



PDF Download
3688574.3688583.pdf
08 January 2026
Total Citations: 0
Total Downloads: 378

Latest updates: <https://dl.acm.org/doi/10.1145/3688574.3688583>

RESEARCH-ARTICLE

Fuzzy-based Trust in Distributed Networks: A State-of-the-art Review

DONGSHENG JIA, Shanghai Institute of Microsystem and Information Technology Chinese Academy of Sciences, Shanghai, Shanghai, China

WEIDONG FANG, Shanghai Institute of Microsystem and Information Technology Chinese Academy of Sciences, Shanghai, Shanghai, China

WUXIONG ZHANG, Shanghai Institute of Microsystem and Information Technology Chinese Academy of Sciences, Shanghai, Shanghai, China

Open Access Support provided by:

Shanghai Institute of Microsystem and Information Technology Chinese Academy of Sciences

Published: 24 July 2024

[Citation in BibTeX format](#)

BDE 2024: 2024 6th International
Conference on Big Data Engineering
July 24 - 26, 2024
Xining, China

Fuzzy-based Trust in Distributed Networks: A State-of-the-art Review

Dongsheng Jia
Science and Technology on
Microsystem Laboratory, Shanghai
Institute of Microsystem and
Information Technology, Chinese
Academy of Sciences, Shanghai
201899, China; University of Chinese
Academy of Sciences, Beijing 100049,
China
jds@mail.sim.ac.cn

Weidong Fang*
Science and Technology on
Microsystem Laboratory, Shanghai
Institute of Microsystem and
Information Technology, Chinese
Academy of Sciences, Shanghai
201899, China; University of Chinese
Academy of Sciences, Beijing 100049,
China; Shanghai Research and
Development Center for Micro-Nano
Electronics, Shanghai 201210, China
weidong.fang@mail.sim.ac.cn

Wuxiong Zhang
Science and Technology on
Microsystem Laboratory, Shanghai
Institute of Microsystem and
Information Technology, Chinese
Academy of Sciences, Shanghai
201899, China; University of Chinese
Academy of Sciences, Beijing 100049,
China; Shanghai Research and
Development Center for Micro-Nano
Electronics, Shanghai 201210, China,
wuxiong.zhang@mail.sim.ac.cn

ABSTRACT

Distributed networks have gained increasing popularity due to their high reliability, resource-sharing convenience, and ample bandwidth. Distributed networks play a pivotal role in enabling a wide range of applications, including wireless sensor networks, cloud computing, social networks, and mobile ad hoc networks. Nevertheless, security and privacy concerns have consistently posed obstacles to the development of distributed networks. Trust management is an effective method for addressing these challenges. However, dealing with the uncertainty of trust has always been a challenging academic problem. Currently, many researchers are devoted to finding solutions within uncertainty theories, and one of the most prominent approaches is fuzzy logic. Fuzzy logic permits “imprecise” expression and reasoning that align with human thinking. In this paper, a review of fuzzy-based trust management in distributed networks is conducted. First, applications and uncertainty of trust are introduced. Then, the reasons why fuzzy logic is suitable for trust modeling are analyzed, and a classification method is proposed. Finally, an analysis of current research is presented to inspire further studies of researchers.

CCS CONCEPTS

• **Networks**; • **Network properties**; • **Network security**; • **Security and privacy**; • **Formal methods and theory of security**; • **Trust frameworks**;

KEYWORDS

Information security, distributed networks, fuzzy logic, trust model

*Corresponding author.



This work is licensed under a Creative Commons Attribution International 4.0 License.

BDE 2024, July 24–26, 2024, Xining, China
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1785-7/24/07
<https://doi.org/10.1145/3688574.3688583>

ACM Reference Format:

Dongsheng Jia, Weidong Fang, and Wuxiong Zhang. 2024. Fuzzy-based Trust in Distributed Networks: A State-of-the-art Review. In *2024 6th International Conference on Big Data Engineering (BDE) (BDE 2024)*, July 24–26, 2024, Xining, China. ACM, New York, NY, USA, 8 pages. <https://doi.org/10.1145/3688574.3688583>

1 INTRODUCTION

In the big data ecosystem, data perception, storage, and processing are of paramount importance. However, due to the complexity of tasks, it often requires the collaboration of multiple devices to complete. The choice of network structure is important. Since distributed networks (DNs) outperform centralized networks in terms of storage, computing, network bandwidth and security, more and more researchers are focusing on DNs, such as the processing of complex tasks [1], blockchain-based storage [2], and federated learning [3]. DNs comprise numerous heterogeneous nodes dispersed across various geographical locations [4], and P2P structure is adopted between nodes. Since there is no central server, the likelihood of a distributed network paralysis is reduced. Due to the decentralization, scalability, high robustness, self-organization, and multi-hop routing features inherent in DNs [2, 3], the application of DNs have been applied in many fields such as the Internet of Things and cloud computing. However, privacy and security have consistently been the focal points of attention in DNs.

Network attacks can cause significant harm to a network. Network attacks can be categorized into internal attacks and external attacks [7]. Traditional security mechanisms are conventional methods for mitigating security attacks. They are often referred to as “hard security” [8], which is usually based on key management systems. These methods can be deemed secure only if the keys are not exposed to adversaries. Nevertheless, Compromised nodes and selfish nodes possess communication keys, rendering it challenging for traditional security mechanisms to detect and counteract these nodes [6–10]. Zhang et al. systematically analyzed the shortcomings of the traditional key system [14]. In 1996, Blaze et al. [15] introduced the concept of “trust management” to address security issues of the Internet. Trust management is a form of “soft security” [8], where the trustworthiness of nodes is determined based on

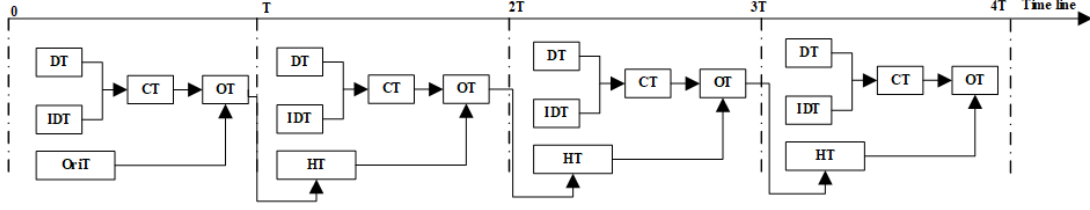


Figure 1: Relationships among DT, IDT, OT, HT, CT and OriT.

behavioral evidence collected. Since the trust model is controlled by the network itself, it is better suited for DNs[14]. Current trust review mainly focuses on specific application scenarios. It lacks an investigation of specific mathematical methods in trust. Therefore, we have reviewed the application of fuzzy logic in trust. We aim to analyze the uncertainty in trust and the reason using fuzzy logic in trust. At the same time, we compare the advantages and disadvantages of fuzzy logic with other methods. We propose a classification method for fuzzy-based trust. We introduce the current research progress according to the classification and hope it can inspire researchers. The main contributions of the paper are as follows:

1. Analyze the uncertainty of trust modeling in DNs.
2. Analyze the reasons why fuzzy logic can be applied to trust and compare fuzzy logic with other mathematical methods.
3. Propose a new classification about fuzzy-based trust, analyze the current research systematically to inspire researchers.

The remaining sections of the paper are organized as follows: Section 2 introduces the application of trust in DNs and uncertainty in trust modeling. Section 3 focuses on the importance and necessity of applying fuzzy logic in trust modeling. Moreover, we propose a classification of fuzzy-based trust. Section 4 systematically analyzes the current research. Conclusions are given in Section 5.

2 TRUST IN DISTRIBUTED NETWORKS

In this section, the application of trust in DNs and uncertainty in trust modeling are introduced.

2.1 Applications of Trust in Distributed Networks

Trust is a sociological concept that originally refers to a social relationship. Introduction of trust into network security means considering the trustworthiness of entities. Trust in DNs has not yet been explicitly defined. It can be viewed as a comprehensive manifestation of multiple properties (such as reliability, security, privacy) of entity in a specific context. Trust is characterized by subjectivity, asymmetry, partial transitivity, context sensitivity and dynamicity [16]. Common types of trust include direct trust (DT), indirect trust (IDT), historical trust (HT), overall trust (OT), original trust (OriT) and current trust (CT). The relationships among these trusts are illustrated in Fig.1. An example is illustrated in Fig.2. Node A sends packets to base station (BS) through the intermediate node B, assuming that trust updates periodically. At the moment $3T$, node A calculate the interval direct trust $DT(3T)$ in B according to its interaction records in the time interval $[2T, 3T]$ (the orange

line). At the same time, neighbors of node A (node C and D) send their recommendations about node B to node A (the green line). Node A get the indirect trust in node B ($IDT(3T)$) according to these recommendations. $CT(3T)$ is the result of integrating $DT(3T)$ with $IDT(3T)$, which means the trust of A to B in the time interval $[2T, 3T]$. Node A has a trust table. It records the HTs of nodes that have interacted with node A. Node A can get the $OT(3T)$ by integrating $CT(3T)$ and $HT(3T)$ about B. Then node A will determine whether to send packets to node B based on $OT(3T)$ within the time interval $[3T, 4T]$. OriT represents the original trust of nodes, which is set by researchers.

Trust has been widely applied in DNs. The applications of trust in DNs are mainly divided into trust-based security mechanism and trust-based service management[17]. Trust-based security mechanism includes trust-based intrusion detection system and trust-based dynamic access control policy. Trust-based service management includes trust-based selection of cloud services and trust-based route selection. Trust-based intrusion detection system takes trust into consideration intrusion detection system. It can effectively address the issues of low detection rate and insufficient intelligence[18]. Trust-based dynamic access control policy can grant corresponding access to nodes according to their trustworthiness, effectively preventing malicious nodes from overusing node information. Trust-based selection mechanism of cloud services chooses cloud services according to trust and trust update, improving the quality of the selected services. Trust-based route selection mechanism identifies malicious and selfish nodes by trust calculation. it simultaneously improves the overall network performance through trust-based decision-making.

2.2 Uncertainty of Trust Modeling

Uncertainty means the inability of individuals to determine or predict the outcomes or states of things. Trust modeling often contains numerous uncertainties and fuzziness, which are influenced by the nature of trust and the physical environment[19]. The uncertainty in trust modeling is summarized as below.

2.2.1 Uncertainty of trust expression. Trust is a qualitative concept. Trust is usually described as “trust”, “medium trust”, “distrust”. However, trust in digital systems tends to be described as real value. The trust described as numerical values requires clear boundaries, while the qualitative description of trust is often vague. Different people may have different understandings of different trust, which creates uncertainty in the semantics of trust. How to handle the relationship between quantitative and qualitative descriptions of trust is a problem. At the same time, how to quantitatively and

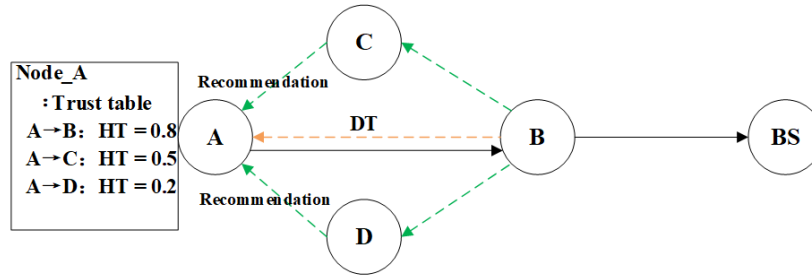


Figure 2: Trust calculation in wireless sensor network

effectively describe trust is worth considering, which is related to subsequent trust evaluation and application.

2.2.2 Uncertainty of trust evaluation. The uncertainty in trust evaluation is manifested in the fact that the obtained trust value cannot fully reflect the trustworthiness of node behavior in the network. The reasons include: (1) Uncertainty in data collection, (2) Incomplete information, (3) Limitations in node computing power and storage.

Uncertainty in data collection. During the process of collecting trust evidence, the dynamic changes in the network environment, interference of malicious nodes, communication failures, and delays can lead to incompleteness of data collection. Additionally, some sensitive information of nodes in the network may be hidden or anonymized, resulting in the inability to obtain certain information.

Incomplete information. The trust mechanism is essentially a kind of behavior-based security mechanism. During the evaluation process, the evaluating node may not have access to all the interaction records or related information of the evaluated node. Furthermore, limited or non-existent interactions between evaluating node and evaluated node can lead to significant evaluation errors. Finally, recommendations can mitigate the problem of limited interactions. However, it can be challenging to obtain evaluation results from all nodes that have interacted with the evaluated node.

Limitations in node computing power and storage. For some nodes in the internet of things, they may have limited computing and storage capabilities[20], which may prevent them from performing complex trust calculations and storing large amounts of trust data. This can lead to inaccuracies and uncertainties in trust evaluations.

2.2.3 Uncertainty of trust decision. Trust decision-making is the next phase of trust evaluation. On one hand, the uncertainty in decision-making is influenced by the uncertainty in trust evaluation. On the other hand, decision-making does not only take trust of nodes into consideration, but also various other factors, such as distance and the number of hop. These factors add complexity to the decision-making process.

3 FUZZY LOGIC IN TRUST

Mathematics is a tool to describe natural phenomena [21]. In 1965, Professor Zadeh introduced fuzzy sets to describe the uncertainty in nature, which cannot be resolved well by traditional logic [22].

Fuzzy logic abandons the binary logic mindset and expresses the membership relationship of elements through degrees of membership. In this section, we mainly explain why fuzzy logic can be applied to trust and propose a classification of fuzzy-based trust.

3.1 Advantages of Fuzzy Logic

Fuzzy logic possesses numerous advantages, which makes it feasible for trust modeling. Here are the reasons why fuzzy logic can be applied to trust.

Handling fuzziness. Professor Zadeh created the fuzzy theory because he realized that it was impossible to precisely describe the complex real world, but a reasonable model was needed[23]. The degree of membership and membership function provide the foundation for dealing with the fuzzy world. Acquiring the trustworthiness of nodes does not only rely on mathematical models and observational data, but also the expertise. Fuzzy system is created to integrate all of them [23]. Trust is full of uncertainty. Using fuzzy sets and membership functions, fuzzy logic can quantify the uncertainty of trust and conduct reasonable reasoning and judgment on it.

Imitating human reasoning. Fuzzy logic imitates the reasoning process and uncertainty judgment of the human brain [24], which makes it more in line with human behavior. In trust model, fuzzy logic can better simulate the complexity and diversity of human reasoning when dealing with trust relationships.

Handling uncertainty caused by missing information. When dealing with issues of missing or fuzzy information caused by environmental impacts or uncertainty, fuzzy logic can employ linguistic variables and membership functions to conduct qualitative analysis of the data, and derive qualitative knowledge and experience through fuzzy rules [25].

Flexibility and scalability. Fuzzy logic allows for the use of different membership functions and fuzzy rules to describe and process trust relationships, which gives trust models greater flexibility and scalability. The trust model can be customized and adjusted according to specific application scenarios and needs.

3.2 Comparison on Mathematical Methods

In trust modeling, researchers typically employ mathematical methods such as Bayesian analysis, Dempster-Shafer evidence theory, game theory, machine learning and fuzzy logic [19]. When building a trust model, these methods can be used jointly, such as Dempster-Shafer evidence theory for cross-layer trust and fuzzy theory for

Table 1: Comparison among mathematical methods

Mathematical theory	Advantages	Disadvantages
Fuzzy logic	Effective handling of uncertain problem. Mimics human reasoning, easy to understand. Flexibility and scalability.	The existence of curse of dimensionality. Difficulties in designing membership functions and fuzzy rules
Bayesian analysis	Simple calculation and good prediction for small-scale data.	Requires determining the knowledge distribution of prior probabilities or stochastic probabilities.
D-S evidence theory	Strong intuitiveness and effective handling of uncertain information.	Requires independence of evidence and the combination rules lack solid theoretical support.
Game theory	Understanding the decision-making process and predicting the behavior of the subject.	The assumption does not align with reality. High computational complexity.
Machine learning	Efficient processing of big data, strong adaptability and intelligent decision making.	Lack of transparency and interpretability in decision-making.

link trust [26]. However, when addressing the same problem, such as calculating direct trust, these methods may lead to different results or complexity due to their distinct characteristics. In order to select the most appropriate method, the advantages and disadvantages of these methods are needed, as is shown in Table 1 [19, 27, 28].

3.3 Classification of fuzzy-based Trust

Trust management involves the processes of collecting, storing, modeling, transferring, and trust-based decision making [4, 13]. But the main research of trust is modeling, transferring and trust-based decision making. Fuzzy-based trust can be categorized into five classes based on the application of fuzzy logic: acquisition of trust factors, description of trust, calculation of trust (excluding indirect trust), acquisition of indirect trust and trust-based decision making. Acquisition of trust factors refers to the stage from collecting the original behavioral data to calculating trust factors. Description of trust means how to describe the trustworthiness of a node qualitatively or quantitatively. Calculation of trust refers to how to map to get trust value of nodes according to trust factors [16]. The acquisition of indirect trust entails more processes, we will allocate a separate section, titled “Acquisition of Indirect Trust”. Trust-based decision making refers to the system or node’s response based on precompiled trust values.

4 FUZZY-BASED TRUST

Currently, numerous researchers have embraced fuzzy theory for trust modeling. In this part, we will analyze recent research based on the classification of fuzzy-based trust.

4.1 Acquisition of Trust Factors

Obtaining trust factors is a critical preliminary step in calculating trust values. Prioritizing security indices is occasionally essential. The prioritization of security metrics provides a reliable reference for the selection of weights. Analytic hierarchy process is a common method to determine the weight of elements, but traditional

analytic hierarchy process cannot deal with the relationship between elements and their relative importance. Linguistic variables introduced can effectively solve this problem and improve the accuracy and consistency of sorting [13].

The number of trust factors is worth considering. When the number of trust factors increases, fuzzy methods can be more complex due to the curse of dimensionality and hyper-fuzziness [23]. A common solution is the hierarchical structure. This main thought is to divide trust factors into multiple levels, breaking down a complex fuzzy method into several simpler fuzzy methods for calculation, as is shown in Fig.3. For instance, Alhanahnah [29] and Ashtiani [30] employed hierarchical fuzzy analytic hierarchy process for calculating trust factors. Moreover, hierarchical FIS is also a commonly method, such as Shirgahi [31] and Soleymani [32]. However, how to adjust the relationships among various trust factors remains an important challenge [33].

4.2 Description of Trust

Trust modeling centers on the description, measurement and trust evaluation [34]. The description of trust in DNs is not just “trust” or “distrust”. It can be “highly trust”, “medium trust”, “distrust”. Generally, trust can be represented by real values within the interval $[0,1]$. People tend to use qualitative descriptions such as “trust”, “highly trust”, and “distrust” in their knowledge bases. However, real values are easier for devices processing, the linguistic values are easier to understand. Combining the two is a question worth considering. Fuzzy logic is a solution for this. In fuzzy-based trust, trust can be treated as a linguistic variable, with values such as “highly trust”, “medium trust,” and “distrust”. The real value can be obtained by membership function. The membership function serves as a converter between linguistic variables and specific numerical values. Typically, the expression of linguistic variables is grounded in the membership function of type-1 fuzzy set [7, 17, 28, 31–41]. However, type-1 fuzzy set cannot effectively handle linguistic uncertainty [47]. Therefore, Yang et al. [6, 42] utilized interval type-2 fuzzy set to represent trust, improving accuracy in trust computation.

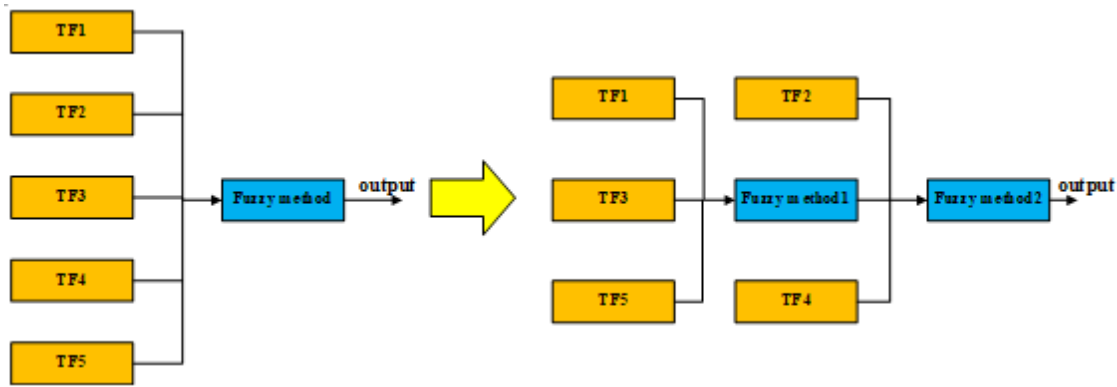


Figure 3: Hierarchical structure of fuzzy methods

4.3 Trust Calculation (excluding for indirect trust)

How to calculate trust accurately is worth considering. Due to the nature of trust, it is difficult to calculate trust. The weighted average method is the simplest way. However, trust is a subjective concept characterized with fuzziness and uncertainty [49]. The weighted average method cannot effectively handle such subjectivity. Experiments conducted by Ram [38] and Alnasser [45] demonstrate that fuzzy-based trust models outperform weighted average-based models.

Fuzzy inference system (FIS) is commonly used for trust calculation. In Fig. 4, trust factor is uniformly transformed into linguistic values by fuzzifier. The trustworthiness of nodes can be obtained by fuzzy inference engine. The crisp trust value is derived through defuzzifier. By FIS, the trust can be obtained by the way of conforming to human thinking, such as [7, 28, 31, 32, 34, 36, 37, 39, 44–48]. In general, FIS refers to type-1 fuzzy inference system (T1 FIS). However, the membership function of T1 FIS is deterministic. It may hinder its effectiveness in handling linguistic and numerical uncertainty [55]. Additionally, the trade-off between system precision and speed can also result in T1 FIS being less effective in addressing system fuzziness [55]. Research has demonstrated that interval type-2 FIS outperforms T1 FIS in handling uncertainty and achieving smoother control surfaces [56]. Currently, some researchers have tried interval type-2 FIS in trust calculation, such as [6, 42]. The experiments demonstrate that the trust model based on interval type-2 FIS has better performance than those based on T1 FIS.

Fuzzy clustering is another way to consider. Trusted nodes are typically designated as members of a cluster, with the most trusted node often serving as the cluster head. The main idea of fuzzy clustering is to categorize nodes into several groups such as “distrust”, “trust”, “highly trust” by membership degree. Traditional clustering analysis methods are typically grounded in conventional mathematical techniques [57]. These algorithms may not align well with practical applications because they cannot address the issue of unclear classification boundaries. Fuzzy clustering is a frequently employed method to tackle such issues. The key advantage of fuzzy clustering is its suitability for handling overlapping data, where a

data point can belong to one or more clustering centers [18]. For instance, Devi et al. [58] applied K-means clustering to choose the most reliable cluster head based on node trust values, distance, and energy levels. Veeraiah et al. [18] applied C-means clustering to select the most trusted cluster head, and a similar approach could be observed in [54–56].

In the trust evaluation process, a node must combine both direct trust and indirect trust to obtain a more accurate trust value [12]. Due to the fuzziness of trust, how to obtain global trust remains a challenge. To address this issue, Alnasser et al. [45] employed a FIS to evaluate node trustworthiness based on direct, indirect, and past trust. However, Alnasser treated trust information from the past as equal, which might not adequately reflect the varying impact of historical information on trust evaluation at different times. Chen et al. [12] incorporated historical information into local trust through trust update and computed node trust by combining fuzzy relations. This approach effectively captures the relational nature of trust.

4.4 Acquisition of Indirect Trust

Research on indirect trust primarily revolves around two key aspects: trust transferring and the computation of indirect trust. In general, indirect trust and recommendations play a crucial role in node trust evaluation. Currently, there are three primary methods for expressing the transitivity of trust through fuzzy logic. One approach is to directly multiply the trust values of nodes [62]. Whereas it is a simple method, it may not fully capture the relational nature of trust. Chen et al. [12] considered trust as a fuzzy relationship and expressed trust transferring through the transmission of fuzzy relationships. This approach is more in line with reality. FISs are considered as a means to realize trust transferring, such as Long [63]. By using the trust of each state as input to the FIS, nodes were able to determine the attitude of neighbor nodes towards the target node. Although this approach is innovative, it has to consider the design complexity caused by the curse of dimensionality.

In order to handle the uncertainty in indirect trust, Alroshan and Alhyasat applied fuzzy logic to the calculation of indirect trust [59, 60]. The articles considered factors such as information sharing, manufacturer and sensor quality but did not take into account the role of neighboring nodes.

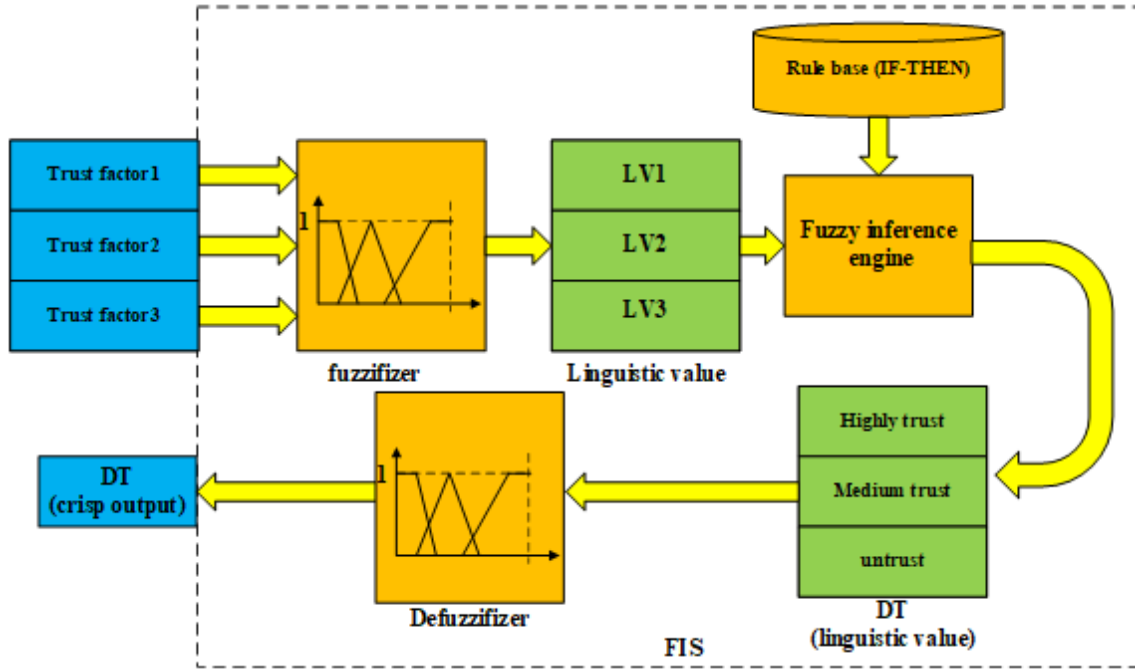


Figure 4: Direct trust calculation based on FIS

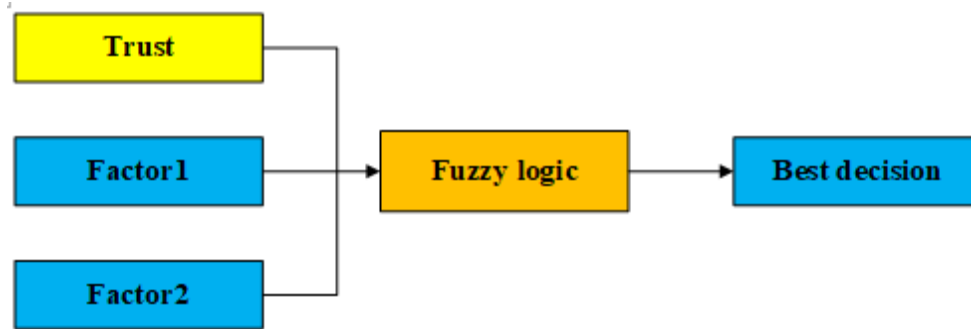


Figure 5: Trust decision (trust as an input)

4.5 Trust-based Decision Making

Trust-based decision making involves making more reliable judgments based on trust value. One approach is to utilize the trust values of nodes as a “sieve” for filtering out malicious nodes, such as Rajeswari [66]. Another common method for decision-making is to consider trust as one of the inputs for the decision-making process. Many fuzzy methods are used. For instance, Velusamy et al. [46] selected reliable routes based on node trust values, hop count, and link stability. Similarly, Garg [39] and Kranthikumar [67] also adopted a similar approach in their work. It is important to note that designing an effective FIS in the context of big data can be challenging. This is because of the curse of dimensionality in FIS and the difficulty of designing appropriate membership functions.

Hence, Velusamy et al. [26] employed the water cycle algorithm to design and optimize the fuzzy rules and membership functions, thereby reducing the complexity of the design and enhancing the storage efficiency of the device.

5 CONCLUSION

As an extension of traditional security mechanisms, trust management plays a crucial role in network security. Fuzzy logic is an effective method for addressing the uncertainty in trust. In this paper, we briefly introduce the applications of trust in DNs and the uncertainty in trust. Subsequently, we explain why fuzzy logic is suitable for trust modeling. We further propose a fuzzy-based trust classification. Based on the classification, we systematically review the current research. Through these analyses, we hope to

inspire researchers to better improve trust models and enhance the security of networks.

ACKNOWLEDGMENTS

This work was funded in part by the Shanghai Natural Science Foundation (grant number 21ZR1461700), in part by the National Natural Science Foundation of China (grant number 62071450), and in part by the Key Research and Development Task Special Project of the Xinjiang Uygur Autonomous Region (grant number 2022B01009).

REFERENCES

- [1] Amir Masoud Rahmani and Mojtaba Rezvani. 2009. A Novel Genetic Algorithm for Static Task Scheduling in Distributed Systems. *IJCTE*, 1,1 (April 2009), doi: 10.7763/IJCTE.2009.V1.1.
- [2] Boyi Lei, Jianhong Zhou, Maode Ma, and Xianhua Niu. 2023. DQN based Blockchain Data Storage in Resource-constrained IoT System. In *2023 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, Glasgow, United Kingdom, 1–6. doi: 10.1109/WCNC55385.2023.10118634.
- [3] Yunxiang Wang, Jianhong Zhou, Gang Feng, Xianhua Niu, and Shuang Qin. 2023. Blockchain Assisted Federated Learning for Enabling Network Edge Intelligence. *IEEE Network*, 37, 1(January 2023), doi: 10.1109/MNET.115.2200014.
- [4] Ming Li and Yueyang Liu. 2007. Comparison of Three Wireless Distributed Networks. *Telecommunication Science* 2 (2007), 95–98.
- [5] Ying Gao. 2013. Trust Management in P2P Network. Tsinghua University Press. Beijing, China.
- [6] Yu Feng and Bin He. 2012. Wireless Distributed Network Analysis and Military Applications. *Sichuan Armaments Engineering Journal* 33, 4 (2012), 91–93.
- [7] Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni, and Yinxuan Yang. 2020. Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey. *Wireless Communications and Mobile Computing* 2020, (September 2020), 1–20. <https://doi.org/10.1155/2020/2643546>
- [8] Audun Josang. 2006. Trust and reputation systems. in *Foundations of Security Analysis and Design IV, FOSAD 2006/2007 Tutorial Lectures*. Heidelberg, Berlin, Germany, 209–245.
- [9] Liu Yang, Yinzi Lu, Simon X. Yang, Tan Guo, and Zhifang Liang. 2021. A Secure Clustering Protocol With Fuzzy Trust Evaluation and Outlier Detection for Industrial Wireless Sensor Networks. *IEEE Trans. Ind. Inf.* 17, 7 (July 2021), 4837–4847. <https://doi.org/10.1109/TII.2020.3019286>
- [10] Azam Beheshtiasl and Ali Ghaffari. 2019. Secure and Trust-Aware Routing Scheme in Wireless Sensor Networks. *Wireless Pers Commun* 107, 4 (August 2019), 1799–1814. <https://doi.org/10.1007/s11277-019-06357-3>
- [11] Baohe Pang, Zhijun Teng, Huiyang Sun, Chunqiu Du, Meng Li, and Weihua Zhu. 2021. A Malicious Node Detection Strategy Based on Fuzzy Trust Model and the ABC Algorithm in Wireless Sensor Network. *IEEE Wireless Commun. Lett.* 10, 8 (August 2021), 1613–1617. <https://doi.org/10.1109/LWC.2021.3070630>
- [12] Dong Chen, Guiran Chang, Dawei Sun, Jiajia Li, Jie Jia, and Xingwei Wang. 2011. TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *ComSIS* 8, 4 (2011), 1207–1228. <https://doi.org/10.2298/CSIS110303056C>
- [13] Sunday Oyinlola Ogundoyin and Ismaila Adeniyi Kamil. 2020. A Fuzzy-AHP based prioritization of trust criteria in fog computing services. *Applied Soft Computing* 97, (December 2020), 106789. <https://doi.org/10.1016/j.asoc.2020.106789>
- [14] Wenzheng Zhang, Xiuhua Geng, Yu Zhou, Dianhua Tang, Junli Zhang, and Daoguang Mu. 2018. Trust Management System in Network. National Defense Industry Press. Beijing, China.
- [15] Matt Blaze, Joan Feigenbaum, Jack Lacy, T Research, and Murray Hill. Decentralized Trust Management. in *Proceedings 1996 IEEE symposium on security and privacy*, Oakland, USA, 164–173.
- [16] Osman Khalid, Samee U. Khan, Sajjad A. Madani, Khizar Hayat, Majid I. Khan, Nasro Min-Allah, Joanna Kolodziej, Lizhe Wang, Sherali Zeadally, and Dan Chen. 2013. Comparative study of trust and reputation systems for wireless sensor networks: Trust and reputation systems for wireless sensor networks. *Security Comm. Networks* 6, 6 (June 2013), 669–688. <https://doi.org/10.1002/sec.597>
- [17] Abdelmutlib Ibrahim Abdalla Ahmed, Siti Hafizah Ab Hamid, Abdullah Gani, Suleman Khan, and Muhammad Khurram Khan. 2019. Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges. *Journal of Network and Computer Applications* 145, (November 2019), 102409. <https://doi.org/10.1016/j.jnca.2019.102409>
- [18] Neenavath Veeraiah and B. Tirumala Krishna. 2019. Trust-aware FuzzyClus-Fuzzy NB: intrusion detection scheme based on fuzzy clustering and Bayesian rule. *Wireless Netw* 25, 7 (October 2019), 4021–4035. <https://doi.org/10.1007/s11276-018-01933-0>
- [19] Jun Xu. 2017. A Review of Trust Modeling in Uncertainty Theory. *Minicomputer Systems* 38, 1 (2017), 99–106.
- [20] Tao Feng and Xian Guo. 2017. *Wireless Sensor Networks*. Xidian University Press. Xi'an, China.
- [21] Jijian Xie and Chengping Liu. 2006. *Fuzzy method and its application* (3rd ed.). Huazhong University of Science and Technology Press. Wuhan, China.
- [22] Lotfi A. Zadeh. 1965. FUZZY SETS. *INFORMATION AND CONTROL* 8, 3 (1965), 338–. [https://doi.org/10.1016/S0019-9958\(65\)90241-X](https://doi.org/10.1016/S0019-9958(65)90241-X)
- [23] Jingwen Li. 2014. Research on Trust Evaluation Mechanism Based on Improved D-S Evidence Theory. Master Thesis, Nanjing University of Posts and Telecommunications.
- [24] Lotfi A. Zadeh. 1973. Outline of a New Approach to the Analysis of Complex Systems and Decision Processes. *IEEE Trans. Syst., Man, Cybern.* SMC-3, 1 (1973), 28–44. <https://doi.org/10.1109/TSMC.1973.5408575>
- [25] Yizhou Li. Risk Management for Maritime Transportation under Incomplete Information Conditions. PhD Thesis, School of Shipbuilding and Ocean Engineering, Shanghai Jiaotong University.
- [26] Durgadevi Velusamy and GaneshKumar Pugalandhi. 2020. Water Cycle Algorithm Tuned Fuzzy Expert System for Trusted Routing in Smart Grid Communication Network. *IEEE Trans. Fuzzy Syst.* 28, 6 (June 2020), 1167–1177. <https://doi.org/10.1109/TFUZZ.2020.2968833>
- [27] Jingwen Li. 2014. Research on Trust Evaluation Mechanism Based on Improved D-S Evidence Theory. Master Thesis, Nanjing University of Posts and Telecommunications.
- [28] Zhiqi Li, Weidong Fang, Chunsheng Zhu, Zhiwei Gao, and Wuxiong Zhang. 2023. AI-Enabled Trust in Distributed Networks. *IEEE Access*, vol. 11, pp. 88116–88134 (2023) doi: 10.1109/ACCESS.2023.3306452.
- [29] Mohammadh Alhanahnah, Peter Bertok, Zahir Tari, and Sahel Alouneh. 2018. Context-Aware Multifaceted Trust Framework for Evaluating Trustworthiness of Cloud Providers. *Future Generation Computer Systems* 79, (February 2018), 488–499. <https://doi.org/10.1016/j.future.2017.09.071>
- [30] Mehrdad Ashtiani and Mohammad Abdollahi Azgomi. 2016. Trust modeling based on a combination of fuzzy analytic hierarchy process and fuzzy VIKOR. *Soft Comput* 20, 1 (January 2016), 399–421. <https://doi.org/10.1007/s00500-014-1516-1>
- [31] Hossein Shirgahi, Mehran Mohsenzadeh, and Hamid Haj Seyyed Javadi. 2017. A three level fuzzy system for evaluating the trust of single web services. *IFS* 32, 1 (January 2017), 589–611. <https://doi.org/10.3233/JIFS-152526>
- [32] Seyed Ahmad Soleymani, Abdul Hanan Abdullah, Mahdi Zareei, Mohammad Hossein Anisi, Cesar Vargas-Rosales, Muhammad Khurram Khan, and Shidrokh Goudarzi. 2017. A Secure Trust Model Based on Fuzzy Logic in Vehicular Ad Hoc Networks With Fog Computing. *IEEE Access* 5, (2017), 15619–15629. <https://doi.org/10.1109/ACCESS.2017.2733225>
- [33] Koji Shimojima, Toshio Fukuda, and Yasuhisa Hasegawa. 1995. Self-tuning fuzzy modeling with adaptive membership function, rules, and hierarchical structure based on genetic algorithm. *Fuzzy Sets and Systems* 71, 3 (May 1995), 295–309. [https://doi.org/10.1016/0165-0114\(94\)00280-K](https://doi.org/10.1016/0165-0114(94)00280-K)
- [34] Wenbao Jiang. 2012. Trust Management and Network Security. Tsinghua University Press. Beijing, China.
- [35] Vani Krishnaswamy and Sunilkumar S. Manvi. 2021. Trusted node selection in clusters for underwater wireless acoustic sensor networks using fuzzy logic. *Physical Communication* 47, (August 2021), 101388. <https://doi.org/10.1016/j.phycom.2021.101388>
- [36] Rajkumar V. Patil, Parikshit N. Mahalle, and Gitanjali R. Shinde. 2022. Trust score estimation for device to device communication in internet of thing using fuzzy approach. *Int. j. inf. tecnol.* 14, 3 (May 2022), 1355–1365. <https://doi.org/10.1007/s41870-020-00530-9>
- [37] Rupayan Das, Dinesh Dash, and Mrinal Kanti Sarkar. 2020. HTMS: Fuzzy Based Hierarchical Trust Management Scheme in WSN. *Wireless Pers Commun* 112, 2 (May 2020), 1079–1112. <https://doi.org/10.1007/s11277-020-07092-w>
- [38] V. Ram Prabha and P. Latha. 2017. Fuzzy Trust Protocol for Malicious Node Detection in Wireless Sensor Networks. *Wireless Pers Commun* 94, 4 (June 2017), 2549–2559. <https://doi.org/10.1007/s11277-016-3666-1>
- [39] Mukesh Kumar Garg, Neeta Singh, and Poonam Verma. 2018. Fuzzy rule-based approach for design and analysis of a Trust-based Secure Routing Protocol for MANETs. *Procedia Computer Science* 132, (2018), 653–658. <https://doi.org/10.1016/j.procs.2018.05.064>
- [40] Gayathri M and C. Gomathy. 2022. Fuzzy based Trusted Communication in Vehicular Ad hoc Network. In *2022 2nd International Conference on Intelligent Technologies (CONIT)*, June 24, 2022. IEEE, Hubli, India, 1–4. <https://doi.org/10.1109/CONIT55038.2022.9847823>
- [41] Alagumani Selvaraj and Subashini Sundararajan. 2017. Evidence-Based Trust Evaluation System for Cloud Services Using Fuzzy Logic. *Int. J. Fuzzy Syst.* 19, 2 (April 2017), 329–337. <https://doi.org/10.1007/s40815-016-0146-4>
- [42] Siri Guleng, Celimuge Wu, Xianfu Chen, Xiaoyan Wang, Tsutomu Yoshinaga, and Yusheng Ji. 2019. Decentralized Trust Evaluation in Vehicular Internet of Things. *IEEE Access* 7, (2019), 15980–15988. <https://doi.org/10.1109/ACCESS.2019.2893262>
- [43] Mohammad Dahman Alshehri and Farookh Khadeer Hussain. 2019. A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT).

- Computing 101, 7 (July 2019), 791–818. <https://doi.org/10.1007/s00607-018-0685-7>
- [44] Md. Mahmudul Hasan, Mosarrat Jahan, Shaily Kabir, and Christian Wagner. 2021. A Fuzzy Logic-Based Trust Estimation in Edge-Enabled Vehicular Ad Hoc Networks. In 2021 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). IEEE, Luxembourg, Luxembourg, 1–8. <https://doi.org/10.1109/FUZZ45933.2021.9494428>. 2021.7.
- [45] Aljawharah Alnasser and Hongjian Sun. 2017. A Fuzzy Logic Trust Model for Secure Routing in Smart Grid Networks. IEEE Access 5, (2017), 17896–17903. <https://doi.org/10.1109/ACCESS.2017.2740219>.
- [46] Durgadevi Velusamy, Ganeshkumar Pugalendhi, and Karthikeyan Ramasamy. 2020. A Cross-Layer Trust Evaluation Protocol for Secured Routing in Communication Network of Smart Grid. IEEE J. Select. Areas Commun. 38, 1 (January 2020), 193–204. <https://doi.org/10.1109/JSAC.2019.2952035>
- [47] Wei Chen and Zengqi Sun. 2003. A Review of Type-2 Fuzzy Systems. In China Intelligent Automation Conference, 22–31. Hongkong, China.
- [48] Liu Yang, Yinshi Lu, Simon X. Yang, Yuanchang Zhong, Tan Guo, and Zhifang Liang. 2021. An Evolutionary Game-Based Secure Clustering Protocol With Fuzzy Trust Evaluation and Outlier Detection for Wireless Sensor Networks. IEEE Sensors J. 21, 12 (June 2021), 13935–13947. <https://doi.org/10.1109/JSEN.2021.3070689>
- [49] Xinfei Liao. Research on Subject Trust Evaluation Based on Fuzzy Theory. Advanced engineering forum.(September 2011), 52–56. <https://doi.org/10.4028/www.scientific.net/AEF.1.52>.
- [50] Golnaz Aghaee Ghazvini, Mehran Mohsenzadeh, Ramin Nasiri, and Amir Masoud Rahmani. 2020. MMLT: A mutual multilevel trust framework based on trusted third parties in multicloud environments. Softw: Pract Exper 50, 7 (July 2020), 1203–1227. <https://doi.org/10.1002/spe.2798>
- [51] Zhaozheng Li and Weimin Lei. 2018. A service trust evaluation model using clustering fuzzy inference for guiding network service selection. Int J Commun Syst 31, 17 (November 2018), e3790. <https://doi.org/10.1002/dac.3790>
- [52] Sihem Benfriha and Nabila Labraoui. 2022. Insiders Detection in the Uncertain IoD using Fuzzy Logic. In 2022 International Arab Conference on Information Technology (ACIT). IEEE, Abu Dhabi, United Arab Emirates, 1–6. <https://doi.org/10.1109/ACIT57182.2022.9994119>. 2022.11
- [53] Kamini Joshi, Milanjit Kaur, and Lipika Gupta. 2023. Design of Clustering Algorithm for Energy Efficient and Secure WSN using Fuzzy Logic. In 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS). IEEE, Coimbatore, India, 1448–1453. <https://doi.org/10.1109/ICSCSS57650.2023.10169657>. 2023.6.
- [54] R. A. Isabel and E. Baburaj. 2018. An Optimal Trust Aware Cluster Based Routing Protocol Using Fuzzy Based Trust Inference Model and Improved Evolutionary Particle Swarm Optimization in WBANs. Wirel. Pers. Commun. 101, 1 (July 2018), 201–222. <https://doi.org/10.1007/s11277-018-5683-8>
- [55] Hani Hagras. 2007. Type-2 FLCs: A new generation of fuzzy controllers. IEEE COMPUTATIONAL INTELLIGENCE MAGAZINE 2, 1 (February 2007), 30–43. <https://doi.org/10.1109/MCI.2007.357192>
- [56] Wei Peng, Chengdong Li, Guiqing Zhang, and Jianqiang Yi. 2020. Interval type-2 fuzzy logic based transmission power allocation strategy for lifetime maximization of WSNs. ENGINEERING APPLICATIONS OF ARTIFICIAL INTELLIGENCE 87, (January 2020). <https://doi.org/10.1016/j.engappai.2019.103269>
- [57] Xianggao Li and Hongxing Li. 1994. Fuzzy Cluster Analysis and Its Application. Guizhou Science and Technology Press. Guizhou, China.
- [58] Vallala Sowmya Devi and Nagaratna P Hegde. 2018. Multipath Security Aware Routing Protocol for MANET Based on Trust Enhanced Cluster Mechanism for Lossless Multimedia Data Transfer. Wireless Pers Commun 100, 3 (June 2018), 923–940. <https://doi.org/10.1007/s11277-018-5358-5>
- [59] Neenavath Veeraiah, Osamah Ibrahim Khalaf, C. V. P. R. Prasad, Youseef Alotaibi, Abdulmajeed Alsufyani, Saleh Ahmed Alghamdi, and Nawal Alsufyani. 2021. Trust Aware Secure Energy Efficient Hybrid Protocol for MANET. IEEE Access 9, (2021), 120996–121005. <https://doi.org/10.1109/ACCESS.2021.3108807>
- [60] Uppalapati Srilakshmi, Saleh Ahmed Alghamdi, Veera Ankalu Vuyyuru, Neenavath Veeraiah, and Youseef Alotaibi. 2022. A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks. IEEE Access 10, (2022), 14260–14269. <https://doi.org/10.1109/ACCESS.2022.3144679>
- [61] Uppalapati Srilakshmi, Neenavath Veeraiah, Youseef Alotaibi, Saleh Ahmed Alghamdi, Osamah Ibrahim Khalaf, and Bhimineni Venkata Subbayamma. 2021. An Improved Hybrid Secure Multipath Routing Protocol for MANET. IEEE Access 9, (2021), 163043–163053. <https://doi.org/10.1109/ACCESS.2021.3133882>
- [62] Zhaoyi Li, Fei Xiong, Ximeng Wang, Zhe Guan, and Hongshu Chen. 2020. Mining Heterogeneous Influence and Indirect Trust for Recommendation. IEEE Access 8, (2020), 21282–21290. <https://doi.org/10.1109/ACCESS.2020.2968102>
- [63] Hongyi Long and Dan Pan. 2009. Indirect Recommendation Trust Transitivity Study based on Fuzzy Theory. Journal of Wuhan University of Technology, 114–117.
- [64] Ayat Alroshan, Tayba Asgher, Munawar Hussain, Muhammad Shahzad, Faiz Rasool, and Ahmed Abu-Khadrah. 2022. Virtual Trust on Driverless Cars Using Fuzzy Logic Design. In 2022 International Conference on Business Analytics for Technology and Security (ICBATS). IEEE, Dubai, United Arab Emirates, 1–7. <https://doi.org/10.1109/ICBATS54253.2022.9759077>. 2022.2
- [65] Khaled Mohamed Kayed Alhyasat, Nahia Mourad, Omar Sattar, Faiz Rasool, Ali Sheraz Akram, and Tayba Asgher. 2022. Estimation of Virtual Trust on Driverless Cars using Type-1 Fuzzy logic. In 2022 International Conference on Cyber Resilience (ICCR). IEEE, Dubai, United Arab Emirates, 1–11. <https://doi.org/10.1109/ICCR56254.2022.9996058>. 2022.9
- [66] A. R. Rajeswari, K. Kulothungan, Sannasi Ganapathy, and A. Kannan. 2019. A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks. Peer-to-Peer Netw. Appl. 12, 5 (September 2019), 1076–1096. <https://doi.org/10.1007/s12083-019-00766-8>
- [67] Bhukya Kranthikumar and R. Leela Velusamy. 2023. Trust aware secured energy efficient fuzzy clustering-based protocol in wireless sensor networks. Soft Comput. (April 2023). <https://doi.org/10.1007/s00500-023-08098-9>