity.

Corresponding Author:

Israa Nasir Abdulhussien
General Directorate of Education in Al-Qadissiyah Governorate/Ministry of Education
Qadissiyah, Iraq
Email: Ijmm2010@gmail.com

1. INTRODUCTION

Mitola and Maguire [1] was proposed the concept of cognitive radio for the first time. Mitola later characterized it in his doctoral dissertation as a novel technique for wireless communications [2] [3], [4]. Cognitive radio has two basic goals: extremely dependable communication whenever and wherever it is needed, and effective use of the radio spectrum [5], [6]. The main idea of the cognitive radio is that through the surrounding environment it can be learned and communicated to realize the available spectrum in space, as well as reduce and restrict the occurrence of conflict [7], [8]. A cognitive radio network (CRN) is also known as the unlicensed network, secondary network, or dynamic spectrum access network [9]. There are two categories of users in a CR network: primary users (PU) and secondary users (SU) [10], [11]. PUs have first access to channels. SUs are unlicensed users; therefore, when licensed users return, they vacate the spectrum. The SUs can use channels without interfering with the PUs [12]–[14].

Mobile station (MS), base station/access point (BSs/APs) and backbone/core networks are the three basic units of the CRN. These units are the fundamental components of the three architectures: Mesh, ad-hoc, and infrastructure architectures [15], [16]. In the Infrastructure architecture, a MS can only access a BS/AP in one hop manner. MSs under the transmission range of the same BS/AP shall communicate with each other through the BS/AP. Communications between various cells are routed through backbone/core networks [17], [18].

In an ad-hoc network, this kind of architecture does not depend on infrastructure support but it's set up on the fly. In mesh architecture, it is considered as a combination between infrastructure-based and ad-hoc architectures. MSs in Mesh CRNs act as relay nodes between their neighbors and the BS. MSs can either access the BSs/APs directly or use other MSs as multi-hop relay cognitive radio networks nodes [19]–[22]. In this paper, we focus on ad-hoc architecture. Decision-based on fuzzy logic and the way that a PU/SU makes this decision based on the information available from (authentication number, time, ID cluster) to make a final decision.

Fuzzy logic (or ambiguity reasoned) is one of the forms of logic, used in some expert systems and applications of artificial intelligence. The scientist Lotfi Zadeh from the University of California originated this logic in 1965 [23]. He developed it to use it as a better way to process data but his theory did not receive attention until 1974 [24], [25].

To deal with the issue of partial truth, fuzzy logic is a type of many-valued logic [26], [27]. Fuzzifier, inference rule, and defuzzifier make up the fuzzy logic controller FLC [28]–[30], it can reason and make reliable conclusions, and it makes the true decision if there any ambiguous [31], [32]. With the development of computers and software, we need inventor or program systems that could deal with inaccurate information similar to humans arose, but this created a problem as the computer can only deal with specific accurate data and it resulted. This approach is known as expert systems or artificial intelligence, and fuzzy logic is one of the theories by which such systems can be built [33].

In [34] solved a spectrum handoffs in cognitive radio networks if there was harmful interference from secondary user with a primary user by using a fuzzy logic system. The disadvantage of this approach is that it is not capable of maintaining recognition of illegitimate user activities that handoff this channel. In [35] proposed an authentication scheme based fuzzy logic system for mobile access control. It is capable of maintaining recognition of legitimate user activities. However, the main disadvantage of this scheme can not enable timely detection of adversary user behavior.

Because fuzzy logic is the main methodology used in this study, our proposed was efficacy, no obviously, needs no user intervention. The next part includes a brief discussion of the method as well as the underlying rationale for using it. Following that, each module will be describing and discussing in depth.

2. RESEARCH METHOD

The proposed system contains node A, node B, and cluster head. Node A, node B which be either a primary user or secondary user. The proposed system also represents a distribution of primary/secondary users in one cluster and each cluster is connected to a cluster as in Figure 1.

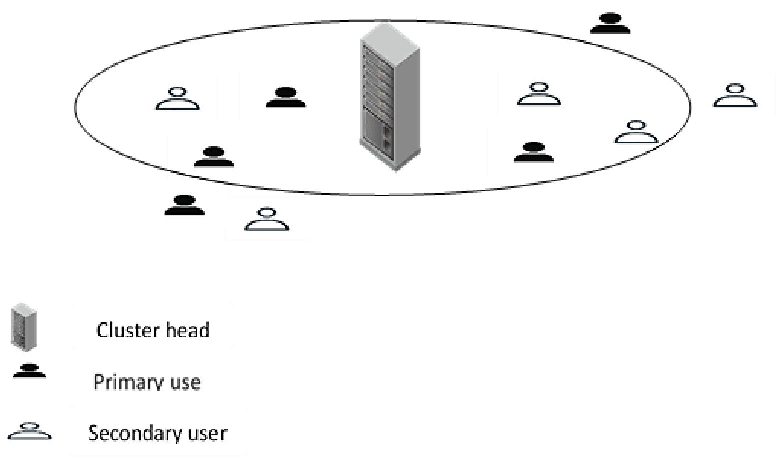

Figure 1. Show primary user, secondary user, and cluster head in one cluster

When node A (node A must be in the same cluster or from another cluster) sends a message to node B (node B must be in the same cluster. Node B sends a message to the cluster head that node A wants to communicate with it. The cluster head must verify if node A is authenticated or not. The cluster head checks if node A has authenticated number or not, here is the first check. The second checking from the timestamp of the message, and the decipher must be in the timestamp. If the decipher was out timestamp, then the user that sends the message doubts it to be unauthorized. The last checking from the ID node, which verifies from node A if it has an ID cluster or not. The three checkups (authenticate number, cipher message (timestamp), ID cluster) are entering into a fuzzy logic system to make the final decision if node A authenticated or not. In the proposed trust system, we have approved the message's sender's integrity and accuracy. To do this, we used fuzzy logic. The system model is being as Figure 2.

Three inputs (authenticate number, cipher message (timestamp), ID cluster) are entering into the fuzzy logic system as shown in Figure 2 above. In a fuzzy logic system, the first step is called "fuzzification". In this stage, it converts the input to a set of ambiguous phrases. The ambiguous phrases are conducting as in the algorithm 1 and 2:

Algorithm 1: authenticate by Authenticate number and ID cluster
Input: Authenticate number, ID cluster
Output: AN=high or medium or low
if authenticate number = authenticate threshold and ID cluster =true Then
AN=high
else
If round(authenticate number)= authenticate threshold and ID cluster =true then
AN=medium
Else
if authenticate number<> authenticate threshold and ID cluster =false Then
AN=low
Discard message
Go to the next step

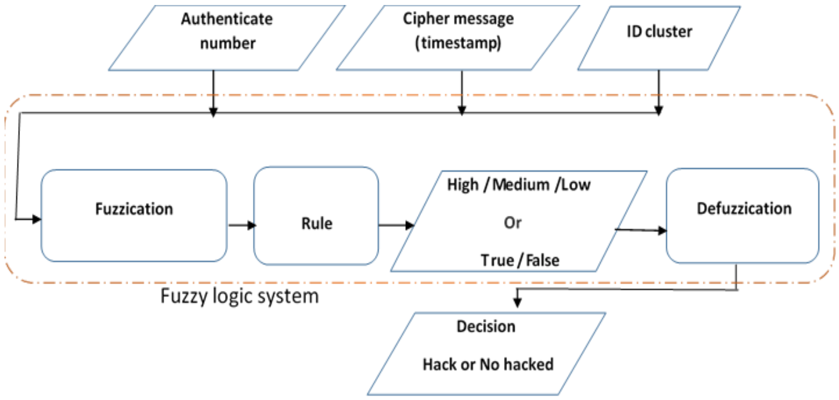

Figure 2. Shows a fuzzy logic diagram

The cluster head checks node A if it has an ID cluster to assign ambiguous phrases (true/false), if it has ID cluster assignment as true, otherwise ID cluster assignment as false. Authenticate threshold value is used to compare and give an ambiguous phrase either (high/medium/low). If the authenticate number and authenticate threshold are equal, it gives "high", and if the authenticate number and authenticate threshold are near, it gives "medium", and if it is not equal, it gives a" low". The results from the fuzzification stage of the algorithm 1 are high, medium, or low. Then, the cluster head sends a cipher message to node A to check if the decipher in timestamp or not as in the algorithm 2:

Algorithm 2: Authenticate by timestamps
Input: T send cipher, T decipher
Output: T1=high or medium or low
T dsr=Time stamp(T send cipher, T decipher)
T threshold = Time Extract threshold (cipher msg)
if T dsr = T threshold Then
T1=high
Else
if Round(T dsr)= T threshold then
T1=medium
Else
if T dsr > T threshold or T diff < T threshold Then
T1=low
Discard message
Go to next step

Where T dsr denotes the time difference between sending cipher message and decipher it. T threshold value is used to compare and give an ambiguous phrase either high or medium, or low. After T dsr and T threshold are computed, then the comparison process begins between T threshold and T dsr to give value to T1. The decision-making module depends on the authenticate number, T1, ID cluster, and rules as in Table 1. After giving ambiguous values to the proposed inputs in the system. Decision based on a fuzzy logic system. In particular, we propose to use fuzzy logic to deal with the incompleteness, uncertainty, and heterogeneity of a cognitive radio scenario, and fuzzy control to implement the decision making process in this kind of scenario.

Table 1. The performance of the rule matrix

Rule	AN	T1	ID cluster	Decision level
R1	High (H)	High (H)	True	No hack
R2	Medium (M)	High (H)	True	No hack
R3	Low (L)	High (H)	True	No hack
R4	High (H)	Medium (M)	True	No hack
R5	Medium (M)	Medium (M)	True	No hack
R6	Low (L)	Medium (M)	True	No hack
R7	High (H)	Low (L)	True	No hack
R8	Medium (M)	Low (L)	True	Hack
R9	Low (L)	Low (L)	True	Hack
R10	High (H)	High (H)	False	No hack
R11	Medium (M)	High (H)	False	No hack
R12	Low (L)	High (H)	False	Hack
R13	High (H)	Medium (M)	False	No hack
R14	Medium (M)	Medium (M)	False	No hack
R15	Low (L)	Medium (M)	False	Hack
R16	High (H)	Low (L)	False	Hack
R17	Medium (M)	Low (L)	False	Hack
R18	Low (L)	Low (L)	False	Hack

3. RESULTS AND DISCUSSION

The first phase of FLC is called “fuzzifier” which transfers input values into degrees of matching with linguistic values and it includes determine the membership functions of the income variables to detect the degree of truth in each rule. Membership function consider the performance of FLC. In the proposed model Three gaussmf type membership functions are employed with a 0.5 cross-point and uniformly distributed throughout the universe of discourse within a range of [0, 100]. The set of symbols {H, M, L, T, F} represent the fuzzy sets {high, medium, low, true, false}, respectively. Three fuzzy inputs (AN, T1, ID cluster) and the fuzzy output ”Decision” are using the same membership function type as in Figures 3, 4, 5, 6, the fuzzifed output values are then utilized to evaluate the rules to establish the sender's decision level.

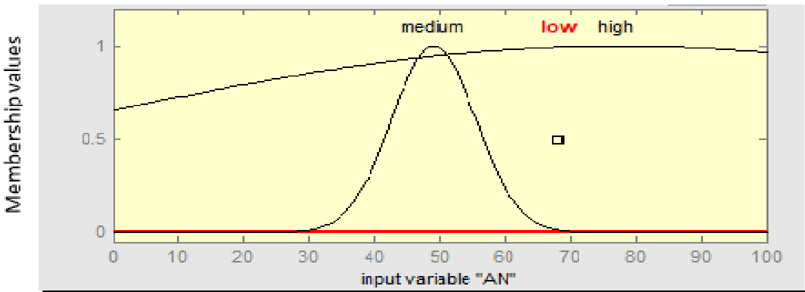

Figure 3. AN membership function

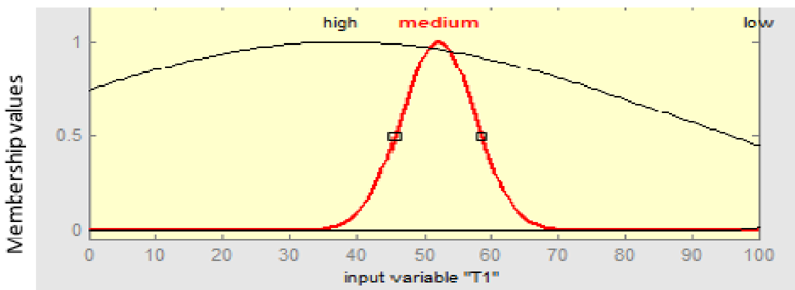

Figure 4. T1 membership function

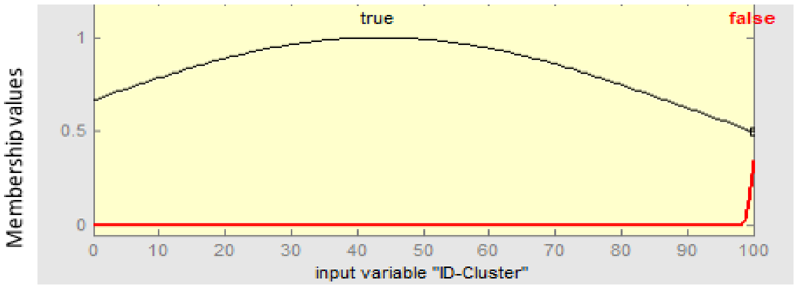

Figure 5. ID cluster membership function

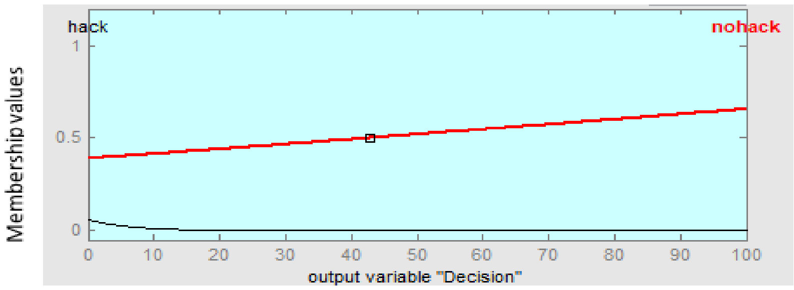

Figure 6. Decision membership function

The next phase of FLC is called the "Inference rule" which includes determining the result of each rule alone, and its inputs are the outputs of the previous step "fuzzifier". The outputs of this step are the inferred value of the outputs of each rule from the application of inference rules. As a result, in this FLC, 18 IF-THEN fuzzy rules are generated to refuse the decision level after the fuzzification stage as in Table 1

The IF-THEN linguistic rules are used to create a link between FLC inputs and outputs. Let the symbols α, β, φ, and € represent (AN, T1, ID cluster, and Decision level) respectively. Then, an example of a linguistic rule is given as (1).

$$IF\alpha \text{ is } A \text{ } AN \text{ } \beta \text{ is } B \text{ } AND \text{ } \varphi \text{ is } C \text{ } THEN \text{ €} \text{ is } D \quad (1)$$

The linguistic variables A, B, C, and D are denoted by the fuzzy sets high, medium, low, true, and false. The Mamdani inference approach, which is based on the min-type operator for implication and the max-type operator for aggregation, is utilized in this case. The fuzzy inference engine that is utilized to determine the "decision level" based on the rules of Table 1 above are shown in Figure 7.

The Figure 7 which represented 18 fuzzy rules in Table 1 based on linguistic values, for example R1 in Table 1, which is represented as: IF (AN is high AND T1 is high AND ID cluster is True) THEN decision level = no hack the decision comes from value which enter as (AN= 70-100, T1= 70-100, ID cluster=50-100) which it based on make decision. In Figure 8 shows a correlation between inputs (AN, T1, ID cluster) and output (decision level) of a fuzzy logic system based on enterd linguistic values and inference rule.

The final step of fuzzy logic is called "defuzzification" which converts the fuzzy result of all the rules recommended in the previous step to an integer that is not fuzzy and it determines the decision's value. In our model of the system, we used the centroid defuzzification approach for accounting in the defuzzificating stage. The following equation is using to calculate the centroid defuzzification technique.

$$Decsion\ level = \frac{\int x_i \cdot m(x_i)}{\int m(x_i)}$$

where
Decision level: the output that has been defuzzifed (it is the membership degree of output)
m(xi): the membership function that is aggregated
xi: the fuzzy value

A centroid defuzzification approach is used to convert the inference engine output to a crisp fuzzy output value. It based on a pre-defined membership function and this is the most widely used method, and it is fairly accurate. Finally, we show that the proposed system works accurately for determining if any doubt entry wants to enter the system. The system can decide that it is a hacker or not.

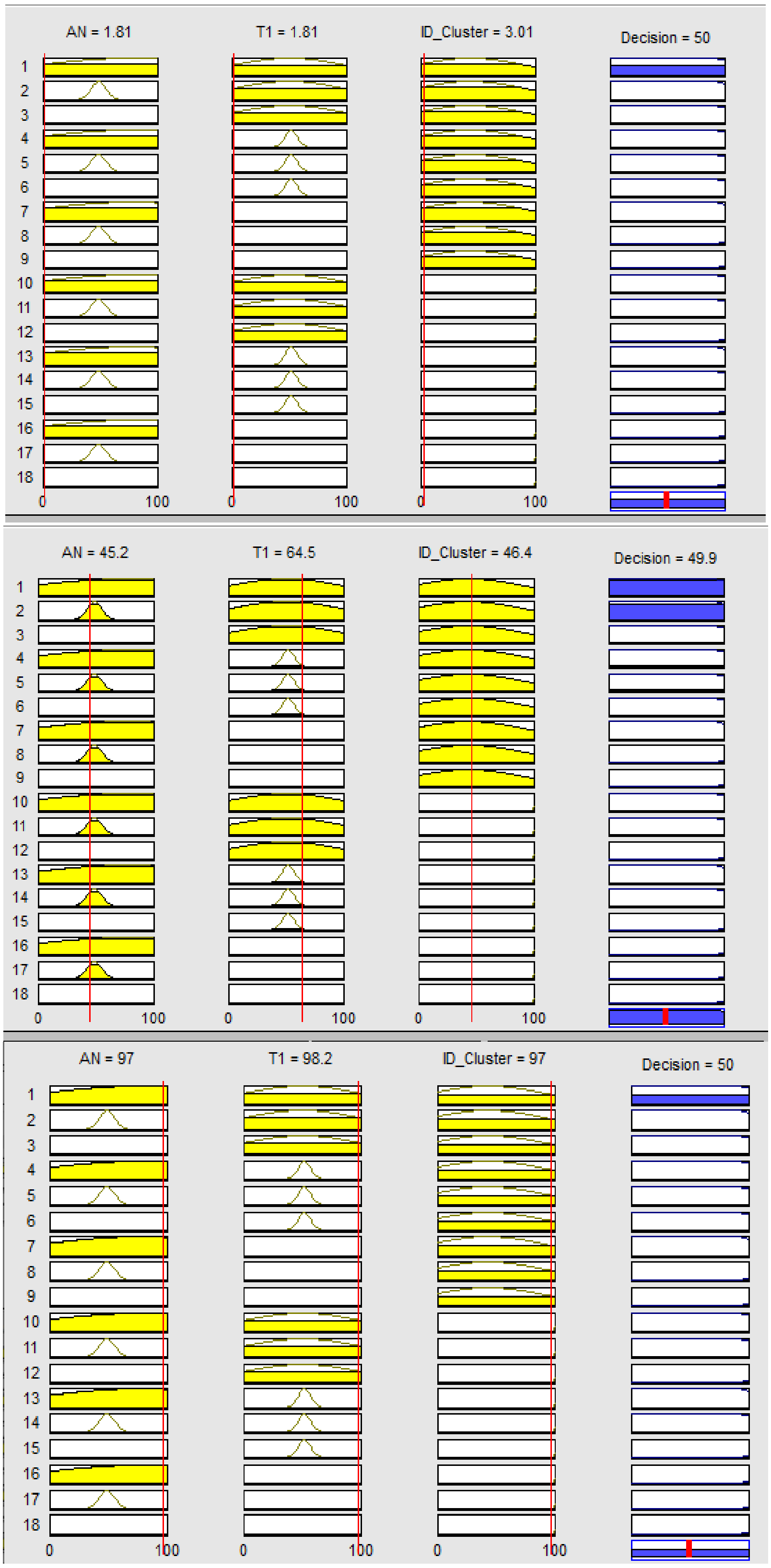

Figure 7. Fuzzy rule base

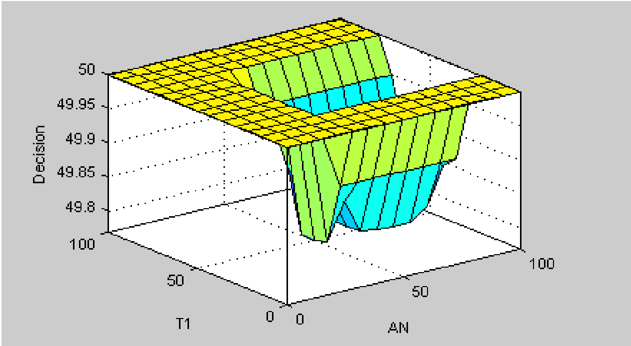

Figure 8. Correlation between inputs and output

4. CONCLUSION

The identification of security elements is a critical component of network maintenance. Since CRNs see authentication as a fundamental security characteristic that ensures protection from threats. In this paper, we propose a fuzzy logic-based implicit authentication strategy for CRNs to detect the user activity's trust state and to make the effective decision for the doubtable cognitive nodes to stay or leave the network.

Extensive experiments were conducted using real data from two users to determine the efficacy of the proposing authentication approach, which does not require user intervention, no obviously, and produces explicit authentication to avoid unwanted access, and also is characterized by simplicity, uncomplicated and a final decision making from ambiguous inputs is being effective, quick, and accurate. Based on the analysis of the experiments, it is possible and realistic to implement an intelligent access control technique using easily accessible everyday hack data and it is a very successful and applicable scheme on cognitive radio networks.

REFERENCES

[1] J. Mitola and G. Q. Maguire, “Cognitive radio: making software radios more personal,” *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999, doi: 10.1109/98.788210.
[2] J. Mitola, “Cognitive radio-an integrated agent architecture for software defined radio,” *Royal Institute of Technology (KTH)*, 2000.
[3] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, Feb. 2005, doi: 10.1109/JSAC.2004.839380.
[4] A. M. Wyglinski, M. Nekovee, and T. Hou, *Cognitive radio communications and networks: principles and practice*. Academic Press; 1st edition, 2009.
[5] E. Hossain, D. Niyato, and Z. Han, *Dynamic spectrum access and management in cognitive radio networks*. Cambridge: Cambridge University Press, 2009.
[6] Q. Mahmoud, *Cognitive networks: towards self-aware networks. John Wiley & Sons*. John Wiley & Sons, 2007.
[7] L. Tang and J. Wu, “Research and analysis on cognitive radio network security,” *Wireless Sensor Network*, vol. 04, no. 04, pp. 120–126, 2012, doi: 10.4236/wsn.2012.44017.
[8] M. Khasawneh and A. Agarwal, “A survey on security in cognitive radio networks,” in *2014 6th International Conference on Computer Science and Information Technology (CSIT)*, Mar. 2014, pp. 64–70, doi: 10.1109/CSIT.2014.6805980.
[9] I. F. Akyildiz, Won-Yeol Lee, M. C. Vuran, and S. Mohanty, “A survey on spectrum management in cognitive radio networks,” *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40–48, Apr. 2008, doi: 10.1109/MCOM.2008.4481339.
[10] N. Kaabouch and W. Chwn, *Handbook of research on software-defined and cognitive radio technologies for dynamic spectrum management*. IGI Global, 2015.
[11] A. Khattab, D. Perkins, and M. Bayoumi, *Cognitive radio networks: from theory to practice*. Springer, 2013.
[12] P. Varzakas, “Estimation of radio capacity of a spread spectrum cognitive radio Rayleigh fading system,” *Proceedings of the 17th Panhellenic Conference on Informatics - PCI ’13*, 2013, doi: 10.1145/2491845.2491854.
[13] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, “On the security of cognitive radio networks,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3790–3795, Aug. 2015, doi: 10.1109/TVT.2014.2358624.
[14] T. M. Salem, S. M. A. El-Kader, S. Abdel-Mageid, and M. Zaki, *Cognitive networks: applications and deployments*, v1 ed. CRC Press, 2014.
[15] K.-C. Chen and R. Prasad, *Cognitive radio networks*. John Wiley & Sons, 2009.
[16] Z. I. A. M. Ahmed, K. H. Bilal, and M. M. Alhassan, “Cognitive radio network review,” *International Journal of Engineering, Applied and Management Sciences Paradigms*, vol. 35, no. 1, pp. 19–26, 2016.
[17] K.-C. Chen, Y.-J. Peng, N. Prasad, Y.-C. Liang, and S. Sun, “Cognitive radio network architecture: part I--general structure,” in *Proceedings of the 2nd international conference on Ubiquitous information management and communication - ICUIMC ’08*, 2008, pp. 114–119, doi: 10.1145/1352793.1352817.
[18] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, “Cognitive radio network security: a survey,” *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1691–1708, Nov. 2012, doi: 10.1016/j.jnca.2012.06.006.
[19] M. Dipobagio, “An overview on ad hoc networks,” Inst. Comput. Sci. (ICS), Freie Univ. Berlin, 2009.
[20] N. Meghanathan and Y. B. Reddy, *Cognitive radio technology applications for wireless and mobile ad hoc networks*. IGI Global, 2013.
[21] F. R. Yu and H. Tang, *Cognitive radio mobile ad hoc networks*. New York, NY: Springer New York, 2011.

[22] A. Popescu, *Cognitive radio networks: elements and architectures*. Blekinge Institute of Technology, 2014.
[23] B. Sarwar, I. Bajwa, S. Ramzan, B. Ramzan, and M. Kausar, “Design and application of fuzzy logic based fire monitoring and warning systems for smart buildings,” *Symmetry*, vol. 10, no. 11, Nov. 2018, doi: 10.3390/sym10110615.
[24] L. A. Zadeh, “Is there a need for fuzzy logic?,” *Information Sciences*, vol. 178, no. 13, pp. 2751–2779, Jul. 2008, doi: 10.1016/j.ins.2008.02.012.
[25] A. Almeida and D. López-de-Ipiña, “Assessing ambiguity of context data in intelligent environments: towards a more reliable context managing system,” *Sensors*, vol. 12, no. 4, pp. 4934–4951, Apr. 2012, doi: 10.3390/s120404934.
[26] W. Pratiwi, A. Sofwan, and I. Setiawan, “Implementation of fuzzy logic method for automation of decision making of Boeing aircraft landing,” *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 10, no. 3, pp. 545–552, Sep. 2021, doi: 10.11591/ijai.v10.i3.pp545-552.
[27] W. Tang and D. Peng, “Spectrum handoff in cognitive radio with fuzzy logic control,” *Journal of Electronics (China)*, vol. 27, no. 5, pp. 708–714, Sep. 2010, doi: 10.1007/s11767-011-0507-y.
[28] M. F. Farhan, N. S. A. Shukor, M. A. Ahmad, M. H. Suid, M. R. Ghazaliv, and M. F. B. M. Jusof, “A simplify fuzzy logic controller design based safe experimentation dynamics for pantograph-cateary system,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 14, no. 2, pp. 903–911, May 2019, doi: 10.11591/ijeecs.v14.i2.pp903-911.
[29] A. N. Kasruddin Nasir, M. A. Ahmad, and M. O. Tokhi, “Hybrid spiral-bacterial foraging algorithm for a fuzzy control design of a flexible manipulator,” *Journal of Low Frequency Noise, Vibration and Active Control*, pp. 1–9, Aug. 2021, doi: 10.1177/14613484211035646.
[30] X. Li, H. Wen, Y. Hu, and L. Jiang, “A novel beta parameter based fuzzy-logic controller for photovoltaic MPPT application,” *Renewable Energy*, vol. 130, pp. 416–427, Jan. 2019, doi: 10.1016/j.renene.2018.06.071.
[31] S. A. Soleymani *et al.*, “A Secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing,” *IEEE Access*, vol. 5, pp. 15619–15629, 2017, doi: 10.1109/ACCESS.2017.2733225.
[32] T. Sarkar, R. Bhattacharjee, M. Salauddin, A. Giri, and R. Chakraborty, “Application of fuzzy logic analysis on pineapple rasgulla,” *Procedia Computer Science*, vol. 167, pp. 779–787, 2020, doi: 10.1016/j.procs.2020.03.410.
[33] F. Spagnolo, “Fuzzy logic, fuzzy thinking and the teaching/learning of mathematics in multicultural situations,” in *Proceedings Int. Conference. on Mathematics Education in the 21st Century*, 2003, pp. 17–28.
[34] L. Giupponi and A. I. Perez-Neira, “Fuzzy-based spectrum handoff in cognitive radio networks,” in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, May 2008, pp. 1–6, doi: 10.1109/CROWNCOM.2008.4562535.
[35] F. Yao, S. Y. Yerima, B. Kang, and S. Sezer, “Fuzzy logic-based implicit authentication for mobile access control,” in *2016 SAI Computing Conference (SAI)*, Jul. 2016, pp. 968–975, doi: 10.1109/SAI.2016.7556097.

BIOGRAPHIES OF AUTHORS

Israa Nasir Abdulhussien gets a master's degree in computer science from Iraq’s Kufa university in 2019 and works as a teacher in the Ministry of Education, Iraq. The researcher has many research articles that have been published, as well as research participation in conferences. Email of author is Ijmm2010@gmail.com.

Safa Abdulridha Abduljaleel holds a master's degree in computer science from Turkey's Atilim University and works in the Ministry of Education, Iraq. The researcher has many research articles that have been published, as well as research participation in conferences. Email of author is safa14.2014@gmail.com.