Scholar Publishing Group
Distributed Processing System
https://doi.org/10.38007/DPS.2022.030309
ISSN 2790-0916 Vol. 3, Issue 3: 72-81

Distributed System Access Control for Fuzzy Mathematics and Probability Theory

Kishita Naoko*

Univ Rennes, INRIA, CNRS, IRISA, Rennes, France

**corresponding author*

Keywords: Fuzzy Mathematics, Probability Theory, Distributed Systems, Access Control

Abstract: AC is to control and manage the access rights of legitimate users who enter the system on the basis of user identity authentication, so that the user's access rights are limited within the allowable range. It is an important part of information security technology. Implementing AC to users through technical means plays an important role in information security. The main purpose of this paper is to use fuzzy mathematics (FMs) and probability theory (PT) to study the access control (AC) of distributed systems (DS). This paper adds trust elements on the basis of the AC model, sets roles for each trust level, and sets a series of permissions for each role. The user determines the trust level to which he belongs by being judged by other users, and then obtains the corresponding authority through the role corresponding to the trust level. Experiments show that by evaluating the trust degree and the reputation value of user behavior, the ability of user trust degree and service and access behavior is greatly improved. Compared with the existing trust evaluation algorithm, it has a good correlation. At the same time, it satisfies the rule of "slow increase and sudden decrease" of the target change trust degree, which can effectively resist malicious users' phishing attacks, bleaching attacks, collusion attacks and other security attacks, and has higher security.

1. Introduction

The study of uncertainty mathematics is one of the mainstream directions of mathematics research today. Fuzzy sets and rough sets play an important role in uncertainty mathematics. Therefore, as basic models of information systems, they have important research value. With the advent of the era of big data, we are increasingly faced with complex and huge data in the information system. How to prune redundant data without changing the data structure, such as attribute reduction and decision rules, and how to mine potentially useful information is very important [1-2].

In a related study, Hafeez et al. proposed a method to detect faults from component-based system requirements during acceptance testing using fuzzy logic methods and historical information [3]. This approach identifies error-prone component selections for test case extraction and test case prioritization to validate components in acceptance testing. Empirical findings show that the proposed method is significantly superior in component selection and acceptance testing. Khan et al. introduced the types of relations on complex fuzzy sets and discussed the application of complex fuzzy (CF) relations in the futures commission market (FCM) [4]. The results show that the introduction of the CF relationship into the application of FCM can provide an important method for describing the time dependence between the parameters of the futures commission market.

This paper uses FMs and PT to study the AC of DSs. A subjective trust evaluation model based on fuzzy subset theory is proposed. Aiming at the characteristics of subjectivity and ambiguity of trust, fuzzy subsets in FMs are used to represent the level of trust. Using the fuzzy comprehensive evaluation method to quantitatively measure trust, a new type of fuzzy operator is defined to form a fuzzy relation matrix according to the factor set and evaluation set, and the trapezoidal function is used as the membership function to calculate the membership degree. According to the proposed theoretical model, a trust-based resource AC prototype system is designed and implemented. The system implements various algorithms proposed in the model and provides the functions of adding and accessing resources. Each user can set roles and permissions for his own resources, and the weight distribution of each factor of trust is also calculated by each user according to his own habits.

2. Design Research

2.1. The Principle of AC

Security is a relative concept, and the design of AC technology depends on the particularity of the protected environment [5-6].

To implement AC to an information system, first of all, it is necessary to thoroughly investigate and analyze the security requirements under the application background of the information system, such as organizational structure, number of users, task requirements, types, etc. What kind of service the user provides. On the basis of fully considering the security requirements, we design policies and rules to meet the security requirements. Only the access that meets the policies and rules can be allowed, and the access that violates the policies and rules is regarded as illegal access and will be prohibited.

One of the most important principles for AC is the "principle of least privilege", that is, what the user knows or what he does must be his job responsibilities and his identity and position in the information system to determine the operations he must have. The permissions assigned by the system to each user must be the minimum set of permissions required to complete the task, and must not be assigned to other permissions than the permissions required by the user to perform the task.

After the AC policy is determined, the system must implement the AC policy by completing three tasks: one is to authorize each user or some users according to the security policy of the system; the other is to identify and confirm the user when the user makes an access request, The third is to execute or reject the user's request according to the system's authorization and AC rules for the user. Generally speaking, AC mainly includes two aspects of authorization and control, and is carried out according to the security policy formulated in advance by the system [7-8].

2.2. Introduction to Traditional AC Model

(1) Discretionary AC Model (DAC)

DAC is based on the mapping relationship between identity and authority. In this chain structure, the upper-level authorizer only has the right to manage the lower-level permission acquirer, and there is no case of leapfrog management [9-10]. The basic architecture of the model is shown in Figure 1:

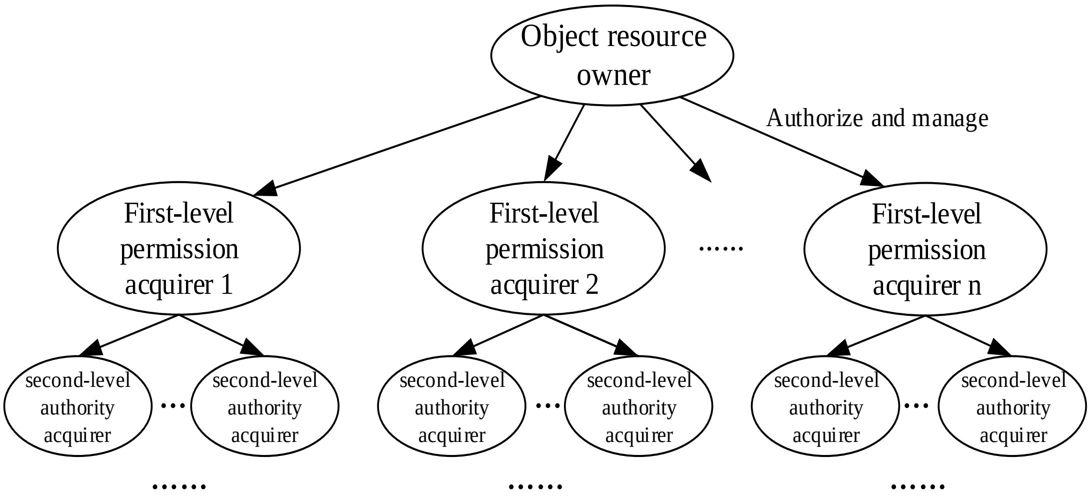
Object resource owner
Authorize and manage
First-level permission acquirer 1
First-level permission acquirer 2
......
First-level permission acquirer n
second-level authority acquirer
...
second-level authority acquirer
second-level authority acquirer
...
second-level authority acquirer
second-level authority acquirer
...
second-level authority acquirer
......
......
......

Figure 1. Basic architecture of the DAC model

Although this authorization mode greatly improves the distribution efficiency of object rights, it also reduces the management difficulty in the entire structural network. However, since the rights management is limited to the upper and lower levels, it is difficult for the owner of the object to control the rights acquired by nodes other than the nodes managed by itself. If a malicious node obtains resources through the third-level or lower authority owner, it will cause damage to the owner's rights and interests. In addition, the amount of permissions allocated depends on the owner, and each node has different permissions. With the increase in the complexity of the chain structure network, the management difficulty of the system administrator will increase infinitely, which will affect the efficiency of the system.

(2) Trust-Based AC Model (TBAC)

The TBAC model is based on the trust evaluation technology, and determines its trustworthiness by measuring the trust value of the node, and then grants the corresponding operation authority. In this type of model, the designer sets a unified permission control strategy, and any node can make an access request, but only nodes that reach a certain trust value can pass the strategy test and obtain resources [11-12]. The basic architecture of this model is shown in Figure 2:

This type of model supports unfamiliar users to access the system and has a unified control strategy, so the model has strong applicability and can effectively solve the AC problem of DSs. However, because trust is a subjective concept, it is difficult to quantify, and it is difficult to define grades, resulting in weak objectivity of most trust assessments, and it is difficult to evaluate the reliability and validity of models. Secondly, many studies are only based on one-way evaluation of user nodes, and there are few studies on the reliability of resource pools. Although the security of resources is guaranteed, the security of users themselves is ignored. In addition, many literatures only regard trust evaluation as a one-way process when building a model, without feedback and update, and the real-time performance of trust value is not guaranteed, so it is difficult to avoid the risk of accumulative trust node attacks.

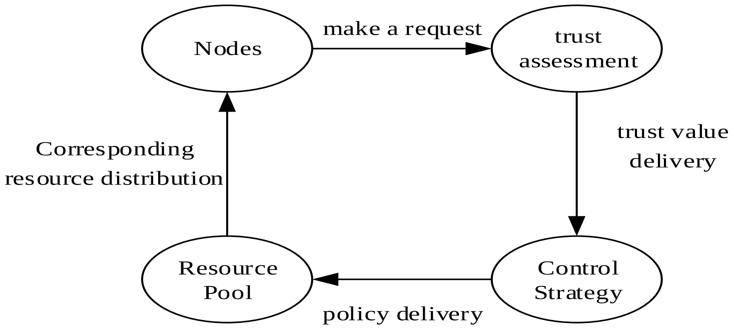

Figure 2. TBAC basic architecture

(3) Mandatory AC Model (MAC)

MAC is mainly used in high-level security control fields such as government and military. The basic idea of MAC is to identify the corresponding target objects by setting corresponding security attribute labels to the subject and object in the system. Among them, the label of the subject reflects the authority possessed by the node, and the label of the object reflects the security level of the resource [13-14]. In a system using this type of model, after the subject sends a request, the model will not only detect the subject's authority but also review the resource's security level, which belongs to a two-way control mode and achieves better protection of resources. The basic architecture of such a model is shown in Figure 3:

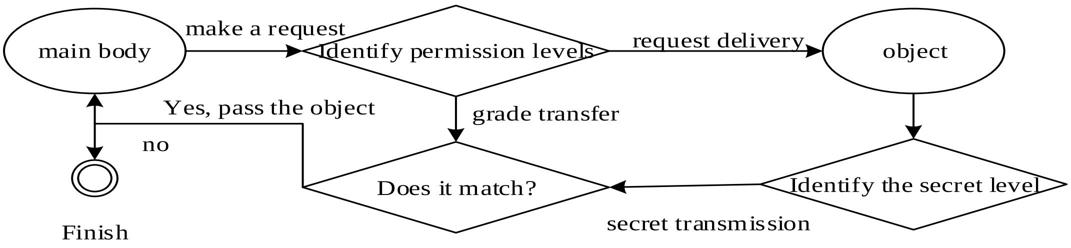

Figure 3. MAC Basic Architecture

MAC forces resources to flow in a specific direction by enforcing policies. Only when the subject authority level matches the object's security level, the resource request will be satisfied. A strict matching system will effectively prevent the leakage of sensitive information [15-16]. However, this kind of method needs to set labels for the nodes in the system in advance and match the matching system. With the increasing number of system nodes and the accumulation of the number of resources, it will bring problems to the system management. Furthermore, such methods are not suitable for general situations since only the subjects who have been assigned the level have access.

(4) Role-Based AC Model (RBAC)

RBAC is similar to MAC to a certain extent, that is, both have modules to obtain permissions based on the identity of the subject. Unlike MAC, TBAC sets the role of the access subject to avoid the subject directly corresponding to the permissions. The system only needs to Set the permissions corresponding to different roles and the number of resources under the corresponding permissions, and the subject can enter the identity for verification when accessing. This greatly simplifies the management work of the system administrator and reduces the system pressure caused by too many visitors. However, in this type of model, the user only needs to verify his identity to obtain the corresponding resources. When the user cannot obtain the desired information by using one role, he is likely to access it through another role to achieve his purpose, that is, this class The model is very vulnerable to Sybil attack. At the same time, the permissions corresponding to roles in the model are static and cannot change with the change of different conditions, so the model is less dynamic [17-18]. The basic architecture of RBAC is shown in Figure 4:

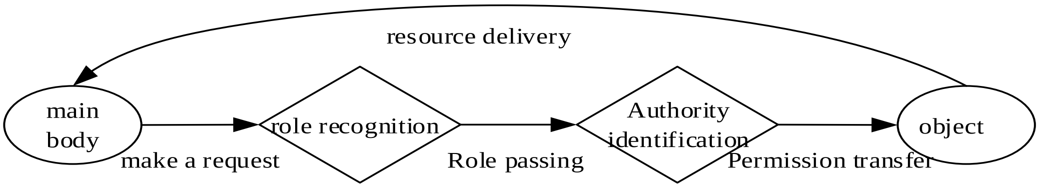

Figure 4. RBAC basic architecture

2.3. Algorithm Research

(1) Global trust value

Because trust is fuzzy and transferable, which is very consistent with the fuzzy relationship matrix in FMs, it can be used as an effective tool for trust analysis. The fuzzy relationship matrix uses a number between 0 and 1 to represent the strength of the relationship between elements, with 0 being irrelevant and 1 being strongly correlated. The fuzzy relation matrix representation is shown in Equation 4.11:

$$Frm = \begin{array}{c|cccc|} & e_1 & e_2 & \Lambda & e_m \\ e_1 & 1 & u_{12} & \Lambda & u_{1m} \\ e_2 & u_{21} & 1 & \Lambda & u_{2m} \\ \mathrm{M} & \mathrm{M} & \mathrm{M} & \mathrm{O} & \mathrm{M} \\ e_m & u_{m1} & u_{m2} & \Lambda & 1 \end{array} \qquad (1)$$

where e1, e2,...,em are the nodes in the system, and uij(i,j∈m) is the mutual trust value between node i and node j.

In the initial fuzzy relationship matrix, the interaction between a node and itself is considered to be a complete trust interaction relationship, and the trust value is 1. In addition, the mutual trust value between directly interacting nodes is equal to the mean value of the direct trust values of the two nodes, that is, if there is a direct interactive relationship between node a and node b, then uab=[D(a)+D(b)]/2.

The so-called transitive fuzzy relationship matrix means that there may be such a situation in the initial fuzzy relationship, there is a direct interaction relationship between ei and es, and there is also a direct interaction relationship between ej and es, but the difference between the two interval elements ei and ej is There is no direct interaction between them. The indirect trust value between ei and ej is calculated by using the transitivity of the fuzzy relationship. which is:

$$idt_{ij} = IDT(e_i, e_j) = \vee e_{K\in E}(Frm(e_i, e_k) \wedge Frm(e_k, e_j)), (i, j = 1, 2, \mathrm{K}, n) \qquad (2)$$

In addition, since the relationship data between nodes is constantly changing, in the process of fuzzy relationship transfer, the fuzzy relationship transfer closure theorem can be used to obtain the global fuzzy relationship matrix to avoid the possibility of overwriting the original relationship data due to new data. lead to distortion of real data. That is, Frm’=Frm∪(Frm2)∪(Frm^3)…(Frmn):

$$Frm' = \begin{array}{c} \\ e_1 \\ e_2 \\ M \\ e_m \end{array} \begin{array}{c} \begin{array}{cccc} e_1 & e_2 & \Lambda & e_m \end{array} \\ \begin{bmatrix} 1 & u'_{12} & \Lambda & u'_{1m} \\ u'_{21} & 1 & \Lambda & u'_{2m} \\ M & M & O & M \\ u'_{m1} & u'_{m2} & \Lambda & 1 \end{bmatrix} \end{array} \tag{3}$$

Here n can be adjusted according to the specific environment. Changing the value of n according to the actual environment can maximize the optimization of accuracy and time.

(2) Fuzzy sets and fuzzy relationships

Denote the universe of discourse U as a non-empty finite set, denote I=[0,1]. set

$$U = \{x_1, x_2, \ldots\ldots, \ x_n\} \tag{4}$$

Fuzzy sets are extensions of classical sets. A fuzzy set P on U is defined as a membership function from U to I, that is, each element x on U corresponds to a value P(x) on I, where P(x) represents the degree to which element x belongs to the fuzzy set P.

In this paper, we denote IU as all fuzzy sets on U. The potential of a fuzzy set P∈IU is defined as follows:

$$|P| = \sum_{i=1}^{n} P(x_i) \tag{5}$$

3. Experimental Study

3.1. Analysis of AC Requirements

Due to the following characteristics of its member structure and operation mode, its AC process is more complicated than that of traditional enterprises:

(1) Members of the virtual business can join or leave at any time. The organizational structure of the virtual business changes dynamically, and user permissions and corresponding application resources should also change dynamically;

(2) There is a business relationship between members that is both cooperative and competitive;

(3) The members are geographically concentrated and some are scattered, and must operate through a distributed network communication platform;

(4) There are many internal members, which makes the management of roles and rights distribution very complicated. We should try to reduce the difficulty of resource rights management by administrators.

The AC model needs to meet the following requirements:

(1) The user has the right to access resources in the external domain only when performing tasks, which meets the dynamic AC requirements of the workflow system;

(2) Under the premise of not changing the original roles and permissions of the current user, assign corresponding roles and permissions to the newly added users according to the needs of the

task, and prevent the leakage of confidential information among member companies;

(3) AC across enterprise boundaries can be achieved, enabling enterprises to manage and share resources with project teams as the basic unit;

(4) Realize the automatic allocation of user roles and role rights, reduce the difficulty of resource rights management by system administrators, and meet more fine-grained user rights allocation;

(5) Meet the active and passive AC principles, the full and partial inheritance principles of roles, the principle of least privilege and the principle of separation of duties.

3.2. Implementation Framework of AC System

According to the characteristics of the environment and the requirements of resource management, the technical realization mechanism of the DS AC model is given.

Global certificate authentication center: a third-party authentication agency, which stores the digital certificates of all users, and is mainly responsible for authenticating users and notifying the AC module of the authentication results.

AC Center: The leader enterprise is responsible for the establishment, maintenance and management. Its main functions include the following points: Provide interactive interfaces to resource requesting users, administrators at all levels and other modules; Update and authenticate user information, and be responsible for the creation of project teams, Manage and revoke; Generate user access authorization list according to the AC module to authorize users.

Identity authentication module: query the digital certificate from the global certificate authentication center according to the provided user information, and authenticate the user's identity.

Low-level AC module: When a user requests to access the private resources of the enterprise, according to the acquired role, call the permission to return the role, and return the permission to access the private resources of the enterprise for the user through the call.

AC module: Create the virtual role of the user in the project team according to the module role and project requirements, update the permission list of the project team user according to the sent public permission list, responsible for the creation, management and revocation of the project, responsible for activating the current task, responsible for activating The virtual role required in the current task execution returns the task status information during the project execution process. When the user needs to access the public resources, it is called to perform automatic role assignment, and then it is called to automatically authorize the user role.

4. Experiment Analysis

4.1. Membership Function Parameters

Due to the large number of trust levels, the number of membership functions is also large. In order to express each membership function conveniently, the parameters of the membership function are stored in an array during the experiment, and a membership function is represented by a function and an expression. The values are shown in Table 1.

Table 1. Parameter array for membership function

Array index	0	1	2	3	4	5	6	7	8	9	10	11
Parameter value	0.75	1.58	2.36	3.07	3.82	4.59	5.24	6.21	6.97	7.65	8.54	9.43

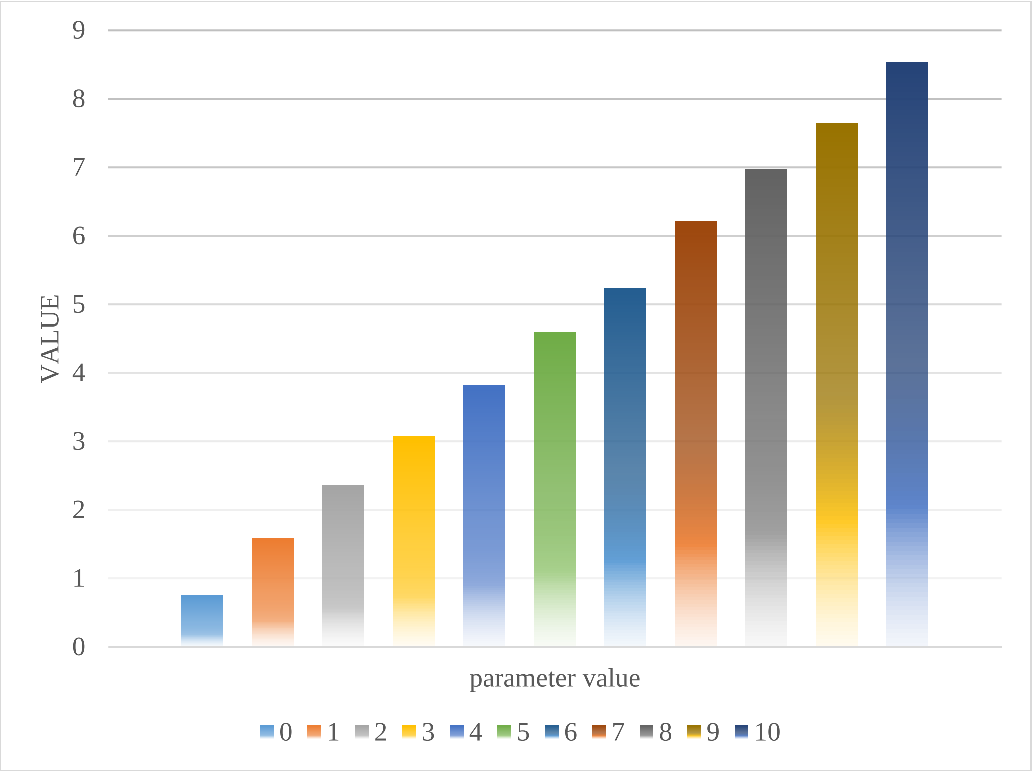

Figure 5. Parameter analysis diagram of membership function

As shown in the figure, the array has a total of 12 values, and the scale of membership for a certain trust level is 0 to 10. These values are calculated in the way of evenly distributing the interval. These 12 values are used in 7 membership functions, in which the parameters of the corresponding membership functions of two adjacent trust levels overlap, which also reflects that a certain trust may belong to multiple trust levels.

4.2. Comprehensive Performance Comparison

The application environment, mathematical method, computational efficiency, AC granularity, whether to evaluate user behavior, and the dynamics, globality, flexibility, convergence and security of trust evaluation are compared respectively. The specific results are shown in the following table:

Analysis of the above table shows that this algorithm has the following advantages and characteristics by combining FMs and PT methods: (1) It has good calculation convergence, and it has a good effect on the user's trust attribute value, behavior credibility and the relationship between virtual characters. A comprehensive evaluation of the trust degree of the network has been carried out, which reflects the global characteristics of trust and has a finer granularity of AC; (2) Each weight factor can be dynamically adjusted according to the needs of the above environment such as users, resources and tasks, which improves the computing power. (3) By evaluating the trust degree and the reputation value of user behavior, the user trust degree and the ability of service and access behavior are greatly improved, and compared with the existing trust evaluation algorithm, it has a good correlation. (4) Satisfying the rule of “slow increase and sudden decrease” of the trust degree of target change, it can effectively resist security attacks such as phishing attacks, bleaching attacks, and collusion attacks by malicious users, and has higher security.

Table 2. Typical trust model algorithm comparison

Trust model	Multi-step dynamic trust evaluation	1	2	3	4
Application environment	Virtual enterprise	Pervasive environment	Grid environment	Virtual enterprise	Pervasive environment
Mathematical method	Fuzzy judgment + pt	D-s theory	Fuzzy logic	Pt	Pt
Computational efficiency	Low	High	Low	High	High
Computational granularity	Thin	Thick	Thick	Thinner	Thinner
Credit rating	Have	Have	None	Have	None
Dynamism	Satisfy	Satisfy	Not satisfied	Satisfy	Not satisfied
Trust global	Satisfy	Not satisfied	Not satisfied	Satisfy	Satisfy
Flexibility	Powerful	Weak	Weak	Powerful	Medium
Computational convergence	Good	Good	Difference	Good	Good
Safety	Powerful	Medium	Weak	Medium	Medium

5. Conclusion

AC technology is a very important information security application technology in the field of modern information security. By authorizing system users and accessing information resources according to authorization constraints, the entire system resources are guaranteed to be accessed safely and controllably. In order to ensure that sensitive information is not illegally obtained by users, system resources are not maliciously added, deleted and modified, and system information is not destroyed by illegal use and tampering. This paper uses FMs and PT to study the AC of DSs. A subjective trust evaluation model based on fuzzy subset theory is proposed. Aiming at the characteristics of subjectivity and ambiguity of trust, the fuzzy subset in FMs is used to represent the level of trust, which can satisfy the rule of "slow increase and sudden decrease" of the trust degree when the target changes, and has higher security.

Funding

This article is not supported by any foundation.

Data Availability

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Conflict of Interest

The author states that this article has no conflict of interest.

References

[1] Khalil O. Pointwise equidistribution and translates of measures on homogeneous spaces. Ergodic Theory and Dynamical Systems, 2020, 40(2):453-477.

[2] Park J, Yoon C. Distributed Medium AC Method through Inductive Reasoning. International Journal of Fuzzy Logic and Intelligent Systems, 2021, 21(2):145-151.

[3] Hafeez Y, Ali S, Jhanjhi N, et al. Role of Fuzzy Approach towards Fault Detection for Distributed Components. Computers, Materials and Continua, 2021, 67(2):1979–1996.

[4] Khan M, Zeeshan M, Song S Z, et al. Types of Complex Fuzzy Relations with Applications in Future Commission Market. Journal of Mathematics, 2021, 2021(4):1-14.

[5] Homaei M H, Soleimani F, Shamshirband S, et al. An Enhanced Distributed Congestion Control Method for Classical 6LowPAN Protocols Using Fuzzy Decision System. IEEE Access, 2020, 8(99):20628-20645.

[6] Kirk N W, Declerck M, Kemp R J, et al. Language control in regional dialect speakers – monolingual by name, bilingual by nature?. Bilingualism: Language and Cognition, 2021, 25(3):511-520.

[7] Wilson S, Glotfelter P, Wang L, et al. The Robotarium: Globally Impactful Opportunities, Challenges, and Lessons Learned in Remote-Access, Distributed Control of Multirobot Systems. IEEE Control Systems Magazine, 2020, 40(1):26-44.

[8] Rezaei A, Smarandache F, Mirvakili S. Applications of (Neutro/Anti)sophications to Semihypergroups. Journal of Mathematics, 2021, 2021(6649349):1-7.

[9] Durairaj M, Asha J. Fuzzy probability based person recognition in smart environments. Journal of Intelligent and Fuzzy Systems, 2021, 40(5):1-16.

[10] Shahrouz S, Salehkaleybar S, Hashemi M. gIM: GPU Accelerated RIS-based Influence Maximization Algorithm. IEEE Transactions on Parallel and DSs, 2021, PP(99):1-1.

[11] Abughazalah N, Yaqoob N, Shahzadi K. Topological Structures of Lower and Upper Rough Subsets in a Hyperring. Journal of Mathematics, 2021, 2021(4):1-6.

[12] Nandanwar A, Nair R R, Behera L. Fuzzy inferencing-based path planning with a cyber-physical framework and adaptive second-order SMC for routing and mobility control in a robotic network. IET Cyber-Systems and Robotics, 2020, 2(3):149-160.

[13] Kim C, Kim W. Coordinated Fuzzy-Based Low-Voltage Ride-Through Control for PMSG Wind Turbines and Energy Storage Systems. IEEE Access, 2020, PP(99):1-1.

[14] Srivastava E. NdRAdAC: Need based AC Framework for an Emergency Response System. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021, 12(5):1414-1428.

[15] Sharma E. A Framework Of Big Data As Service Platform For AC & Privacy Protection Using Blockchain Network. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021, 12(11):476-485.

[16] Gaino R, Covacic M R, Cardim R, et al. Discrete Takagi-Sugeno Fuzzy Models Applied to Control the Knee Joint Movement of Paraplegic Patients. IEEE Access, 2020, PP(99):1-1.

[17] Dichev K, Sensi D D, Nikolopoulos D S, et al. Power LognRoll: Power-Efficient Localized Rollback for MPI Applications Using Message Logging Protocols. IEEE Transactions on Parallel and DSs, 2021, PP(99):1-1.

[18] Kozhaya D, Decouchant J, Rahli V, et al. PISTIS: An Event-Triggered Real-time Byzantine Resilient Protocol Suite. IEEE Transactions on Parallel and DSs, 2021, PP(99):1-1.