future internet

MDPI

Article

Fuzzy Multi-Criteria Based Trust Management in Heterogeneous Federated Future Internet Testbeds

Dimitrios Dechouniotis *, Ioannis Dimolitsas, Konstantinos Papadakis-Vlachopapadopoulos and Symeon Papavassiliou

School of Electrical & Computer Engineering, National Technical University of Athens—NTUA, 9, Iroon Polytechniou Street, Zografou, GR 157 80, Greece; el11089@central.ntua.gr (I.D.); cpapad@netmode.ntua.gr (K.P.-V.); papavass@mail.ntua.gr (S.P.)
* Correspondence: ddechou@netmode.ntua.gr; Tel.: +30-210-772-1451

Received: 22 May 2018; Accepted: 21 June 2018; Published: 25 June 2018

Abstract: A federation of heterogeneous testbeds, which provides a wide range of services, attracts many experimenters from academia and industry to evaluate novel future Internet architectures and network protocols. The candidate experimenter reserves the appropriate testbeds' resources based on various diverse criteria. Since several testbeds offer similar resources, a trust mechanism between the users and the providers will facilitate the proper selection of testbeds. This paper proposes a fuzzy reputation-based trust framework that is based on a modification of the fuzzy VIKOR multi-criteria decision making method and combines the user's opinion from previously-conducted experiments with retrieved monitoring data from the utilized testbeds, in order to quantify the reputation of each testbed and the credibility of the experimenter. The proposed framework can process various types of numeric and linguistic data in an on-line fashion and can be easily extended for new types of testbeds and services. Data from active federated testbeds are used to evaluate the performance of the fuzzy reputation-based trust framework under dynamic conditions. Furthermore, a comparison of the proposed framework with another existing state of the art trust framework for federated testbeds is presented, and its superiority is demonstrated.

Keywords: federated testbeds; fuzzy systems; trust management

1. Introduction

Nowadays, web services are shifting gradually from the client-server paradigm to more distributed delivery models consisting of several individual software components. The architecture of the on-line services can be categorized as single, composite and communities [1]. Single services do not interact with other services, while composite ones consist of a set of single services to offer more complex functionalities. Recently, various developed communities of services have distributed the computational load of a service's request among several individual users. Furthermore, people interact increasingly with e-services through mobile devices, which means many heterogeneous network and computing devices are involved in every on-line transaction. In such a complex environment, the user of a service must select the appropriate provider that fulfills his/her requirements, and this decision is based on numerous versatile technical and human-centric criteria. Similarly to the human transactions, a trust mechanism between the user and the provider is necessary. The trust is defined as the subjective belief of Entity A that Entity B will perform a given action [2]. Reputation is a complementary concept that helps entities trust each other. Reputation is defined as "the general belief about a person's or thing's character or standing", according to the Concise Oxford Dictionary. The main difference between these notions is that reputation is public and produced by a group of people or entities, while trust is personal and subjective.

Over the last decade, many testbeds have been offered to academia and industry to deploy and evaluate novel network services and architectures. A single testbed usually offers a specific type of resource, which is suitable for small- or medium-scale experimentation. Thus, many research initiatives, such as FED4FIRE [3], FED4FIRE+ [4] and GENI [5], federate heterogeneous testbeds in terms of wired, wireless, computing and virtualized resources. The management framework of these projects supports all phases of the experimental lifecycle, i.e., discovering, booking and provisioning the appropriate resources. The federated environment enables the experimenters to select among different testbeds and services. According to each experiment scenario, a number of different resources with specific functionalities will be required. For most scenarios, testbed federations offer plenty of resources with the same or similar functionalities. In this case, the user should select the resources meeting his/her requirements. For example, an experiment on on-line gaming has strict low-latency requirements, while a video streaming experiment focuses mainly on a high and stable data transfer rate. Thus, it is important to establish a trust mechanism among the entities of the experiment in order to facilitate the successful conduction of the experiments and provide a comprehensible testbed reputation score based on specific performance metrics.

In this paper, we design and deploy a scalable reputation-based trust framework for a federated testbed environment in order to enable the selection of the appropriate testbed according to the experimenters' requirements. The proposed system can process a set of diverse performance criteria and quantify the testbeds' reputation leveraging Quality of Service (QoS) and Quality of Experience (QoE) measurements. The trust framework is based on a modification of the fuzzy VIKOR multi-criteria decision-making method and leverages both numeric and linguistic values to infer the reputation score of the federated testbeds. Upon the completion of an experiment, the users are prompted to submit their rating for the performance of the infrastructure utilized using QoS and QoE criteria. The QoS metrics of each testbed, e.g., node availability and network latency, are measured by numerical values, while the QoE metrics, e.g., usability and support satisfaction, are evaluated by fuzzy numbers. Fuzzy logic and systems are widely used in research problems of computer networks, e.g., [6,7], and conveniently express the human opinion on vague concepts. Furthermore, the proposed framework evaluates the credibility of the experimenters, using Service Level Agreement (SLA) data, in order to mitigate the effect of abnormal or malicious evaluations and guarantees that the reputation score is fairly computed. The operation of the proposed framework over an existing real federation of testbeds environment is demonstrated, and its performance using monitoring data and user ratings from actual federated testbeds is evaluated. Finally, the operational superiority of the proposed system against an existing reputation-based trust framework, i.e., FTUE [8] that processes exclusively numerical values, is highlighted and discussed.

The rest of the paper is structured as follows: Section 2 discusses related work. Section 3 presents the details of the introduced reputation system and credibility mechanism. Section 4 contains indicative numerical results about the operation and performance of the introduced trust framework over real federated testbeds, while comparative results against the FTUE framework are presented. Our conclusions and future work are drawn in Section 5.

2. Related Work

A federation of future Internet testbeds provides various types of resources, such as wired, wireless, cloud computing and virtualized (e.g., Software Defined Networks (SDN)) resources. Thus, this section presents the most interesting trust and reputation approaches on these types of services in the literature. For general information on future internet security architectures, the interested reader can refer to [9].

Wahab et al. [1] presented a complete survey on trust and reputation systems for three types of web services, named single, composite and communities. The authors of [10] proposed a Bayesian network reputation and trust model for single web services that was based on direct user feedback, the recommendation of other users and QoS data. Furthermore, a credibility mechanism for the

users was provided. RATEWeb [11] is a trust framework for selecting and composing web services. The reputation score is computed with a statistical method that utilizes the credibility of the users, their personalized references, the immediate knowledge and the temporal sensitivity. A game-theoretic model for composite services was proposed by Yahyaoui [12]. A Bayesian model was used to derive the trust value of each service for possible collaboration with other services. This value was used to compute a trust-based cost in order to find the winner service, which was eventually allocated with tasks.

Several approaches were proposed for reputation and trust management in wireless sensor and ad hoc networks. In [13], a reputation framework for data integrity in wireless sensor networks was presented, where each node evaluated the past activities and predicted the future behavior of other nodes by maintaining reputation values. A Bayesian formulation was adopted for reputation representation and evolution. Furthermore, a consensus-based outlier scheme was used as the credibility mechanism of data reading. Ren et al. [14] presented a trust management approach for unattended wireless sensor networks based on subjective logic. This study aims at providing trusted data storage and generation. Furthermore, the authors used the trust similarity function to detect outliers and protect against trust pollution attacks. ART [15] aimed at detecting malicious attacks and evaluating the trustworthiness of mobile nodes and data in vehicular ad hoc networks. In this study, node trust had a two-dimensional meaning in terms of fulfilling a functionality and recommendation to other nodes. The Dempster–Shafer theory of evidence was used for data analysis, and these pieces of evidence were utilized to derive the trustworthiness of the node and data. The recommendation trust of nodes was evaluated by collaborative filtering.

In the cloud computing environment, reputation and trust management systems have been broadly used for provider selection or security. CloudArmour [16] is a reputation-based trust management framework that focuses on availability and security. A credibility model was proposed to detect feedback collision and Sybil attacks, while an availability model spread the trust management service nodes in order to manage the users' feedback in a decentralized manner. Manuel [17] proposed a trust model for selecting resources from different cloud providers. The trust value is a weighted composition of some QoS metrics, e.g., availability and data integrity, and the candidate cloud user negotiates with the system manager to make the final decision. CloudRec [18] is a recommendation mechanism designed for mobile cloud services. It is based on adaptive QoS management, and it monitors the performance of cloud services and recommends the ideal one to users according to their contextual information.

With the advent of 5G technologies, many researchers have focused on Network Function Virtualization (NFV) and SDN. The trust management of this type of networks is an open challenge. In [19], the authors proposed a trust platform for NFV infrastructure that was responsible for the QoS guarantee of a Virtual Network Function (VNF) to fulfill the user's requirements. The reputation of VNF was quantified by local monitoring data and from trust information of other devices. FlowBroker [20] is a brokering agent architecture suitable for the coordination of distributed SDN controllers. The broker's reputation is based on metrics of the end-to-end delay, the max link utilization ratio and the packet loss ratio and is used by other agents in order to accept flow rule changes and peer broker forwarding updates. A machine learning method, named linear discriminant analysis, is adopted for the quantification of the reputation of each broker.

An interesting category of trust and reputation systems is that implemented on Peer-to-Peer (P2P) networks. The following trust management frameworks are also applied to other distributed systems. The EigenTrust algorithm [21] was designed to protect P2P network users from downloading malicious or inauthentic files. It calculated and assigned a global trust value to every peer by using a recursive method and the users' opinions. The algorithm was based on power iteration and can be implemented both as a centralized and distributed service. The ROCQ mechanism [22] proposed a reputation-based trust management system that produced reputation values in order to represent the trustworthiness of peers in P2P networks. The evaluation of peers was provided after the end of each transaction between

peers. The ROCQ system could be implemented in a distributed manner, and the reputation value was based on the user's opinion, the user's credibility produced by his/her previous evaluations and the quality that represented the confidence of a peer in the accuracy of his/her evaluation.

There were very few studies that have proposed a reputation or trust management approach for different types of resources. FTUE [8] is a reputation-based trust management framework for federated testbeds. It utilized user feedback and monitoring data to compute the reputation metric per service per testbed. Four different scenarios were used to characterize the user's credibility, which was considered based on the reputation score. Brinn et al. [23] proposed an approach for federated trust in the context of the GENI project. The concept of trust had three different meanings, named credibility, endorsement and reliance. GENI provided an authentication and authorization mechanism to realize the trust operation between the federated entities.

The overwhelming majority of the aforementioned approaches have focused only on a specific type of resource. In a federated environment, the calculation of reputation and trust value is more challenging, because there are many different metrics and requirements that must be considered. Compared with these studies, the main difference of our approach is that it can take simultaneously into account various QoS, QoE and SLA data from different types of resources and testbeds in a scalable way and without any assumption about the experimenter's willingness.

3. Proposed Fuzzy VIKOR Reputation System

This section presents a fuzzy reputation-based trust management system for federated testbeds and a credibility mechanism for the experimenters' ratings. The fuzzy VIKOR reputation framework has a horizontal structure, which can easily scale up and is actually a multi-criteria decision technique. It can process simultaneously various types of data, e.g., binary, numeric and linguistic values. This allows us to use numeric QoS and SLA data combined with linguistic QoE data that are appropriate to express the vague and subjective user preferences. Each testbed provides a set of services. The services of a testbed depend on the type of available resources and refer to computing or network Key Performance Indicators (KPIs), e.g., node/link/server availability or network delay, bandwidth and packet loss ratio. The proposed framework considers various QoS and QoE criteria from SMICloud [24]. In a federated environment, several experimenters can use the same testbed with different goals. Thus, in our approach, each experimenter is able to adjust the weight of criteria according to his/her needs. The consistency of the weights is checked in order to provide meaningful rates and discourage malicious evaluators.

Our framework is based on fuzzy VIKOR (Visekriterijumsko Kompromisno Rangiranje), which is a multi-objective decision-making approach. This technique is applicable to cases where the best provider must be selected among different alternatives. For instance, the fuzzy VIKOR approach is used for renewable energy planning [25]. The fuzzy VIKOR method handles only fuzzy inputs. Thus, we propose a modification of fuzzy VIKOR that considers both numeric and linguistic values. Furthermore, the user can assign the weight of each criterion according to his/her requirements. The reputation system modifies the reputation score of each testbed after conducting an experiment. Furthermore, a credibility mechanism compares the experimenter's opinion with SLA and monitoring measurements in order to protect the reputation of testbeds against malicious users. We choose this multi-objective methodology to investigate the effectiveness of using both numerical and fuzzy inputs on the reputation score of the federated testbeds. The evaluation of our framework in Section 4 showcases the importance of using fuzzy criteria for the QoE metrics. Appendix A presents the basic information on fuzzy numbers and sets.

3.1. Fuzzy VIKOR

Fuzzy VIKOR is a multi-criteria decision-making approach that simultaneously measures the closeness to the best and worst alternative. It can be applied to any scenario in which a user has to select among alternative providers, such as cloud services [26] and renewable energy resources [25].

The original fuzzy VIKOR approach uses explicitly a group of fuzzy KPIs. For the computation of the reputation score of a testbed, we extend this approach in order to process also numeric KPIs, as shown in Figure 1, where the reputation value is directly derived from the KPIs. In Figure 1, the level of criteria categories does not contribute to the computation of the reputation value, and it indicates only the different nature of the underlying KPIs. The purple (left) technical KPIs refer to QoS metrics, and they are numeric, while the pink (right) non-technical KPIs correspond to fuzzy KPIs. These numeric inputs are converted to fuzzy numbers, as explained in the following subsection. For each pair of KPIs, an assigned fuzzy weight indicates the relative importance between them. Table 1 presents the linguistic terms and the corresponding membership functions for the fuzzy weights, while Table 2 presents the information about the fuzzy numbers used for the KPIs' evaluation. The experimenter's evaluation is compared to the perfect evaluation of a virtual user in order to acquire a quantitative measure of the closeness to the best testbed's performance. The following steps include all the necessary computations of the reputation score of a federated testbed.

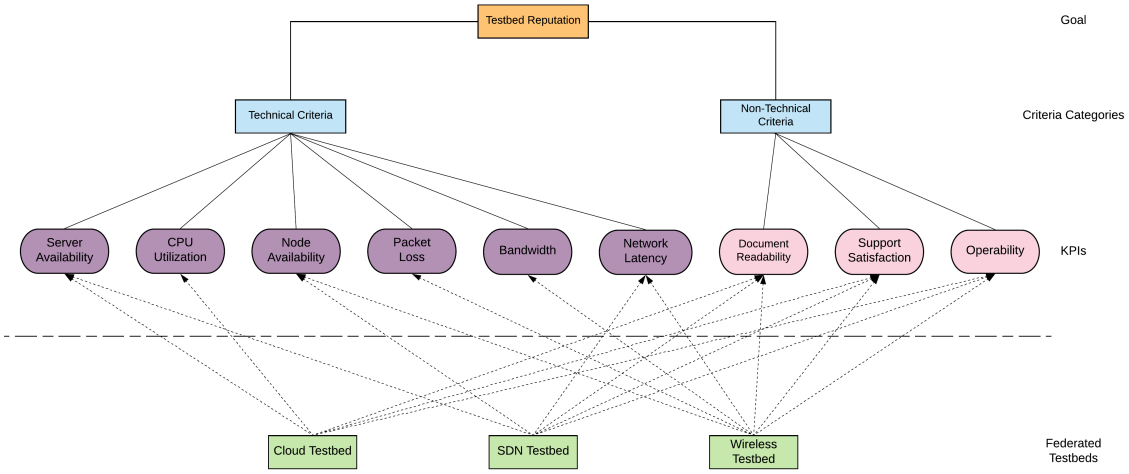


Figure 1. Modified Fuzzy VIKOR reputation model for federated testbeds.

Table 1. Linguistic terms and membership functions of fuzzy weights.

Linguistic Term	Membership Function
Absolutely Strong (AS)	$(2, 5/2, 3)$
Very Strong (VS)	$(3/2, 2, 5/2)$
Fairly Strong (FS)	$(1, 3/2, 2)$
Slightly Strong (SS)	$(1, 1, 3/2)$
Equal (E)	$(1, 1, 1)$
Slightly Weak (SW)	$(2/3, 1, 1)$
Fairly Weak (FW)	$(1/2, 2/3, 1)$
Very Weak (VW)	$(2/5, 1/2, 2/3)$
Absolutely Weak (AW)	$(1/3, 2/5, 1/2)$

Table 2. Linguistic terms and membership functions of fuzzy KPIs.

Linguistic Term	Membership Function
Extremely Poor (EP)	$(0.1, 1, 2)$
Very Poor (VP)	$(1, 2, 3)$
Poor (P)	$(2, 3, 4)$
Medium Poor (MP)	$(3, 4, 5)$
Fair (F)	$(4, 5, 6)$
Medium Good (MG)	$(5, 6, 7)$
Fair Good (FG)	$(6, 7, 8)$
Good (G)	$(7, 8, 9)$
Very Good (VG)	$(8, 9, 10)$
Excellent (E)	$(9, 10, 10)$

Step 1. Definition of the testbed KPIs: The testbed provider defines all the QoS and QoE KPIs that determine the performance of the testbed. Furthermore, the QoS KPIs are included in an SLA between the provider and the experimenter.

Step 2. Definition of relative importance weights: The experimenter assigns the linguistic term for the relative importance weight of all possible KPI pairs from Table 1. Assuming a testbed with N KPIs, we formulate the fuzzy Pairwise Importance Comparison Matrix (PICM) as follows:

$$PICM = \begin{array}{c} \\ K_1 \\ K_2 \\ \vdots \\ K_N \end{array} \begin{array}{c} \begin{array}{cccc} K_1 & K_2 & \dots & K_N \end{array} \\ \begin{bmatrix} 1 & FS & \cdots & VW \\ FW & 1 & \cdots & E \\ \vdots & \vdots & \ddots & \vdots \\ VS & E & \cdots & 1 \end{bmatrix} \end{array} \tag{1}$$

Then, the PICM's elements are defuzzified using (A6) of Appendix A. Since the weights are derived from the subjective preferences of individuals, the final computation of reputation can be based on inconsistent and conflicting KPIs. Thus, in order to avoid such inconsistencies, the Consistency Ratio (CR) [27] is calculated for each group of sibling attributes. The CR is the degree of randomness in the weight assignment between several sibling attributes. CR values less than 0.1 are acceptable to continue to the next phase; otherwise, the experimenter must correct the assigned weights.

Step 3. Computation of the KPIs weight vector: The fuzzy Analytical Hierarchical Process (AHP) is a methodology for determining the relative importance of the selection criteria. In our approach, the extended analysis on fuzzy AHP, as proposed by Chang [28], is adopted to determine the KPIs' weight vector.

The following steps of extent analysis on fuzzy AHP are applied. Let the N-dimensional fuzzy $PICM = \left[a_{ij}\right]$, $i, j = 1, \dots, N$; the fuzzy synthetic extent is defined by,

$$D_i = \left(D_i^l, D_i^m, D_i^u\right) = \sum_{j=1}^{N} a_{ij} \otimes \left(\sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}\right)^{-1} \tag{2}$$

We find the attribute with the higher fuzzy synthetic degree by computing the degree of possibility for a fuzzy number to be greater than other one,

$$\begin{aligned} V\left(D_i \geq D_j\right) &= hgt\left(D_i \cap D_j\right) \\ &= \begin{cases} 1 & \text{if } D_i^m \geq D_j^m \\ \frac{D_j^l - D_i^u}{\left(D_i^m - D_i^u\right) - \left(D_j^m - D_j^l\right)} & \text{if } D_i^m \leq D_j^m \text{ and } D_j^l \leq D_i^u \\ 0 & \text{otherwise} \end{cases} \end{aligned} \tag{3}$$

The degree of possibility that a fuzzy synthetic extent D_i is greater than the remaining synthetic fuzzy extents of the fuzzy PICM is,

$$d_i = V\left(D_i \geq D_k, \forall k = 1, \dots, N, k \neq i\right) = \min V\left(D_i \geq D_j\right) \tag{4}$$

Finally, the normalized weight vector of KPIs is obtained,

$$W = [w_1 \dots w_N] \text{ where } w_i = \frac{d_i}{\sum_{k=1}^{N} d_k} \tag{5}$$

Step 4. Evaluation of an experiment: Upon the completion of an experiment, the user is prompted to submit his/her judgment of the performance of the testbeds used. In order to mitigate the effect of malicious ratings, the experimenter's credibility is considered. Thus, for the QoS KPIs, the user's opinion x is properly modified to $\tilde{x}$ by the credibility mechanism of the following subsection. For the fuzzy KPIs, the experimenter evaluates the testbeds using the linguistic values of Table 2. For the numeric KPIs, the user assigns crisp values, which are converted to fuzzy numbers using

the membership functions of Table 2. Assume that the numeric evaluation $\tilde{x}$, modified by the credibility mechanism, corresponds to two adjacent linguistic values A and B and μ_A and μ_B are the respective membership functions. Then, the modified linguistic value $\tilde{X}$ that corresponds to the numeric evaluation is obtained by $\tilde{X} = \mu_A A + \mu_B B$. We use a virtual user's rating with Excellent linguistic values (E) for all KPIs in order to represent the best possible performance of the testbed. Thus, the obtained Fuzzy Evaluation Matrix (FEM) for the conducted experiment is,

$$FEM = \begin{array}{c} \\ U \\ V \end{array} \begin{array}{c} \begin{array}{cccc} K_1 & K_2 & \cdots & K_N \end{array} \\ \begin{bmatrix} \tilde{x_1} & \tilde{x_2} & \cdots & \tilde{x_N} \\ E & E & \cdots & E \end{bmatrix} \end{array} \tag{6}$$

where the first row of FEM corresponds to the modified experimenter's (U) opinion, while the second row corresponds to the perfect ratings of the Virtual user (V).

Step 5. Computation and update of reputation: In this step, the modified fuzzy VIKOR method is actually applied. Let the weight vector W and the fuzzy evaluation matrix $FEM = [x_{ij}]$, $i = 1, 2$, $j = 1, \ldots, N$; we determine the fuzzy best value $\tilde{f}_j^+$ and the fuzzy worst value $\tilde{f}_j^-$. Since the virtual user ratings are perfect, the fuzzy best and worst values are,

$$\tilde{f}_j^+ = x_{2j},\ j = 1, \ldots, N$$
$$\tilde{f}_j^- = x_{1j},\ j = 1, \ldots, N$$

Then, the separation measure of x_{ij} from the fuzzy best and worst value is obtained by,

$$\tilde{S}_i = \frac{\sum_{j=1}^{N} w_j \left(\tilde{f}_j^+ - x_{ij} \right)}{\tilde{f}_{j.u}^+ - \tilde{f}_{j.l}^-} \tag{7}$$

$$\tilde{R}_i = \max_j \left[\frac{w_j \left(\tilde{f}_j^+ - x_{ij} \right)}{\tilde{f}_{j.u}^+ - \tilde{f}_{j.l}^-} \right] \tag{8}$$

Next, the best and worst values of $\tilde{S}_i$, $\tilde{R}_i$ are calculated,

$$\tilde{S}^+ = \min_i \tilde{S}_i,\ \tilde{S}^- = \max_i \tilde{S}_i \tag{9}$$

$$\tilde{R}^+ = \min_i \tilde{R}_i,\ \tilde{R}^- = \max_i \tilde{R}_i \tag{10}$$

Then, the evaluation index $\tilde{Q}_i$ contains the fuzzy reputation score of the experimenter and the virtual user and is computed as,

$$\tilde{Q}_i = \alpha \frac{\tilde{S}_i - \tilde{S}^+}{\tilde{S}^- - \tilde{S}^+} + (1 - \alpha) \frac{\tilde{R}_i - \tilde{R}^+}{\tilde{R}^- - \tilde{R}^+} \tag{11}$$

where α is an index of our willingness to penalize the poor testbed performance or reward the good one; in order to have a balance between good and poor behavior. We set $\alpha = 0.4$, because the virtual user always has excellent ratings. We defuzzify the elements of $\tilde{Q}_i$, using (A6) to get the crisp reputation value of the experiment Q_i. The element Q_i with the minimum value has the best reputation score. Thus, in our case, the virtual user has the best score that is always zero ($Q_2 = 0$). For an experiment, the reputation score R_{exp} is defined as,

$$R_{exp}^T = (1 - Q_1)\, 100\% \tag{12}$$

After the n completed experiments, the overall reputation value of the testbed is updated as,

$$R_n^T = \frac{(n-1) R_{n-1}^T + R_{exp}^T}{n} \tag{13}$$

3.2. User's Credibility

The modified fuzzy VIKOR considers the credibility of the user for computing the reputation score in order to prevent malicious users from giving misleading evaluations. The QoE KPIs are excluded from our credibility mechanism, since they are subjective opinions of the experimenter and cannot be compared with any real measurement. On the contrary, the QoS KPIs can be compared with objective SLA and monitoring data, which consist of the ground truth of every experiment. Some reputation mechanisms, i.e., FTUE [8], define different categories of experimenters based on the comparison between their past evaluations and monitoring data, and their credibility varies accordingly. In our case, we do not assume any category of user's behavior. Our proposed mechanism leverages SLA and monitoring data to infer and update the credibility of experimenters in the federated environment.

Algorithm 1, presented below, shows how the user's credibility is calculated for a testbed of the experiment. If the experiment used more than one testbed, the credibility value was sequentially calculated for every testbed. The inputs of the credibility algorithm are the user opinion vector $UO = [UO_i]^\top,\ i = 1,\ldots,k$ containing the evaluations of the k QoS KPIs of the testbed, the SLA data vector $SD = [SD_i]^\top,\ i = 1,\ldots,k$ and the monitoring data vector $MD = [MD_i]^\top,\ i = 1,\ldots,k$, which contain the respective SLA and monitoring values for these KPIs. The output of the algorithm is the updated user's credibility CR and the modified user opinion vector $\widetilde{UO} = [\widetilde{UO_i}]^\top,\ i = 1,\ldots,k$ (Lines 1–2). For all KPIs of an involved testbed, four possible cases are identified (Lines 4–7). In the first case, named $CASE1$, the user's opinion and the monitoring value for a specific KPI are smaller than the SLA value, while in the second case, CASE2, both user's opinion and monitoring data satisfy the SLA. In CASE3 and CASE4, there is a significant deviation between the user's opinion and the monitoring data with respect to the predetermined SLA value. These cases correspond to suspicious ratings. More specifically, in CASE3, the user's opinion is lower than the SLA value, while the monitoring data show that the SLA is satisfied. In CASE4, the monitoring data are lower than the SLA value, while the user's rating is higher than the SLA value. Then, the relative errors of the monitoring and opinion values and the relative distance between the user's opinion and the actual monitoring value regarding the SLA are defined (Lines 8–9). The elements of the correction vector, $C = [c_i]^\top,\ i = 1,\ldots,k$, are actually the credibility value of each KPI. The values of the elements of C depend on which of the above cases is satisfied. The user's credibility for an experiment is calculated as the average value of the correction vector. Then, the overall user's credibility is updated (Lines 11–20). Furthermore, the user' opinion is updated according to the previously-defined cases (Lines 21–35). The modified opinions $\widetilde{UO}$ are used in Step 4 of the fuzzy VIKOR.

Algorithm 1 User credibility mechanism.

Inputs: $UO,\ SD,\ MD$
Outputs: $CR,\ \widetilde{UO}$
for $\forall UO_i \in UO$ **do**
  $CASE1 \equiv (SD_i \geq UO_i)\ \wedge\ (SD_i \geq MD_i)$
  $CASE2 \equiv (SD_i \leq UO_i)\ \wedge\ (SD_i \leq MD_i)$
  $CASE3 \equiv (SD_i > UO_i)\ \wedge\ (SD_i \leq MD_i)$
  $CASE4 \equiv (SD_i \leq UO_i)\ \wedge\ (SD_i > MD_i)$
  $e_M = \frac{|MD_i - SD_i|}{SD_i},\ i = 1, \ldots, k$, Monitoring Relative Error
  $e_O = \frac{|UO_i - SD_i|}{SD_i},\ i = 1, \ldots, k$, Opinion Relative Error
  $e_D = \frac{|UO_i - MD_i|}{SD_i},\ i = 1, \ldots, k$, Relative Distance
  $C = [c_i]^\top,\ i = 1, \ldots, k$, Correction Vector
  if $CASE1 \vee CASE2$ **then**
    $c_i = 1 - e_O$
  else if $CASE3 \vee CASE4$ **then**
    $c_i = 1 - (e_{Mi} + e_{Oi})$
  end if
  $c_i = max(c_i, 0)$
end for
$\hat{c} = avg(c_i)$
$CR_n = \frac{(n-1)CR_{n-1} + \hat{c}}{n}$
for $\forall UO_i \in UO$ **do**
  $\widetilde{UO_i} = UO_i$
  if $CASE1 \vee CASE2$ **then**
    if $UO_i \leq MD_i$ **then**
      $\widetilde{UO_i} = MD_i + e_{Oi} CR_n$
    else if $UO_i < MD_i$ **then**
      $\tilde{UO}_i = MD_i - e_{Oi} CR_n$
    end if
  end if
  if CASE3 **then**
    $\widetilde{UO_i} = MD_i - min(e_{Mi}, e_{Oi}) CR_n$
  end if
  if CASE4 **then**
    $\widetilde{UO_i} = MD_i + min(e_{Mi}, e_{Oi}) CR_n$
  end if
end for

4. Evaluation

The operation of the proposed reputation algorithm has been tested and evaluated in a real future Internet federation of testbeds in the context of the HELNETproject. The HELNET project [29] provides a federation of heterogeneous testbeds aiming to facilitate and promote test-driven research for the future Internet. The federation offers experimentation services in the fields of 4G/3G communications, WiFi networking, software-defined networking and software-defined radios. For the evaluation of the proposed reputation-based trust framework introduced here, the wireless NETMODE [30] and NITOS [31] testbeds are used in particular for demonstration purposes. Figure 2 illustrates the high-level architecture of the HELNET reputation service. The core of the reputation service is the reputation computation engine, where the two proposed reputation systems are developed using the Ruby on Rails MVC. The experimenters submit their evaluation on the portal of federation, while the reputation computation engine collects SLA and monitoring data from the testbeds through different APIs. The testbed management module is responsible for the administrative tasks of the reputation service. Finally, the reputation score of all testbeds and the credibility value of all users are stored in the reputation service repository.

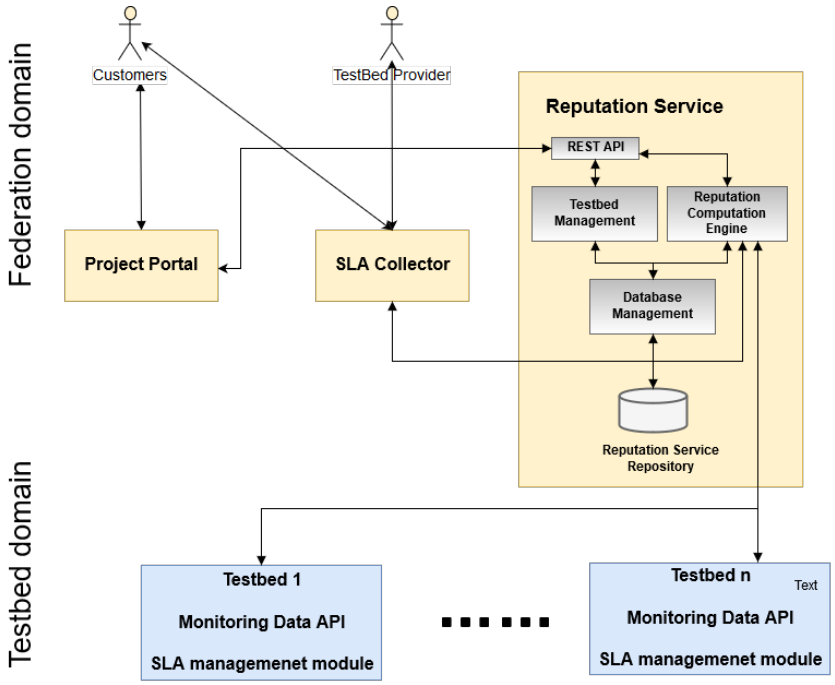


Figure 2. HELNET reputation service.

Initially, we demonstrate the evaluation of the proposed reputation algorithm for the two federated wireless testbeds with four KPIs. Three QoE KPIs are also utilized, i.e., document readability (K1), support satisfaction (K2) and operability (K3) focus on non-technical aspects, while node availability (K4) is the QoS KPI that measures the average availability of all reserved wireless nodes during an experiment. The user submits his/her rating of the reputation service, and in the following, we show the step-by-step computation of the experiment's reputation score, using the modified fuzzy VIKOR and the credibility value using Algorithm 1. In the second use case, one hundred users are assumed to have conducted two thousand experiments on the NETMODE testbed. This dataset contains a mix of random, honest and malicious ratings. This scenario demonstrates the key role of the credibility mechanism and the effect of the α parameter in Step 5. Finally, our proposed solution is compared against an existing reputation-based trust framework, named FTUE [8], which is designed for the federated facilities of FED4FIRE. As mentioned before, FTUE uses only crisp QoS and QoE KPIs

to infer the reputation of a testbed and the experimenter's credibility. In the following subsections, a higher score translates to better reputation for both reputation systems. Consequently, since the corresponding reputation values are obtained as a combination of the perceived users' experience and the usage of technical KPIs, we argue that a high reputation score is a strong indication that the testbed is better as a whole.

4.1. Fuzzy VIKOR Evaluation

In order to evaluate the fuzzy reputation system, the ratings of K1–K3 are obtained by linguistic terms of Table 2, which are mapped onto triangular fuzzy numbers (A1). The ratings of K4 are numeric and converted to fuzzy numbers according to Step 4 of the modified fuzzy VIKOR methodology. In the following paragraphs, we demonstrate the computations of each step of the fuzzy VIKOR methodology for the NETMODE testbed. The computations for the NITOS testbed are similar, and they are omitted. According to Step 2, the experimenter assigns the pairwise importance for each KPI with respect to the others, so we obtain the PICM,

$$PICM = \begin{array}{c} \\ K_1 \\ K_2 \\ K_3 \\ K_4 \end{array} \begin{array}{c} \begin{array}{cccc} K_1 & K_2 & K_3 & K_4 \end{array} \\ \begin{bmatrix} 1 & SW & SW & VW \\ SS & 1 & SW & FW \\ SS & SS & 1 & FW \\ VS & FS & FS & 1 \end{bmatrix} \end{array}$$

$$= \begin{bmatrix} (1,1,1) & (\frac{2}{3},1,1) & (\frac{2}{3},1,1) & (\frac{2}{5},\frac{1}{2},\frac{2}{3}) \\ (1,1,\frac{3}{2}) & (1,1,1) & (\frac{2}{3},1,1) & (\frac{1}{2},\frac{2}{3},1) \\ (1,1,\frac{3}{2}) & (1,1,\frac{3}{2}) & (1,1,1) & (\frac{1}{2},\frac{2}{3},1) \\ (\frac{3}{2},2,\frac{5}{2}) & (1,\frac{3}{2},2) & (1,\frac{3}{2},2) & (1,1,1) \end{bmatrix}$$

The consistency ratio of the defuzzified PICM, $CR = 0.018$, is acceptable. As described in Step 3 of Section 3.1, using the fuzzy extended analysis, we obtain the weight vector for the KPIs,

$$W_j = \begin{bmatrix} 0.109 & 0.199 & 0.233 & 0.46 \end{bmatrix}, \; j = 1, \ldots, 4$$

Then, the experimenter evaluates the fuzzy KPIs by using the linguistic variables in Table 2. For the numeric KPI, assume that the credibility mechanism modifies the user's opinion to 0.90; the SLA value was set at 0.80; and the monitoring data for this KPI is 0.85. The triangular membership function of the modified linguistic value $\widetilde{UO}$ is $\mu_{\widetilde{X}} = (7.9, 8.9, 9.9)$. According to the proposed method, we compute the testbed's reputation score for this experiment. The first row of FEM contains the experimenter's ratings for the KPIs, while the ideal ratings of the virtual user are in the second row,

$$FEM = \begin{array}{c} \\ E \\ V \end{array} \begin{array}{c} \begin{array}{cccc} K_1 & K_2 & K_3 & K_4 \end{array} \\ \begin{bmatrix} E & E & E & \widetilde{UO} \\ E & E & E & E \end{bmatrix} \end{array}$$

The fuzzy best value and fuzzy worst value are determined, and the separation measures are calculated according to (7)–(10). The evaluation indexes Q_i are calculated by (10); $Q_1 = 0.179$ and $Q_2 = 0$. Finally, the reputation score for this experiment is computed by (12),

$$R^T_{exp} = (1 - Q_1)\, 100\% = 82.1\%$$

The following example illustrates the performance of the reputation system and the credibility mechanism in the case of a suspicious evaluation. Assuming that $SD = 0.8$, $MD = 0.9$, $UO = 0.6$, the credibility mechanism modifies the user's opinion to $\widetilde{UO} = 0.8055$ with $\mu_{\widetilde{UO}} = (7.05, 8.05, 9.05)$, and the user's credibility decreases from 0.8 to 0.756. The final reputation value is computed as 73.9%. This case shows that the user is possibly malicious, and his/her credibility is reduced, while the testbed's reputation score is not significantly affected. The credibility mechanism is important to

alleviate the effect of misleading ratings. In the above example, if there were no credibility mechanism, the reputation value would be 66.7%. Finally, it is remarkable that the reputation system based on the modified fuzzy VIKOR is scalable considering the number of KPIs, because the reputation score is computed by simple fuzzy mathematical formulas.

In the second scenario, a dataset of two thousand experiments considers any possible case of the experimenter's behavior to highlight the effect of the credibility mechanism and the resilience of the proposed reputation system against malicious users and their ratings. The initial reputation score of the testbed is set to 0.5. In Figure 3, it is shown which case, CASE1–CASE4 of Algorithm 1, is valid for each experiment of the dataset. The first part of the dataset corresponds to experiments where the ratings are random with respect to SLA and monitoring values.

As shown in Figure 3, in the first part, named RANDOM, the small fluctuations of the reputation score are due to the random difference between monitoring value and the user's opinion. The implementation of the credibility mechanism improves the reputation score by 1%. Then, the reputation score increases rapidly, almost 6%, because the users are honest and their opinions agree with the monitoring data, as in CASE2 of Algorithm 1. In CASE3, the decrease of the reputation score is not steep, only 2%, because contrary to the user's opinion, the monitoring value is higher than the SLA. This case reflects the behavior of malicious users, who try to damage the reputation of a testbed. In CASE1, the users are rightly unsatisfied with the testbed's performance; thus, its reputation score decreases 5%. The last part of Figure 3 corresponds to CASE4, and some biased users try to enhance the testbed's reputation unfairly. However, the increase of the reputation score is negligible due to the fact that the monitoring value violates the SLA value. Furthermore, Figure 3 indicates that the credibility mechanism plays a key role in the robustness of the reputation system. More specifically, CASE3 and CASE4 illustrate that the reputation system without the credibility mechanism is not adequate against the malicious users. In CASE3 and applying the credibility mechanism, the reputation score is 4% higher than without this mechanism. Similarly, in CASE4 and using Algorithm 1, the output of the reputation system is 5% higher than the opposite case.

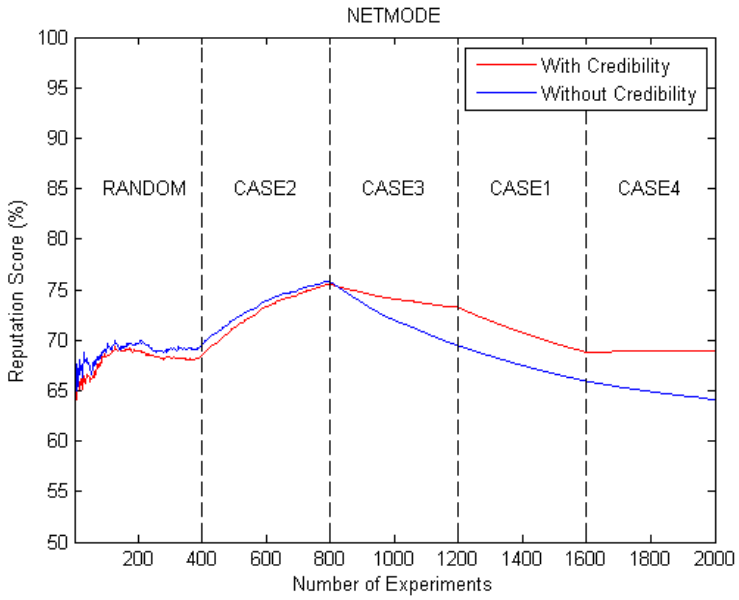


Figure 3. Credibility mechanism effect on the fuzzy VIKOR reputation system.

The most important parameter of the modified fuzzy VIKOR method is parameter α of Step 5. Large values of α mean that we penalize the poor testbed performance, while small values mean that we are lenient with the worse solution. It should be noted here that we compare our testbed performance with the ideal rating of a virtual user, which means that the experimenter's evaluation is always worse

than the virtual one. Figure 4 demonstrates the performance of the fuzzy reputation system for three different values of the α parameter. Generally, the smaller values of α produce higher reputation scores. Thus, for $\alpha = 0.5$, the produced reputation score is too small and does not encourage the experimenter to select a testbed even if it has actually good performance. On the contrary, in the case of $\alpha = 0.3$, the value is over-optimistic and cannot depict the real performance of the testbed. Furthermore, the reputation system ignores bad evaluations and is stiffer. Thus, the selected $\alpha = 0.4$ is a good trade-off that offers a realistic reputation score and enhances the sensitivity of the reputation system.

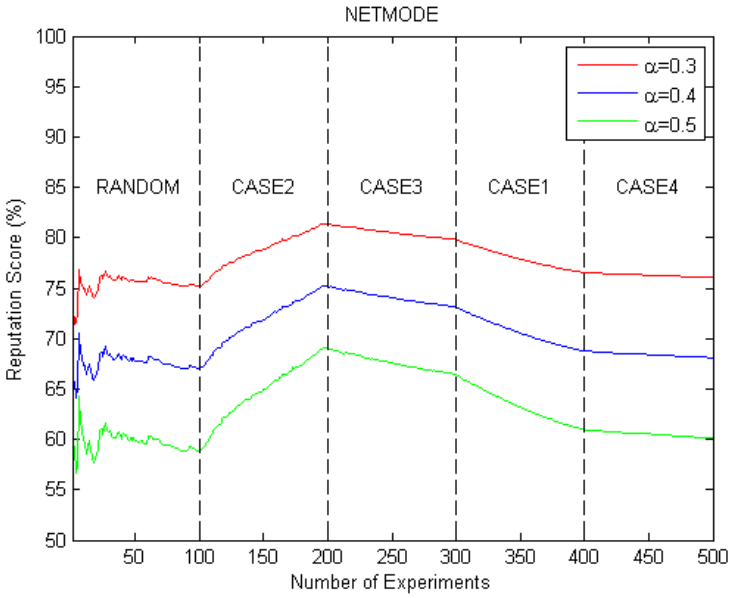


Figure 4. The effect of the α parameter on the modified fuzzy VIKOR method.

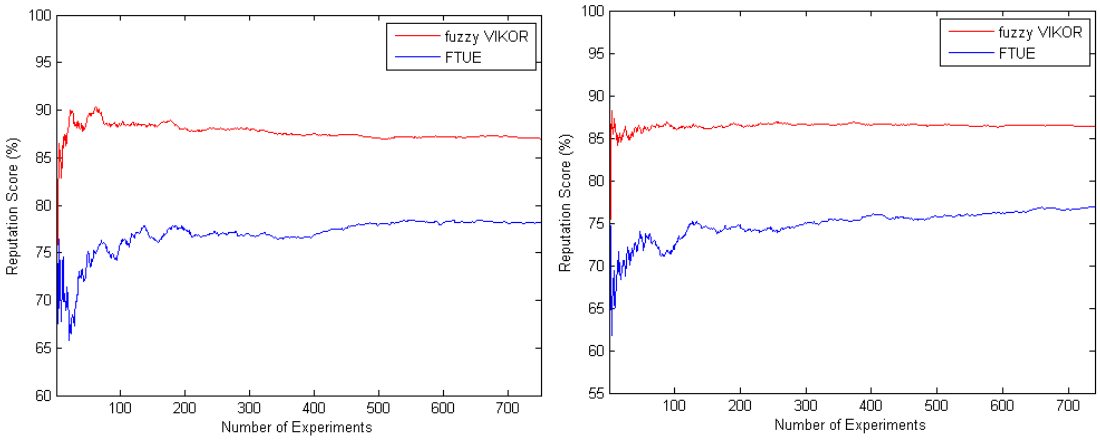
4.2. Comparison with the FTUE Framework

As mentioned earlier, FTUE [8] is a reputation-based trust framework for federated testbeds that uses numerical QoS and QoE KPIs and also provides a credibility mechanism. The FTUE framework assumed four types of experimenters with respect to the difference between the monitoring data and the user opinion, and the experimenter's credibility is updated accordingly. The reputation score per service per testbed is the aggregation of user opinions, weighted by the credibility and the confidence of the user for his/her evaluation. The FTUE framework does not take into account any SLA information.

We compare our proposed reputation system with the FTUE framework following the experimental settings of [8]. Eighty experimenters are truthful, and twenty experimenters are malicious in disguise, who reserve several testbeds and give biased evaluations only for one specific testbed. The nodes of one or both wireless testbeds are reserved by the users to conduct ten experiments and submit the respective ratings.

Figures 5a,b demonstrate the reputation score of the two approaches for the NETMODE and NITOS testbeds, respectively. For both testbeds, the reputation score computed by the FTUE framework is 10% lower than the fuzzy VIKOR approach. Three major remarks can be made regarding this result. First, the numerical evaluation of the FTUE framework is based on a five-star scale for evaluation, which provides coarse rating compared to the fine-grained numerical and fuzzy values of the proposed approach. Secondly, the FTUE credibility value depends heavily on the *Mu* parameter, which is testbed specific. For the results of Figure 5, we follow the experimental setup of the set in [8], and we set $Mu = 0.75$. For this value, we produce the best reputation score for both testbeds. Finally, the credibility mechanism of the compared reputation systems have two important differences that play a key role in their performance. First, our proposed mechanism leverages SLA data to quantify

the user's requirements and check if they are actually satisfied by comparison with the monitoring data. FTUE did not exploit any SLA data. Secondly, FTUE's credibility mechanism is based on four specific types of experimenter behavior, which are quantified by the difference between user's opinion and monitoring values. On the contrary, the proposed reputation system does not assume any specific categorization of user's behavior like the FTUE framework. In Lines 4–10 of Algorithm 1, four cases, CASE1–CASE4, and the necessary relative errors are defined in order to measure exactly the deviation of the user's opinion from the SLA and monitoring value without assuming any specific behavior and covering any possible scenario.



(**a**) NETMODE Testbed (**b**) NITOS Testbed

Figure 5. Comparison of fuzzy reputation system with the FTUEframework.

5. Conclusions

This article presents a fuzzy reputation-based trust framework for heterogeneous federated testbeds. The reputation system uses QoS and QoE KPIs and modifies the fuzzy VIKOR methodology to compute the reputation score of each testbed. Furthermore, the designed credibility mechanism, based on SLA and monitoring data, protects the testbeds' reputation score from malicious users. The proposed reputation system is compared and is shown to outperform the FTUE reputation framework, which is designed for experimental federated environment based only on numerical QoS and QoE metrics. This comparison underlines the importance of mixing several numerical and fuzzy metrics in the computation of the reputation score.

In our future plan, we intend to test the introduced fuzzy reputation-based trust framework with several types of testbeds, while using additional and more sophisticated QoS and QoE KPIs. Furthermore, the reputation score produced by the proposed system and the KPIs weights assigned by the users can be utilized by a recommendation algorithm in order to enable potential users to select the appropriate testbeds for their experiments. Finally, the proposed framework could be further extended and adopted on the one hand by infrastructure and/or service providers in promoting and advertising their services to potential users, while on the other hand, potential users may utilize it for selecting the most appropriate service.

Author Contributions: All authors contributed extensively to the work presented in this paper. S.P. formulated the original scientific problem of our current research work, contributed to the discussions and analysis of the comparative evaluation results and had the overall coordination in the writing of the article. D.D. designed the proposed trust framework and the evaluation experiments, led the discussions and analysis of the comparative evaluation results and had a key leading role in the article writing. I.D. developed the code of the trust framework, ran the evaluation and comparison experiment and contributed to the discussions and analysis of the comparative evaluation results. K.P.-V. produced the results of the FTUE framework, contributed to the discussions and analysis of the comparative evaluation results and had an active role in the writing of the article.

Funding: "This research was funded by the Greek General Secretariat of Research and Technology, Program "Hellenic Research Infrastructure HELNET", part of Initiative "HELIX-National Digital Infrastructures for Research" under Grant Agreement MIS 5002781."

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

QoS	Quality of Service
QoE	Quality of Experience
SLA	Service Level Agreement
SDN	Software-Defined Networks
NFV	Network Function Virtualization
VNF	Virtual Network Function
P2P	Peer-to-Peer
KPI	Key Performance Indicator
VIKOR	Visekriterijumsko Kompromisno Rangiranje
PICM	Pairwise Importance Comparison Matrix
CR	Consistency Ratio
AHP	Analytical Hierarchical Process
FEM	Fuzzy Evaluation Matrix

Appendix A. Preliminaries on Fuzzy Sets

The basic concepts of fuzzy numbers and their mathematical operations are presented in the following. Zadeh defined the fundamental concepts of fuzzy logic and sets in [32]. A fuzzy number A is a fuzzy set, and its corresponding membership function $\mu_A(x)$ must hold the following properties,

- $\mu_A(x) : \mathbb{R} \to [0,1]$, which means that it is a continuous and normalized fuzzy set.
- For exactly one element x_0, $\mu_A(x_0) = 1$.
- $\mu_A(x)$ is a convex fuzzy set.

In modified fuzzy VIKOR, we use positive Triangular Membership Functions (TMF), as shown in Figure A1, which are defined as,

$$\mu_A(x) = \begin{cases} \frac{x-l}{m-l} & \text{if } x \in [l,m] \\ \frac{u-x}{u-m} & \text{if } x \in [m,u] \\ 0 & \text{otherwise} \end{cases} \tag{A1}$$

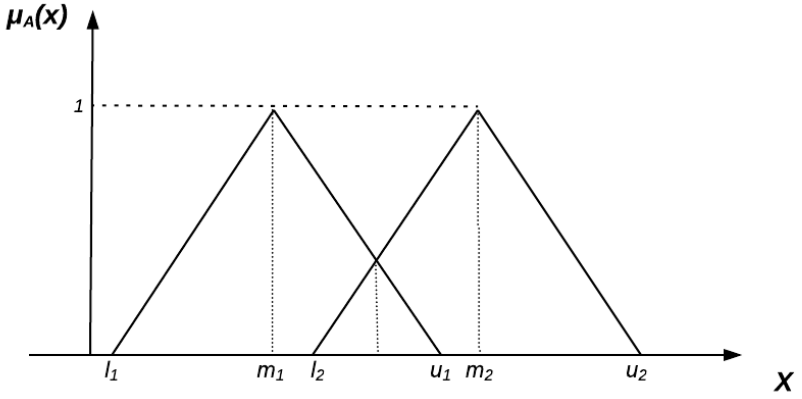


Figure A1. Triangular membership functions.

Assuming that $l \leq m \leq u$, a fuzzy number is denoted as the triplet $A = (l_A, m_A, u_A)$. The following mathematical operation between fuzzy numbers is defined according to [28],

$$A \oplus B = (l_A + l_B, m_A + m_B, u_A + u_B), \tag{A2}$$

$$A \ominus B = (l_A - u_B, m_A - m_B, u_A - l_B), \tag{A3}$$

$$A \otimes B = (l_A * l_B, m_A * m_B, u_A * u_B), \tag{A4}$$

$$A \oslash B = (l_A / u_B, m_A / m_B, u_A * l_B). \tag{A5}$$

The comparison of fuzzy numbers is not straightforward. The most common comparison method is the defuzzification of these numbers; converting them into crisp values. Many defuzzification methods have been proposed in the literature. Adopting the defuzzification approach of [25], the crisp value $\hat{A}$ of the fuzzy number A is defined as,

$$\hat{A} = \frac{l + 4m + u}{6} \tag{A6}$$

References

1. Wahab, O.A.; Bentahar, J.; Otrok, H.; Mourad, A. A survey on trust and reputation models for Web services: Single, composite, and communities. *Decis. Support Syst.* **2015**, *74*, 121–134. [CrossRef]
2. Gambetta, D. Can we trust trust? In *Trust: Making and Breaking Cooperative Relations*; Department of Sociology, University of Oxford: Oxford, UK, 2000; pp. 213–237.
3. FP7 FED4FIRE Project. Federation for Future Internet Research and Experimentation. Available online: https://old.fed4fire.eu/ (accessed on 22 May 2018).
4. H2020 FED4FIRE+ Project. Federation for FIRE Plus. Available online: https://www.fed4fire.eu/the-project/ (accessed on 22 May 2018).
5. GENI Project. Global Environment for Network Innovations. Available online: http://www.geni.net (accessed on 22 May 2018).
6. Dechouniotis, D.; Leontiou, N.; Dimitropoulos, X.; Kind, A.; Denazis, S. Unveiling the underlying relationships over a network for monitoring purposes. *Int. J. Netw. Manag.* **2009**, *19*, 513–526. [CrossRef]
7. Leontiou, N.; Dechouniotis, D.; Denazis, S.; Papavassiliou, S. A hierarchical control framework of load balancing and resource allocation of cloud computing services. *Comput. Electr. Eng.* **2018**, *67*, 235–251. [CrossRef]
8. Kapoukakis, A.; Kafetzoglou, S.; Androulidakis, G.; Papagianni, C.; Papavassiliou, S. Reputation-Based Trust in federated testbeds utilizing user experience. In Proceedings of the 2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Athens, Greece, 1–3 December 2014; pp. 56–60.
9. Ding, W.; Yan, Z.; Deng, R.H. A survey on future Internet security architectures. *IEEE Access* **2016**, *4*, 4374–4393. [CrossRef]
10. Nguyen, H.T.; Zhao, W.; Yang, J. A trust and reputation model based on Bayesian network for web services. In Proceedings of the 2010 IEEE International Conference on Web Services, Miami, FL, USA, 5–10 July 2010; pp. 251–258.
11. Malik, Z.; Bouguettaya, A. Rateweb: Reputation assessment for trust establishment among web services. *VLDB J.* **2015**, *18*, 885–911. [CrossRef]
12. Yahyaoui, H. A trust-based game theoretical model for Web services collaboration. *Knowl. Based Syst.* **2012**, *27*, 162–169. [CrossRef]
13. Ganeriwal, S.; Balzano, L.K.; Srivastava, M.B. Reputation-based framework for high integrity sensor networks. *ACM Trans. Sens. Netw.* **2008**, *4*, 1–37. [CrossRef]
14. Ren, Y.; Zadorozhny, V.I.; Oleshchuk, V.A.; Li, F.Y. A Novel Approach to Trust Management in Unattended Wireless Sensor Networks. *IEEE Trans. Mob. Comput.* **2014**, *13*, 1409–1423. [CrossRef]
15. Li, W.; Song, H. ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Trans. Syst.* **2016**, *17*, 960–969. [CrossRef]

16. Noor, T.H.; Sheng, Q.Z.; Yao, L.; Dustdar, S.; Ngu A.H.H. CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services. *IEEE Trans. Parallel Distrib. Syst.* **2016**, *27*, 367–380. [CrossRef]
17. Manuel, P. A trust model of cloud computing based on Quality of Service. *Ann. Oper. Res.* **2015**, *233*, 281–292. [CrossRef]
18. Tang, W.; Yan, Z. CloudRec: A Mobile Cloud Service Recommender System Based on Adaptive QoS Management. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Washington, DC, USA, 20–22 August 2015; pp. 9–16.
19. Yan, Z.; Zhang, P.; Vasilakos, A.V. A security and trust framework for virtualized networks and software-defined networking. *Sec. Commun. Netw.* **2016**, *9*, 3059–3069. [CrossRef]
20. Marconett, D.; Yoo, S.B. FlowBroker: A software-defined network controller architecture for multi-domain brokering and reputation. *J. Netw. Syst. Manag.* **2015**, *23*, 328–359. [CrossRef]
21. Kamvar, S.D.; Schlosser, M.T.; Garcia-Molina, H. The eigentrust algorithm for reputation management in p2p networks. In Proceedings of the ACM International Conference on World Wide Web, Budapest, Hungary, 20–24 May 2003; pp. 640–651.
22. Garg, A.; Battiti, R. *The Reputation, Opinion, Credibility and Quality (ROCQ) Scheme*; Technical Report DIT-04-104; University of Trento: Trento, Italy, 2004. Available online: http://eprints.biblio.unitn.it/705/1/TR-04-104.pdf (accessed on 22 May 2018).
23. Brinn, M.; Bastin, N.; Bavier, A.C.; Berman, M.; Chase, J.S.; Ricci, R. Trust as the Foundation of Resource Exchange in GENI. *ICST Trans. Sec. Saf.* **2015**, *15*, e1. [CrossRef]
24. Garg, S.K.; Versteeg S.; Buyya, R. SMICloud: A Framework for Comparing and Ranking Cloud Services. In Proceedings of the 2011 Fourth IEEE International Conference on Utility and Cloud Computing, Victoria, NSW, Australia, 5–8 December 2011; pp. 210–218.
25. Kaya, T.; Kahraman, C. Multicriteria renewable energy planning using an integrated fuzzy VIKOR & AHP methodology: The case of Istanbul. *Energy* **2010**, *35*, 2517–2527.
26. Alabool, H.M.; Mahmood, A.K. Trust-based service selection in public cloud computing using fuzzy modified VIKOR method. *Aust. J. Basic Appl. Sci.* **2013**, *7*, 211–220.
27. Coyle, G. The analytic hierarchy process (AHP). In *Practical Strategy: Structured Tools and Techniques*; Pearson Education Ltd.: Harlow, UK, 2004; pp. 1–11.
28. Chang, D.Y. Applications of the extent analysis method on fuzzy AHP. *Eur. J. Oper. Res.* **1996**, *95*, 649–655. [CrossRef]
29. GSRT HELNET Project. Available online: https://nitlab.inf.uth.gr/NITlab/projects/40-projects/current/599-helix (accessed on 22 May 2018).
30. NETMODE Testbed. Available online: http://www.netmode.ntua.gr/main/index.php?option=com_content&view=article&id=103&Itemid=83 (accessed on 22 May 2018).
31. NITOS Testbed. Available online: https://nitlab.inf.uth.gr/NITlab/nitos (accessed on 22 May 2018).
32. Zadeh, L.A. Fuzzy sets. *Inf. Control* **1965**, *8*, 338–353. [CrossRef]