CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE
Concurrency Computat.: Pract. Exper. (2011)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/cpe.1825

LFTM, linguistic fuzzy trust mechanism for distributed networks

Félix Gómez Mármol [1,*,†], Javier G. Marín-Blázquez [2] and Gregorio Martínez Pérez [3]

[1] *Network Research Division, NEC Laboratories Europe, Kurfürsten-Anlage 36, 69115, Heidelberg, Germany*
[2] *Departamento de Ingeniería de la Información y las Comunicaciones, University of Murcia, Facultad de Informática, Campus de Espinardo, 30.071, Murcia, Spain*

SUMMARY

Trust is, in some cases, being considered as a requirement in highly distributed communication scenarios. Before accessing a particular service, a trust model is then being used in these scenarios to determine if the service provider can be trusted or not. It is done usually on behalf of the final user or service customer, and with a little intervention of him or her. This is usually happening with the main aim of automatizing the process and because trust models are normally making use of reasoning mechanisms and models difficult to understand by humans. In this paper, we propose the adaptation of a bio-inspired trust model to deal with linguistic fuzzy labels, which are closer to the human way of thinking. This Linguistic Fuzzy Trust Model also uses fuzzy reasoning. Results show that the new model keeps the accuracy of the underlying bio-inspired trust model and the level of client satisfaction, while enhancing the interpretability of the model and thus making it closer to the final user. Copyright © 2011 John Wiley & Sons, Ltd.

Received 29 December 2010; Revised 8 April 2011; Accepted 18 June 2011

KEY WORDS: Linguistic fuzzy models; trust management; wireless networks

1. INTRODUCTION

The Internet, with its services, has changed our life in the last few years. In fact, we are using it as a way to access online services and applications ranging from simple Web pages with news to online payment systems or e-banking solutions. For the first set of services, trust is advisable, but in most cases, it is not a must. However, for the latter, trust represents a key requirement that should be considered by any user before obtaining access to a service.

Traditional ways of managing trust are no longer applicable when dealing with highly distributed scenarios. To deal with these scenarios, new models have been designed and implemented in the last few years. They are based on different techniques, including fuzzy systems, Bayesian networks, bio-inspired models, social networks, or analytic expressions, among others.

However, most of these techniques usually offer a low level of interpretability of the results being provided as part of the model. As trust is a sensible issue for humans, clients feel more comfortable if they understand how the trust management process works. Poorly interpretable models make difficult both the interaction between the final client and the model and the sense and rationale that users can make of the results being provided by the trust model.

The human mind has the remarkable capability to perceive and reason using words instead of numbers. It is, in fact, the more natural way in which people express and acquire their experience and knowledge. Interestingly, most of the words used to describe perceptions or categories are rather vague and imprecise. Temperature perceptions are usually referred to with words such as ‘warm’,

*Correspondence to: Félix Gómez Mármol, Network Research Division, NEC Laboratories Europe, Kurfürsten-Anlage 36, 69115, Heidelberg, Germany.
†E-mail: felix.gomez-marmol@neclab.eu

'hot', or 'cold' instead of precise measurements or numbers. Science and computers usually work with numbers. In fact, science has been working quite hard to go from perceptions to measurements.

Nevertheless, even with the great successes of this numeric approach, the description of the systems based on measurements tend to be quite difficult to understand, even for experts. It would be interesting to express knowledge about a system using these rather vague words and allow automatic optimization techniques to provide useful models that, using such human words, still provide competitive performances.

Fortunately, there exists a representation and inference tool that allows for that hybridization in a natural way. Such a tool is fuzzy logic. In the work proposed in this paper, linguistic fuzzy logic and fuzzy reasoning provide the framework for knowledge representation, model transparency, and inference for a trust model for distributed environments. An ant-colony optimization will be guided using such Linguistic Fuzzy Trust Model (LFTM). The resultant system is able to provide a platform that achieves very high levels of client satisfaction. This system is, at the same time, easy to interpret, thanks to the use of linguistic fuzzy logic, and is very efficient in its job of providing a good service.

The paper is structured as follows. Section 2 describes the linguistic fuzzy approach and mentions some related work for trust and reputation management. Next, in Section 3, the underlying base trust model is described. Section 4 covers the newly proposed linguistic fuzzy-enhanced trust model. The experiments and results are described in Section 5. Finally, the paper ends in Section 6 where the main conclusions and some future work lines are being presented.

2. BACKGROUND

2.1. *Fuzzy sets*

'Everything is vague to a degree you do not realize till you have tried to make it precise, and everything precise is so remote from everything that we normally think, that you can not for a moment suppose that is what we really mean when we say what we think' [1]. Bertrand Russell states here that humans do not normally think in very precise terms. He also suggests that precision move us away from what we really think. In fact, it is interesting to note that validity of most human concepts is a matter of degree [2]. Therefore, any natural way to express our thinking should allow for the use of vague words.

Fuzzy sets [3] are sets where a member can have partial membership. This provides a good tool to represent the aforementioned vague concepts, categories, or perceptions that human mind is so familiar with. A typical fuzzy set (Figure 1) usually has some members with full membership in a kind of core, prototype, or canonical elements (point b in the figure). There are also some other members with decreasing membership as we move away from the core (points c, a, and d, respectively, in decreasing membership value). This can easily represent the usual category that has some elements that comply with all the characteristics; therefore, we are certain of its categorization. At the same time, there are some other elements that may not comply with all the characteristics, or maybe there is not enough information to be sure, or perhaps the case presents other sources of uncertainty about the membership. These latter elements may still be considered in such category, but, by using fuzzy sets, they will belong with a reduced or partial membership. The fuzzy membership of a value x, defined on a domain D, to a fuzzy set S is usually represented as $\mu_S(x) \in [0..1]$.

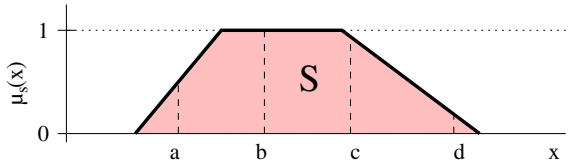


Figure 1. A typical fuzzy set defined over a real domain.

DOI: 10.1002/cpe

It is very important not to mistake fuzziness for probability as they refer to two very different forms of uncertainty. Probability allows to measure the confidence of an expected outcome of a future event that, eventually, will happen, and do so in a precise way. But fuzziness represent the degree of appropriateness of an element being considered as a something, as a member of a group, or as an example of a concept. For example, to say that Patricia is 0.9 very intelligent would mean, in fuzzy terms, that the concept of being very intelligent is very appropriate to describe the intelligence level of Patricia. But to say the same sentence in probability terms would mean that Patricia acts as a very intelligent person 9 out of 10 times, while there will be one time when she behaves as a fool. Clearly, in many situations in real life, fuzziness is the most appropriate way to represent what humans think about the world than probability.

2.2. Linguistic fuzzy logic

One of the most useful features of fuzzy sets is the possibility of attaching a linguistic label, that is, a word, to them [4]. This allows the membership degree of an element to the set to represent the confidence of such element being described by the word. In a way, the membership degree represents the appropriateness degree for an element to be described by the word (the linguistic label).

This use of linguistically labeled fuzzy sets is called linguistic fuzzy approach. This use is not to be confused with the most commonly found precise fuzzy approach. In the precise approach, the fuzzy sets are defined to better fit the data instead of being defined to better fit the words given by humans. Precise fuzzy models are universal approximators with similar performances to neural networks and, to some extent, functionally equivalent to them [5]. Unfortunately, precise fuzzy modeling also shares with neural networks, although to a far less extent, the poor understandability.

In this work, a pure linguistic fuzzy approach is used [6]. This provides transparent models easy to understand. Although this usually comes at the cost of precision, the proposed model is powerful enough as to produce underlying models that match the human-given definitions for the linguistic fuzzy sets without a loss in performance.

In linguistic fuzzy systems, the most common approach is to obtain a fuzzy set first and then associate a linguistic label to such a set [7, 8]. In a way, this is a pseudo-linguistic approach rather than pure linguistic, because the human semantically meaningful words are attached, a posteriori, to computer-generated (usually by data-driven methods) fuzzy sets. In some cases, such attachment may produce awkward associations. The underlying rationale is trying to obtain nice data grouping fuzzy sets and rely on the human skill to manage the real language plasticity, thus giving the human user the responsibility to find an adequate word for such grouping. In summary, in this pseudo-linguistic approach, the computer tells the humans what are the interesting sets to use, and humans find a suitable word to semantically attach to them.

But in the current work, a more human-oriented approach, and in a sense, a more pure linguistic approach, is followed. Here, the usual attachment of labels is performed in the reverse order. That is, given a word or a linguistic label, a human user defines the fuzzy set that matches his subjective semantics about that word. In other words, humans tell the linguistic fuzzy system which words to use, which is his own semantic concept of the word, and the system would try to obtain the best results while using such particular semantic notion of that human user for these words.

So, in this way of creating the semantic attachment between words and fuzzy sets, the elements with total confidence of being represented by the word would obtain full membership values to the underlying fuzzy set. Likewise, elements with less confidence obtain reduced fuzzy membership proportional to the decrease in confidence.

2.3. Fuzzy partitions and the linguistic approach

So fuzziness allows a quantitative domain to be transformed into a quasi-qualitative one with soft boundaries between the different categories. The process of converting a number into a fuzzy word is called fuzzification. Note, however, that not any group of fuzzy set definitions can be used naturally as categories for a variable. In order to be a useful set of categories defined over a domain, some properties should be taken into consideration for the fuzzy definitions and domain partitions. These constraints on the membership functions increase its semantic interpretability [9].

DOI: 10.1002/cpe

One of such important properties is called completeness or coverage, which states that any value of the domain should have some membership to at least one fuzzy set. This means that the categories should cover all possible values. Normality, or that each category have, at least, a value with full membership, is also important to have because a concept that is always somewhat vague is rather questionable and not too representative. Yet another useful property is distinguishability, that is, that no point can have full membership to more than one fuzzy set. This means that the categories do not overlap in its representative values. If they do overlap, then one of the categories would be superfluous and confusing and may easily lead to inconsistencies.

An example would clarify these properties. Let the domain being the water temperature be used in a bath. Let us consider the linguistic (fuzzy) labels to be used in the domain as 'too hot', 'hot', 'nice', 'cold', and 'too cold'. Coverage means that, given any temperature (t), it will have some membership value for at least one of the fuzzy sets, that is, any temperature t is either somewhat (or definitely, depending on the membership value) 'too hot' or 'hot' or 'cold' or 'too cold'. Normality means that each label has a range of (or a single) temperature values where we are certain it fully complies our subjective idea of the label, that is, there is a temperature we are certain that is cold for a bath, or that is definitely too cold, or hot, and so on. If one of the labels does not have temperatures with full membership, let say, nice, then it means that nice is a vague concept never to be sure of. There will always be an uncomfortable feeling of not having a truly nice bath no matter how we play with temperature. These vague concepts should be avoided if possible, although then again, it is a recommendation and not a need. Finally, distinguishability means that there is not a temperature that is, at the same time, fully compliant with two or more labels, that is, no temperature is definitely hot and too hot at the same time with full confidence. If we add the label 'safe' to represent temperatures that would not kill a bath user (either by hypothermia or by boiling him or her), then the system would not be distinguishable as a 'nice' temperature but a 'safe' temperature. Although in some cases, this kind of overlapping may have advantages most of the time just shows that the semantic system can be simplified by removing some labels. It may also show that two abstraction levels have been mixed or that are present at the same time in the representation. indistinguishability is a situation to be handled with great care as it may easily lead to confusion and/or inconsistencies. At the same time, it may provide simpler (because of the abstraction) sets of rules. In the present case, it has been decided not to mix different abstraction levels and keep distinguishability in the semantic labels utilized.

In the current work, a strong fuzzy partition will be used to define the underlying fuzzy sets (that will be linguistically labeled). A strong fuzzy partition has the following properties being S_i the fuzzy sets defined over the domain D and x a value of such domain:

$$\forall i, \exists x \in D, \mu_{S_i}(x) = 1 \tag{1}$$

$$\forall x \in D,\ \exists i, j\ \forall k \quad i \neq j, k \neq i, k \neq j, \quad \mu_{S_i}(x) + \mu_{S_j}(x) = 1 \quad \mu_{S_k}(x) = 0 \tag{2}$$

The first expression ensures normality. The second expression states that any particular value of the domain can belong, at most, to two different fuzzy sets (S_i or S_j) and that the addition of the membership values for any given value of the domain is equal to one. Note that this last expression implies both $\forall x \sum_i \mu_{S_i}(x) = 1$ (sum of all memberships equals one) and $\forall x, \exists i, \mu_{S_i}(x) > 0$ (coverage). Figure 2 shows a typical strong fuzzy partition. Linguistic labels L_i will be associated with each defined fuzzy set S_i.

2.4. Trust and reputation management

Previous subsections have given us a broad view on fuzzy theory (fuzzy sets and fuzzy logic) as well as linguistic labels. As aforementioned, the main goal of the work at hand is to enhance a previous trust and reputation management model by benefiting from the advantages of expressivity of fuzzy sets and linguistic labels.

DOI: 10.1002/cpe

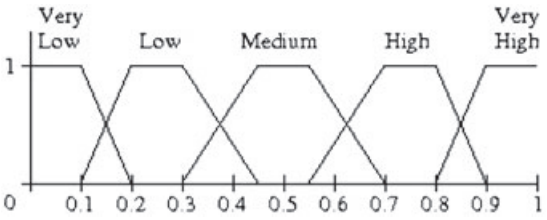


Figure 2. Linguistic labels and its defining fuzzy sets.

Thus, regarding trust and reputation management in distributed and heterogeneous systems [10–13], it is important to point out that it has recently arisen as a novel and powerful solution to cope with some of the current harmful threats [14–16] that slow down the comprehensive deployment and usage of the so-called information technologies.

In those distributed and heterogeneous scenarios or environments where there is a lack of a public key infrastructure, or a central authority monitoring and supervising the proper behavior of the members within a community, accurate mechanisms to avoid malicious users to perform ill-intentioned interactions are needed. Such malicious entities must be, therefore, precisely identified and isolated, preventing this way benevolent users to deal with them.

Many efforts have been done so far in this direction, addressing the issue of trust and reputation management in several environments. Thus, for instance, a number of trust and reputation models have been designed and developed for systems ranging from peer-to-peer networks [17–19], to wireless sensor networks (WSNs) [20–23], to (mobile) ad hoc networks [24–26], to multiagent systems [27, 28], or even to vehicular-to-vehicular networks [29–31].

Recently, trust and reputation management has been also applied to some popular fields such as the so-called cloud computing [32–34], identity management and identity federation [35–37], Web services [38–40], and the so-called Internet of Things [41]. Hence, it is remarkable that the wide acceptance as well as a range of scenarios where the application of a trust and reputation model has been found to be very useful and appropriate.

It is worth mentioning that some authors have already applied bio-inspired algorithms in order to perform such trust and reputation management. Some examples are Quality of Service-based Distance Vector Protocol [21], AntRep [42], Time-based Dynamic Trust Model [43] (which make use of ant colony systems [44] and ant colony optimization [45]), and the one that constitutes the basis of our new proposal, called Bio-inspired Trust and Reputation Model for WSN (BTRM-WSN) [46].

In turn, some other researchers exploited the benefits of fuzzy logic and fuzzy representation in order to deal with this topic, leading this way to the development of models such as Comprehensive Reputation-Based Trust Model With Fuzzy Subsystems [47], A Fuzzy Reputation Agent System [48], or Pervasive Trust Management [26], among others. Nevertheless, to our best knowledge, this is one of the first works combining both methodologies in this field, bio-inspired algorithms and fuzzy logic, profiting from the advantages of each. Bio-inspired techniques have been proved to obtain quite good outcomes. At the same time, the expressivity achieved by the use of fuzzy logic and linguistic labels make the models that use them more human interpretable.

This paper is an enhanced version of a previous paper [49], but in this new version, the background section has been enhanced, and a deeper explanation of the technique being presented has been provided. Additionally, a more detailed experimentation and a new comparison study have been added as parts of the new version of this paper.

3. BASE TRUST MODEL

Our enhancement proposal is based on a previous trust and reputation management scheme for WSNs called BTRM-WSN [46]. In this section, we will summarize the functionality of this trust and reputation mechanism aimed to be applied in WSNs. Its main goal is to provide each sensor

DOI: 10.1002/cpe

in a WSN with an accurate mechanism to decide which other sensor to have a transaction with, according to the reputation of the latter within the community.

This model considers five types of sensors, as it can be observed in Figure 3, namely clients, executing the algorithm in order to find the most reputable server providing a certain service; benevolent servers, providing a good service; malicious servers, providing a worse service than the one they offer; relay nodes, not offering the requested service; and those sensors that swap into an idle state in order to save some energy and that are therefore momentarily not reachable.

BTRM-WSN is a bio-inspired algorithm based on an ant colony system [44], where pheromone traces represent the probability of finding the most reputable sensor through the most trustworthy path. This model fulfills the five generic steps for a trust and reputation model proposed in [10, 50], as shown next.

1. Gathering information
   When the algorithm is launched, a set of artificial ants are deployed over the network. Those ants leave some pheromone traces throughout the paths they travel. Their goal is to find the most trustworthy node providing a certain service, required by the client executing BTRM-WSN. To do so, they follow the pheromone traces left by previous ants. Thus, the greater the pheromone trace a specific path has, the more suitable such route is to be selected as the one leading to the most reputable node.
2. Scoring and ranking
   Once the ants have found a path leading to a node providing the requested service, a score has to be given to each of those paths. Such assessment is performed through the following expression:

$$Q(S_k) = \frac{\overline{\tau}_k}{Length(S_k)^{PLF}} \cdot \%A_k, \tag{3}$$

   where S_k is the path returned by ant k, $\overline{\tau}_k$ is the average pheromone of such path, $PLF \in [0, 1]$ is a path length factor, and $\%A_k$ represents the percentage of ants that have selected the same solution as ant k.

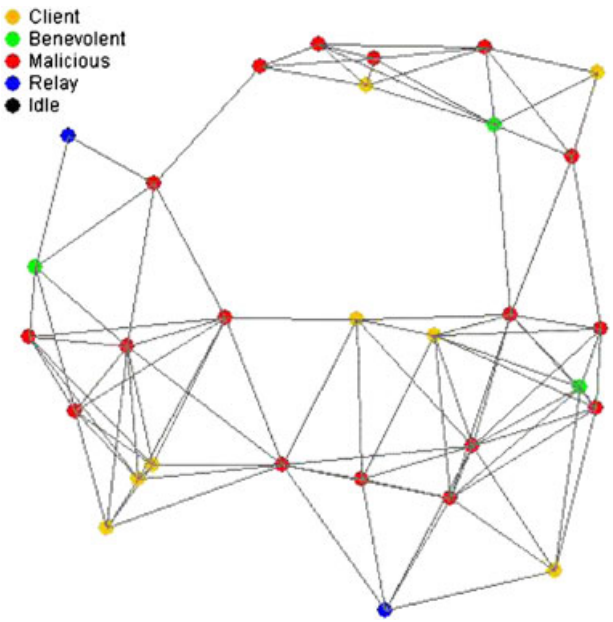


Figure 3. Bio-inspired Trust and Reputation Model for Wireless Sensor Network: a sample wireless sensor network.

DOI: 10.1002/cpe

3. Entity selection
   The path S_i with the highest value of $Q(S_i)$ is selected by BTRM-WSN as the one leading to the most trustworthy server in the network.
4. Transaction
   The client explicitly requests the service to the selected node who will provide such service (the one he was offering) or even a worse one depending on his goodness. The client then evaluates the received service and computes his satisfaction with the performed transaction.
5. Rewarding and punishing
   If the client was satisfied with the received service, a reinforcement in terms of pheromone addition to the path leading to the final service provider is carried out. Otherwise, if the server cheated, a punishment in terms of pheromone evaporation is carried out. Thus, we either promote such path (so future ants will choose it with higher probability) or we downgrade it (having less opportunities to be selected again).

The core of this trust and reputation model consists of the adaptation of the ant colony system algorithm, as shown in Algorithm 1.

The first change we can appreciate is that the main loop is now defined by a generic condition, which may be a certain number of iterations (like in the original algorithm) or it can even be a certain time-out. This definition will depend on the specific WSN this model is going to be applied to. Furthermore, as shown in [16], this approach is also resilient to several security threats specifically applicable to this kind of systems.

```
while (condition) do
  for k = 1 to Number_of_ants do
      S_k ← initial sensor (client)
      Launch ant k

  do
      for every returned ant k do
          if (Q(S_k) > Q(Current_Best)) then
              Current_Best ← S_k
  while (timeout does not expire) and
  (Num_returned_ants < %Number_of_ants)

  if (Q(Current_Best) > Q(Global_Best)) then
      Global_Best ← Current_Best

  Pheromone_global_updating(Global_Best, Q(Global_Best), ρ)

return Global_Best
```

Algorithm 1. Bio-inspired Trust and Reputation Model for Wireless Sensor Network.

As we will see next, the main enhancement we want to achieve, with regards to this BTRM-WSN model, consists of providing a higher interpretability and expressiveness of concepts such as client satisfaction, sever goodness, quality of service, punishment or reward, amongst others. These advanced features will be reached thanks to the application of fuzzy sets, fuzzy logic, and linguistic labels.

4. LINGUISTIC FUZZY TRUST MODEL

The main objective of the current proposal is to assess the application of linguistic fuzzy sets and fuzzy logic to several concepts to enhance our trust and reputation model. On one hand, it will be enjoyed the representation power of linguistically labeled fuzzy sets, as is the case, for instance, of

DOI: 10.1002/cpe

the satisfaction of a client or the goodness of a server. On the other hand, it will be exploited the inference power of fuzzy logic, as in the imprecise dependencies between the originally requested service and the actually received one, or the punishment to apply in case of fraud. The expected outcome will be an easy-to-interpret system with competitive performance.

As mentioned, a set of linguistic labels describing several levels of a variable or concept could be associated to a fuzzy set. The set is defined in a way that captures the underlying notion of such word for that particular concept. Typical linguistic labels include 'very low', 'low', 'medium', 'high', and 'very high'. The defined fuzzy sets associated to such labels for the case of client satisfaction are depicted in Figure 2.

Human users usually have a common sense or an experience-based notion of the dependencies between related concepts. It is also quite common that such perceived dependencies are imprecise in nature. A simplistic example is the common sense-based notion that states that a tall person tends to be quite heavy in weight. That can be expressed as 'IF *person* is Tall then *person* is Heavy', with Tall or Heavy being fuzzy concepts. Linguistic fuzzy if–then rules are an adequate representation and inference tool for such type of knowledge.

Fuzzy rules can be expressed in several forms. For the case of study, a fuzzy grid will be used and explained later. A rule is composed of an antecedent part, where the activation condition is expressed, and a consequent part, where an action or a conclusion is presented. The antecedent is usually a logic expression. In fuzzy rules, a basic logic expression is the membership of a variable value to a set as in '*person* is Tall'. These basic expressions are then connected with logic connectives, being the most common, the AND operator. Likewise, the most common consequent is the membership of an output variable to a fuzzy concept. These are known in fuzzy terminology as Mamdani-type rules. In fuzzy logic, the truth value of logical expressions is not binary but ranges from zero to one allowing for partial truth. The fuzzy logic operators, AND, OR, and NOT are adapted to allow for such partial truth. Fuzzy operators also produce a partial truth value to the whole logic expression. A typical if–then linguistic fuzzy rule would look like

$$\begin{aligned} &\text{If quality is Good AND } \textit{price} \text{ is Low} \\ &\text{THEN } \textit{satisfaction} \text{ is Very High} \end{aligned} \tag{4}$$

The perception of quality being good or price being low may vary from total confidence to no confidence at all. But, unlike traditional logic, it may also be any value in between. In other words, a price being low can be partially true. This partial truth for each condition is combined through the fuzzy AND operator, and the whole logic sentence of the antecedent is so evaluated. As can be guessed, the truth value of the consequent part is precisely that one achieved by the whole antecedent logic expression.

So if, for example, the truth value of the expression 'quality is Good AND price is Low' is 0.3, then the system concludes that the expression 'satisfaction is Very High' has a truth value of 0.3. When in a given situation, several fuzzy rules are activated, a collection of conclusions is produced. These separate conclusions are aggregated into a final result and, if needed, defuzzified back into a numerical value. Details of how fuzzification, fuzzy inference, aggregation, and defuzzification work can be found in [51, 52] . The defuzzification method chosen to be used in this research work is Center of Gravity.

A fuzzy grid is a collection of fuzzy rules in a matrix form. Each row/column represents one of the input variables. In order to represent the whole input space, each row and column includes all the linguistic labels defined over the represented input variable. Remember that, the way in which the fuzzy sets were defined in this work, using a strong fuzzy partition, ensures that any measured value in a variable would have some membership to, at least, one linguistic fuzzy concept (and at most to two), so full coverage is obtained. Each cell in the matrix represent an AND combination of its row/column truth-valued labels, that is, the antecedent of the fuzzy rule. The content of the cell represents the consequent of the rule. Therefore, a fuzzy grid represents as many rules as cells it has. Of course a fuzzy grid can have more than two dimensions.

Each domain has linguistic variables that are more appropriate to use than others. Temperature uses 'warm' or 'hot', length uses 'long' or 'short', and width uses 'wide' or 'thin'. In this work, to

DOI: 10.1002/cpe

keep things simple and to avoid distractions, very generic labels, which can be used in most domains, were used. Nevertheless it is encouraged to use the most natural words/labels for the categories in each variable domain when applied for real. In Table I, the sets of labels used in each variable are shown.

Figure 4 depicts the flow of our approach, emphasizing those steps where we actually applied linguistic fuzzy sets and fuzzy logic. Such steps are as follows:

1. The trust and reputation model BTRM-WSN selects the server to have a transaction with.
2. Such server has a perceived certain goodness ('very high', 'high', 'medium', etc.).
3. According to the required service attributes and the server goodness, the server provides a better, worse, or equal service than the expected.
4. Both the required service and the actually received one are compared using certain subjective and client-dependent weights for the service attributes.
5. The client satisfaction is assessed by means of the service comparison performed in the previous step and the client conformity.
6. Finally, the punishment level is determined by the client satisfaction with the received service, together with his or her goodness.

Next, it will be described the different fuzzy grids used in the proposed model. The tables were created using the knowledge of a human expert and follows a very intuitive notion of the relation among variables. Table II(a) represents the fuzzy rules followed by a server when it decides the quality of the service to be provided. Such decision depends on the server goodness and the requested quality of the service. As can be seen in the grid, very good servers actually provide better services than the requested ones and vice versa. Table II(b) shows the rules used by the servers to decide the price of the service to be provided. In this case, the decision depends on server goodness and the price of the requested service. By looking at the grid, it is easy to see that, for example, if the goodness of the server is 'very high' and the price of the requested service is 'high', then the price of the actually provided service will be 'low'.

In this work, it has been defined a service that is composed by four perceived properties: price, cost, quality, and delivery time. Tables II(c) and II(d) show the fuzzy rules that describe how the user perceives a comparison between same features of two services. The first table (c) is used when comparing attributes where the higher the value the better, as in quality. The second table (d) does

Table I. Sets of linguistic labels used in the different variables.

Variable	Labels
Price, server goodness, quality of service, client satisfaction, client conformity	Very low, low, medium, high, very high
Attribute comparison	Much worse, worse, similar, better, much better

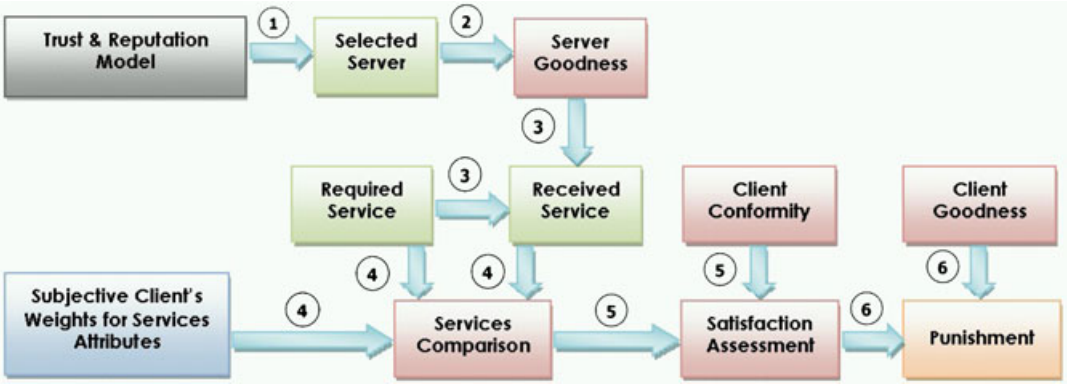


Figure 4. Linguistic Fuzzy Trust Model steps.

DOI: 10.1002/cpe

Table II. Linguistic Fuzzy Trust Model fuzzy rules.

(a) Quality of service provided.

	Required service attribute				
Server goodness	VL	L	M	H	VH
VL	VL	VL	VL	L	M
L	VL	VL	L	M	H
M	VL	L	M	H	VH
H	L	M	H	VH	VH
VH	M	H	VH	VH	VH

(b) Price of the service to be provided.

	Required service attribute				
Server goodness	VL	L	M	H	VH
VL	M	H	VH	VH	VH
L	L	M	H	VH	VH
M	VL	L	M	H	VH
H	VL	VL	L	M	H
VH	VL	VL	VL	L	M

(c) Comparing attributes when the higher the better.

	Service 1 attribute				
Server 2 attribute	VL	L	M	H	VH
VL	S	B	MB	MB	MB
L	W	S	B	MB	MB
M	MW	W	S	B	MB
H	MW	MW	W	S	B
VH	MW	MW	MW	W	S

(d) Comparing attributes when the lower the better.

	Service 1 attribute				
Server 2 attribute	VL	L	M	H	VH
VL	S	W	MW	MW	MW
L	B	S	L	MW	MW
M	MB	B	S	W	MW
H	MB	MB	B	S	W
VH	MB	MB	MB	B	S

(e) Client satisfaction.

	Services similarity				
Client conformity	MW	W	S	B	MB
VL	VL	VL	VL	L	M
L	VL	VL	L	M	H
M	VL	L	M	H	VH
H	L	M	H	VH	VH
VH	M	H	VH	VH	VH

(f) Level of reward.

	Client satisfaction				
Client Goodness	VL	L	M	H	VH
VL	VL	VL	VL	L	M
L	VL	VL	L	M	H
M	VL	L	M	H	VH
H	L	M	H	VH	VH
VH	M	H	VH	VH	VH

VL, very low; L, low; M, medium; H, high; VH, very high; MW, much worse; W, worse; S, similar; B, better; MB, much better.

DOI: 10.1002/cpe

the opposite, that is, it compares features where the lower the value the better, as in price or delivery time.

Once the client receives the service from the server, it compares its attributes individually with the corresponding attributes of the requested service. In our proposal, a client can establish certain subjective weights to each property comparison (a client might consider the price much more important than the quality or the delivery time, or vice versa, for instance). Therefore, a weighted aggregation of the two services property comparison is performed in order to obtain the final service comparison.

Such comparison, together with the client conformity, provides the final client satisfaction with the received service. This assessment is performed by means of the fuzzy rules shown in Table II(e). Thus, a very conformist client will be most of the times highly satisfied, regardless of the behavior of a server (even if it is malicious and provides a worse service than the requested one). On the contrary, a very exigent client will need a very good service in order to be satisfied; otherwise, his or her satisfaction will be 'low' or 'very low'.

Finally, the client satisfaction, together with the client goodness, will decide the level of reward/punishment to be applied to the selected server. Table II(f) shows the fuzzy rules that describe such imprecise relation. A very benevolent client might not want to apply a high punishment (small negative reward), even if he or she was highly unsatisfied (very low satisfaction). But if the client is not that benevolent, then most of the times, a high or very high punishment will be carried out.

If the client satisfaction is 'medium' or higher, the client is supposed to be satisfied, and a reward is performed. Otherwise, the client is supposed to be dissatisfied, and the corresponding punishment is carried out.

Usually, but not necessarily always, both client conformity and goodness might be very related issues. Nevertheless, the main reason for separating both concepts was to make our proposal as much generic as possible, so that it can be applied in a wider variety of scenarios and real use cases.

4.1. Decision surfaces

One of the main features of using linguistic fuzzy rules is that the soft boundaries between categories, and the way that fuzzy reasoning works, provide for smooth transitions between the different output levels. A graphical example of the difference between using the standard rules or using the proposed linguistic rules can be seen in Figures 5 and 6. This feature has several important

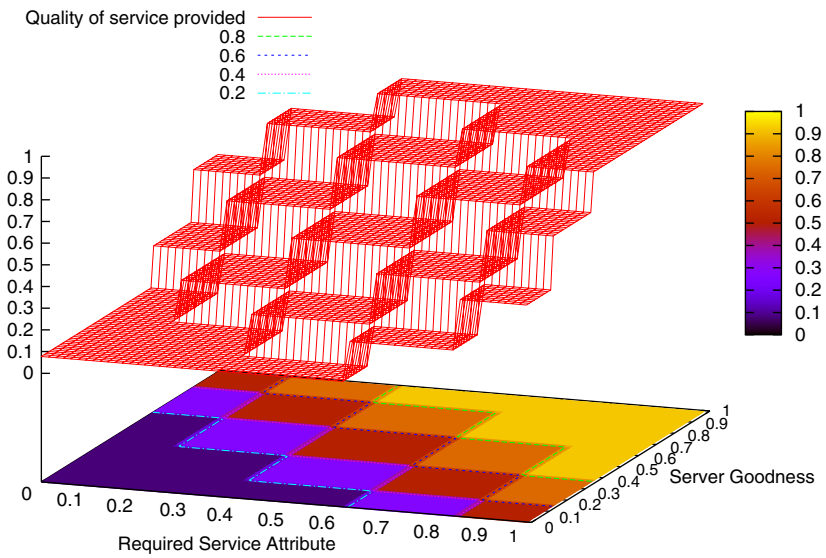


Figure 5. Quality of service provided using traditional (crisp) rules.

DOI: 10.1002/cpe

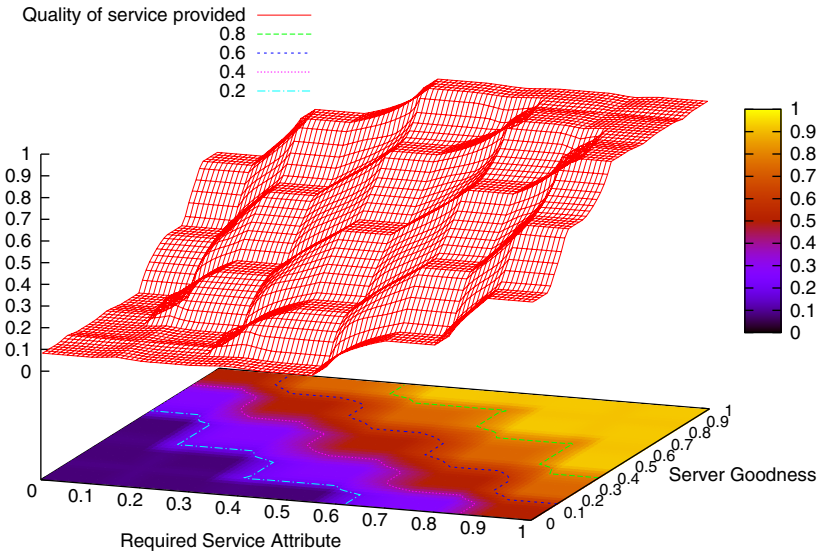


Figure 6. Quality of service provided using linguistic fuzzy rules.

advantages to the proposed system. The first advantage is, as mentioned before, that fuzziness is a more natural representation of the human knowledge about the dependencies between the variables involved. Humans like thinking in vague qualitative terms more than in quantitative ones.

Another advantage, related with the previous one, is that there is no sharp (crisp in the fuzzy logic terminology) change in behavior when the variables have values close to the neighborhood areas of several categories. This feature provides for more stability in the learning process and in the behavior. Besides, most real-life systems show progressive transitions between output levels. It is true that such a progressive transition may show a softer or a steeper slope but almost never a sharp all-or-nothing situation. Even more, when some systems are forced to show such black-and-white behavior, a typical example being the legal system, it clearly shows signs of inadequacy or shortfalls. An example of this, using the aforementioned legal system, is the aberrant situation of an action being a very serious and severely punishable offense or not depending on being committed with a day difference, that is, the day of your legal adult-age birthday or just the day before. Other examples include being fined for speeding or not depending on a 1-km/h difference or paying substantially more or less taxes for a euro/dollar-income difference. Ironically, such systems try to alleviate such shortfalls by adding aggravating or mitigating factors in order to obtain a decision surface more similar to Figure 6 than to Figure 5, but it is performed by adding many complexity to the system in the form of exceptions, safeguard offsets, new black-or-white conditions that add or subtract certain values to the final output, or by directly using corrective factors to modulate the output. Fuzzy rules, instead, provide a powerful and elegant way of capturing the imprecise or degree-based dependencies yet maintaining simplicity and transparency.

A final advantage, that will be further discussed in Section 5.2, is that fuzzy systems are, by its own nature, quite resilient to low precision in the input variables. This means that the measures used to characterize the different features of servers and clients, as server goodness or client conformity, are not required to be very precise. On the other hand, crisp (nonfuzzy) systems usually are very sensitive to the smallest imprecision. As the previous example of legal age clearly shows, a mistake of a few days in the determination of the age of the perpetrator can have very serious consequences; therefore, there is an imperative need in such cases of clearly establishing the exact age of the individual, or the exact speed, or the exact alcohol level in blood, and so on. But as fuzzy decision surfaces, small mistakes usually have just small consequences or, at least, far lesser consequences than a crisp system. How this advantage affects the proposal described here will be further developed in Section 5.2.

DOI: 10.1002/cpe

5. EXPERIMENTS AND RESULTS

In this section, two different set of experiments carried out will be presented. The evaluation environment used in this research work was Trust and Reputation Model Simulator for WSN [53], a generic framework aimed to serve as an assistant tool in order to easily implement and compare trust and reputation mechanisms in distributed environments.

5.1. Bio-inspired Trust and Reputation Model versus Linguistic Fuzzy Trust Model with homogeneous servers and clients

The first set of experiments were performed in order to test the accuracy of the new proposal as well as the enhancement achieved with regards to the previous model where no fuzzy logic was applied. The main aim of this first set was to make a comparison between fuzzy and crisp approaches; hence, some limitations were imposed to the fuzzy version in order to be fair in such a comparison. Such limitations are to fix the values of client conformity and client goodness to 'medium' and to fix the value of server goodness to 'very high' for good servers and 'very low' for malicious servers.

Table III summarizes the parameters used to perform the first set of experiments. We have measured the selection percentage of trustworthy servers, as well as the length of the path leading to such nodes, and the percentage of 'types of satisfaction'; all of them over static networks where neither the topology nor the goodness of each peer varied along the time.

5.1.1. Selection percentage of trustworthy servers. The first result refers to the percentage of trustworthy service providers that each model (BTRM-WSN and LFTM) have been able to achieve. Thus, Figure 7(a) shows the performance of BTRM-WSN on this respect. As it can be observed, the accuracy of the model decreases as the percentage of malicious servers and the total number of nodes increases. However, even in the worst case of a network composed by 500 peers where 90% of the servers are malicious, BTRM-WSN can still succeed and select the appropriate service provider in near the 80% of the cases.

In Figure 7(b), the corresponding result for LFTM have been shown. A slight enhancement has been achieved here, as it can be checked. In most of the cases, the accuracy of the model is never below 95%. Only with the biggest networks, this percentage decreases to a minimum of around 90% (when the amount of malicious nodes is maximum).

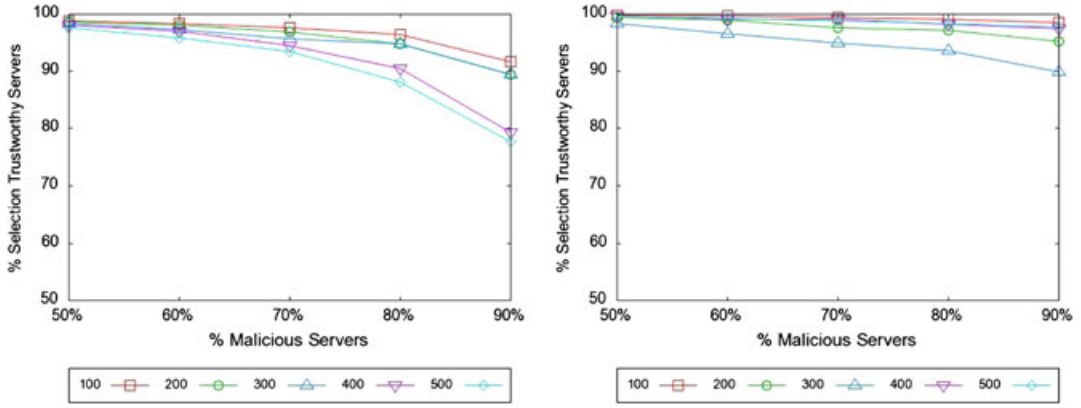
This improvement is mainly due to the reward and punishment mechanism. Because the goodness and conformity values of a client are 'medium' (according to Table III), when a malicious server is

Table III. LTFM experiment parameters.

Network	NumExecutions	100	%Clients	15%
	NumNetworks	100	%Relay	5%
	MinNumSensors	{100, 200, 300, 400, 500}	%Malicious	{50%, 60%, 70%, 80%, 90%}
	MaxNumSensors	{100, 200, 300, 400, 500}	Radio range	{8.92, 6.31, 5.15, 4.46, 3.99}
BTRM	phi	0.01	Nants	0.35
	rho	0.87	Niter	0.59
	TraTh	0.66	PLF	0.71
	alpha	1.0	q0	0.45
	beta	1.0	IniPh	0.85
	PunTh	0.48		
LFTM	benevolentServerGoodness	'Very high'	clientConformity	'Medium'
	maliciousServerGoodness	'Very low'	clientGoodness	'Medium'
	costWeight	0.25	priceWeight	0.25
	deliveryWeight	0.25	qualityWeight	0.25

BTRM, Bio-inspired Trust and Reputation Model; LTFM, Linguistic Fuzzy Trust Model.

DOI: 10.1002/cpe



(a) (b)

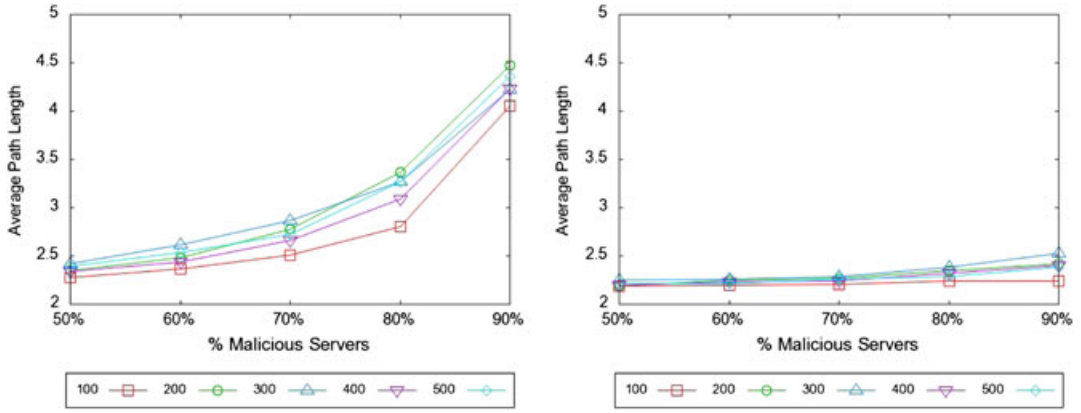
Figure 7. Selection percentage of trustworthy servers: (a) Bio-inspired Trust and Reputation Model for Wireless Sensor Network; (b) Linguistic Fuzzy Trust Model.

unfortunately selected to provide the required service, the service actually provided is 'much worse' than the expected one. Therefore, the satisfaction of the client is 'very low' (Table II(e)), and the reward is 'very low' (Table II(f)) as well, which actually means that a slight punishment is carried out.

This means that when a benevolent server is found, the path leading to such node is highly reinforced (by means of pheromone contribution), and because we are dealing with static networks, such benevolent peer will be very likely to be selected in the future. However, if a malicious service provider is found, the pheromone evaporation applied throughout the path leading to it will not be too severe. This allows forthcoming ants to explore the network in the vicinity of such cheater, so if honest peers are around there, they still can be discovered.

5.1.2. Path length. The second experiment measured the length of the path suggested by each model, leading to the most trustworthy node found. It is worthy to mention here that by adjusting the radio range of the nodes of each network, we are able to have, on average terms, the same number of neighbors regardless the size of the network.

Knowing this, outcomes obtained for BTRM-WSN model can be observed in Figure 8(a). It shows the fact that, as the percentage of malicious severs increases, it is more difficult to find the most trustworthy one, and the ants have to explore longer paths. Additionally, the high punishment



(a) (b)

Figure 8. Path length: (a) Bio-inspired Trust and Reputation Model for Wireless Sensor Network; (b) Linguistic Fuzzy Trust Model.

DOI: 10.1002/cpe

applied when a malicious provider is chosen might force ants to try alternative (and maybe longer) paths in order to find the benevolent nodes. However, in the worst case, the average length of the paths is between 4 and 4.5 hops.

Regarding LFTM, Figure 8(b) depicts its corresponding outcomes for this particular experiment. As we can see, LFTM is able to find closer reputable nodes. The reason is again the same. Because those paths leading to malicious nodes are not so strongly punished, ants can still explore in the proximity of the client. Thus, the largest average path length achieved by LFTM in this experiment is around 2.5 hops from the client.

5.1.3. Client satisfaction. Lastly, we measured in this last experiment the percentage of clients who were 'very high', 'high', 'medium', 'low', and 'very low' satisfied, respectively. The outcomes can be observed in Figure 9.

As expected, most of the clients had either a 'very high' or just a 'high' satisfaction, and this proportion remains almost invariable regardless the size of the network. It slightly worsens, however, as the percentage of malicious server increases. In such situation, some clients had 'low' or even 'very low' satisfaction.

5.2. Linguistic Fuzzy Trust Model with heterogeneous servers and clients

Although the previous experiment was aimed to compare, in similar terms, the BTRM and LFTM, the following experiment will explore a more realistic situation. The previous experiment fixed the goodness values of servers allowing only two levels of the variable, namely 'very high' and 'very low' as to represent benevolent and malicious servers. Likewise, the client conformity and goodness was also fixed to 'medium'. Note that the effect of this is that, from the whole fuzzy tables, only a row or a column is actually used. For example, in the case of client conformity whose fuzzy table is in Table II(e), only the mid row (the 'M' for medium) would be used to obtain the client satisfaction given a service similarity. This limitation has a sense for a fair comparison with BTRM but does not represent a more realistic situation.

In real life, each server and each client has its own features. For example, although two servers may be labeled as malicious, they may be in a different degree. At the same time, each client may vary in its conformity or its goodness. It is unrealistic to expect that all clients have the same level of conformity or goodness, and incidentally, it would be restrictive to do so as well. Therefore, an experiment will be performed where such conditions vary and allows for individual differences for both servers and clients.

Table IV summarizes the general parameters used to perform this second experiment. It has been measured again the selection percentage of trustworthy servers, as well as the length of the path leading to such nodes, and the percentage of 'types of satisfaction'.

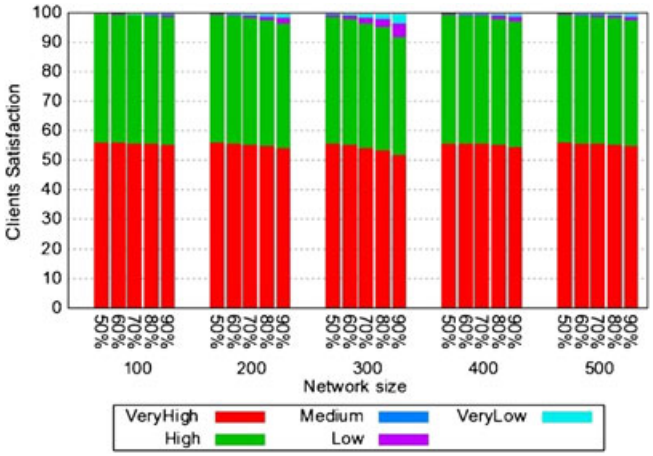


Figure 9. Linguistic Fuzzy Trust Model: client satisfaction.

DOI: 10.1002/cpe

Table IV. Random LTFM experiments parameters.

Network	NumExecutions	100	%Clients	15%
	NumNetworks	100	%Relay	5%
	MinNumSensors	{100, 200, 300, 400, 500}	%Malicious	{50%, 60%, 70%, 80%, 90%}
	MaxNumSensors	{100, 200, 300, 400, 500}	Radio range	{8.92, 6.31, 5.15, 4.46, 3.99}
LFTM		Server Goodness		Client
	Benevolent	'High' or 'very high'	Conformity	Random
	Malicious	'Low' or 'very low'	Goodness	Random
	costWeight	0.25	priceWeight	0.25
	deliverWeight	0.25	qualityWeight	0.25

LTFM, Linguistic Fuzzy Trust Model.

This time, both client conformity and goodness are random for each client, thus creating unique individuals. The goodness/maliciousness of the servers is also random in this experiment, but the proportions between good and malicious servers are kept. These proportions are kept as to be able to compare with the homogeneous version of the experiment, which has these proportionality between good and malicious serves. Note, nevertheless, that in the heterogeneous version, there are different degrees of goodness and maliciousness. The method to keep the proportions of good/malicious, while allowing for randomness in the degrees of it, works by assigning a random value between 0 and 0.4 for the experiment proportion of malicious servers (thus falling in the labels low and very low for server goodness) and a random value between 0.6 and 1 for the proportion of benevolent servers (thus having scores that correspond to the labels high and very high for server goodness).

As mentioned the proposed system was designed to allow for a more realistic grasp of real situations, and these experiments try to reflect it. Of course, this raises the question of how the system would obtain the real-life values that in the experiments are randomly taken. That is, how do we measure the goodness or maliciousness of a server, or a client? There are several ways of doing so. Regarding the client conformity and goodness values, these can be acquired through, for example, self-assignation by the client. Of course, this can be done in cases where there is a high confidence in the cooperativeness and honesty of the clients and in situations where no abuses of this privilege are expected. Another way would be to calculate an estimation of these values based on past behavior of the client. It has to be reminded that the client is expected to express later its degree of satisfaction as feedback. Consistently, low feedback on good service may suggest low client conformity. A third way of deciding these values can be to let the system administrator set them. Such assignment can be carried out based on the load of the network, efficiency, or using schemas where conformity and goodness reflects a payment for service usage. For example, premium paying users would be scored as quite nonconformist and not too good as to ensure good services, whereas free access users would be scored opposite, meaning that they cannot be too demanding when receiving free or low-cost services.

Likewise, with regard to the server goodness, the scores can be assigned based on previous history, performance, feedback of clients, or left to the system administrator's discretion. In summary, obtaining estimations of these values for specific real-life clients or servers should not be a problem.

Here, again, it should be mentioned the advantage of fuzzy systems to allow for, and being quite resilient to, imprecise inputs. The aforementioned scores or values for the servers and clients can be just estimations and do not need for very precise values. Of course, the better the estimation is, the better the results are, but it is not a critical component at all. As the surface shown in Figure 6 suggests, small variances of the values do not substantially change the output variable that depends on such values. Again, as Figure 5 shows, such allowance for small errors in the measurement that fuzzy systems show are not shared by its crisp counterpart. In the Figure 5 example, a server goodness value of 0.85 and 0.849999 have quite different quality of service provided if the required service has values between 0 and 0.625.

Before explaining the results for this experiment, it should be noted that, in general, the heterogeneous version of the problem is more difficult to solve because of the increased complexity.

DOI: 10.1002/cpe

5.2.1. Selection percentage of trustworthy servers. The results depicted in Figure 10 show the percentage of trustworthy service providers that are able to achieve both the linguistic fuzzy model with diverse types of servers and clients (a) next to the results previously shown over a homogeneous environment (b). The results show that for the heterogeneous case, it actually obtains better results as the number of untrustworthy serves increases. The reason is that the ants spread a given total amount of pheromone and that when the number of good servers is small, the paths to these are more strongly selected. In a way, the fewer the number of good servers is, the easier is for them to shine or excel. But while in the homogeneous case the pheromone would be evenly shared by all good servers, and thus the overall paths to them become damped down in the case of heterogeneous goodness, the few very best would even be more pheromoned than other good but not so great ones, and the paths to them would shine more, few paths but more secure to lead to good servers.

On the other hand, this effect may suggest that the system may lead to bottlenecks if it is overloading the very best servers while other good ones are also around. Future work would have to watch for this potential problem and ways to counter it.

Nevertheless, the results for the heterogeneous experiment, which is harder than the homogeneous one, are still highly successful regarding locating trustworthy servers over 90% of the cases in the worst case and over 95% when there are a few good servers.

5.2.2. Path length. With respect to path length (see Figure 11), a similar effect with the selection of trustworthy servers happens. The heterogeneous LFTM obtains better results as the number of good

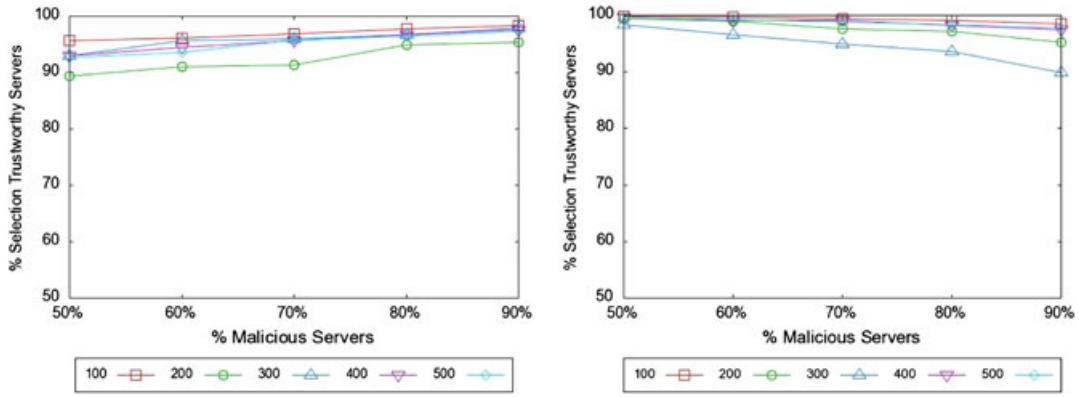


Figure 10. Selection percentage of trustworthy servers: (a) Linguistic Fuzzy Trust Model heterogeneous; (b) Linguistic Fuzzy Trust Model homogeneous.

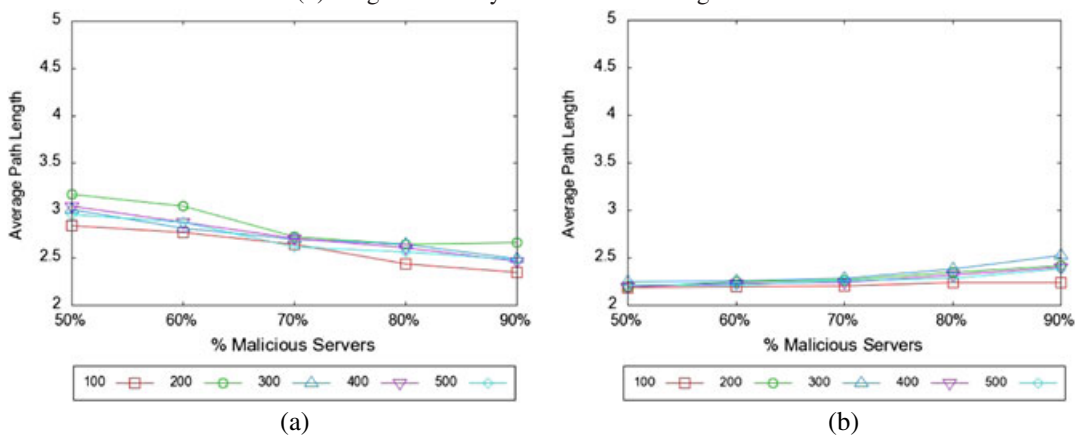


Figure 11. Path length: (a) Linguistic Fuzzy Trust Model heterogeneous; (b) Linguistic Fuzzy Trust Model homogeneous.

DOI: 10.1002/cpe

servers available decreases. Again, the average path lengths from client to server that are obtained in the harder experiments are still competitive, between 2.5 and 3.

5.2.3. Client satisfaction. One interesting effect of having all types of potential clients can be seen in the results on satisfaction shown in Figure 12. Whereas in the previous experiments, most clients ended with a 'very high' or just a 'high' satisfaction, in the new experiment, there are a substantial number of 'medium' satisfaction. This is something to be expected, just by looking at Table II(e). Such table is used to obtain the client satisfaction. Note that a client with very low (VL) conformity would, at most, achieve a medium (M) satisfaction and that only when the client obtains a much better (MB) service similarity. So in the system, there are a substantial number of clients that will never achieve better satisfaction than medium. Besides, depending on the quality of the attributes required, even such satisfaction may not be obtained by the same effect. By looking at Tables II(c) and II(d), it is again clear that a 'much better' result may not be achievable for certain labels, so the client satisfaction of a client with 'very low' conformity can be quite poor.

Even with such difficulties, more than two thirds of the clients fall in the 'very high' and 'high' categories, and almost the other third achieve a 'medium' satisfaction. That can be considered as a great result, taking into consideration the aforementioned ceiling effect for certain groups of clients. Again, as the number of benevolent servers decreases the ant algorithm focuses on the few good ones increasing the efficiency in finding and reaching them.

6. CONCLUSIONS AND FUTURE WORK

Trust and reputation are concepts with which we deal every day. Trust and reputation management in distributed environments has been recently proposed as a mechanism for tackling certain risks not fully covered by traditional network security schemes, obtaining reasonably good results.

Many approaches have been followed for handling these elements. In this paper, we combined two of them, obtaining the benefits and advantages of each one. We have therefore applied linguistic fuzzy logic and fuzzy sets to a previous bio-inspired trust and reputation model for WSNs.

By doing this, we enhance the interpretability of the model, making it more human friendly, or human readable, while keeping, and even improving, the accuracy of the underlying trust and reputation model.

As for future work, we are planning to test our proposal in a wider spectrum of scenarios, for instance, dynamic networks with nodes continuously entering and leaving the community, or oscillating ones, where the behavior of service providers might change along the time.

Besides, it would be monitored if the system may be overloading the very best servers, and if that is the case, changes will be proposed to counter such an effect.

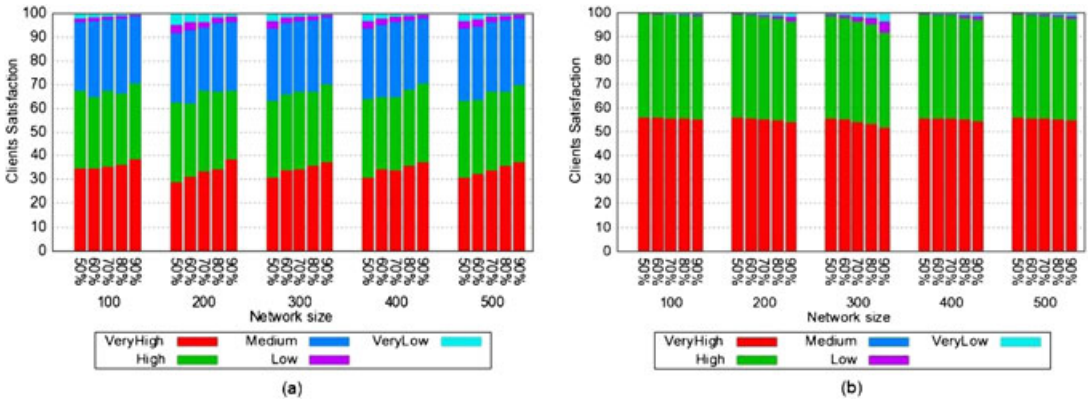


Figure 12. Client satisfaction: (a) Linguistic Fuzzy Trust Model heterogeneous; (b) Linguistic Fuzzy Trust Model homogeneous.

DOI: 10.1002/cpe

Finally, it is worthy to mention that the outcomes obtained in the experiments presented in this paper are directly related to the definition of the fuzzy sets presented in Figure 2. A small variation of those underlying fuzzy definitions would likely change these results as the paths were discovered by the ants using these particular definitions. Because there is a rather long chain of fuzzy decisions (Figure 4), the variations in results, if alternate definitions are used, would accumulate. Note, however, that this is also true for any crisp systems and in a more acute way as transitions are not soft. Fuzzy rules and fuzzy reasoning are, in general, more resilient to such noise than crisp rules or systems. The degree of such resilience to small changes in the underlying fuzzy set definitions while keeping unmodified the ant-discovered paths is an interesting line for future experiments. Likewise, another line would be testing the performance of the ant algorithm for very different definitions as this would show the robustness of its optimization independently of the human words being used.

ACKNOWLEDGEMENTS

This work has been supported by a Séneca Foundation grant within the Human Resources Research Training Program 2007 (code 15779/PD/10) and has been undertaken in the context of SEISCIENTOS project, 'Providing Adaptive Ubiquitous Services in Vehicular Contexts' (TIN2008-06441-C02), funded by the Spanish Ministry of Science and Innovation. Thanks also to the Funding Program for Research Groups of Excellence, granted as well by the Séneca Foundation with code 04552/GERM/06.

REFERENCES

1. Russell B. *The Philosophy of Logical Atomism and Other Essays, 1914–19*, McMaster University edn. Allen & Unwin: London; Boston, 1986.
2. Zadeh LA. From computing with numbers to computing with words—from manipulation of measurements to manipulation of perceptions. *American Institute of Physics* 2001:36–58. DOI: 10.1063/1.1388678. Available from: http://link.aip.org/link/?APC/573/36/1.
3. Zadeh LA. Fuzzy sets. *Information and Control* 1965; **8**:338–353.
4. Zadeh LA. The concept of a linguistic variable and its application to approximate reasoning - I. *Information Sciences* 1975; **8**:199–249.
5. Jang JSR, Sun CT. Functional equivalence between radial basis function networks and fuzzy inference systems. *IEEE Transactions on Neural Networks* Jan 1993; **4**(1):156–159.
6. Marín-Blázquez JG, Shen Q. From approximative to descriptive fuzzy classifiers. *IEEE Transactions on Fuzzy Systems* Aug 2002; **10**:484–497.
7. Casillas J, Cordón O, Herrera Triguero F, Magdalena L (eds). *Studies in fuzziness and soft computing*, Vol. 128. Springer: Heidelberg, 2003.
8. Setnes M, Babuska R, Verbruggen HB. Transparent fuzzy modelling. *International Journal of Human-Computer Studies* 1998; **49**(2):159–179. Available from: http://dx.doi.org/10.1006/ijhc.1998.0197.
9. de Oliveira JV. Semantic constraints for membership function optimization. *IEEE Transactions on Systems, Man, and Cybernetics, Part A* 1999; **29**(1):128–138.
10. Gómez Mármol F, Martínez Pérez G. Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. *Computer Standards & Interfaces* 2010; **32**(4):185–196.
11. Sun Y, Yang Y. Trust establishment in distributed networks: analysis and modeling. *Proceedings of the IEEE International Conference on Communications*, Glasgow, Scotland, 2007.
12. Josang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. *Decision Support Systems* 2007; **43**(2):618–644.
13. Momani M. Trust models in wireless sensor networks: a survey. In *Recent Trends in Network Security and Applications, Third International Conference, CNSA 2010, Communications in Computer and Information Science, vol. 89*, Natarajan M, Selma B, Nabendu C, Dhinaharan N (eds): Chennai, India, 2010; 37–46.
14. Lam SK, Riedl J. Shilling recommender systems for fun and profit. *WWW '04: Proceedings of the 13th International Conference on World Wide Web*, New York, NY, USA, 2004; 393–402.
15. Sun Y, Han Z, Liu K. Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine* Feb 2008; **46**(2):112–119.
16. Gómez Mármol F, Martínez Pérez G. Security threats scenarios in trust and reputation models for distributed systems. *Elsevier Computers & Security* 2009; **28**(7):545–556.
17. Kamvar S, Schlosser M, Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks. *Proceedings of the International World Wide Web Conference (WWW)*, Budapest, Hungary, 2003.
18. Xiong L, Liu L. PeerTrust: supporting reputation-based trust in peer-to-peer communities. *IEEE Transactions on Knowledge and Data Engineering* 2004; **16**(7):843–857.

DOI: 10.1002/cpe

19. Zhou R, Hwang K. PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing. *Transactions on Parallel and Distributed Systems* 2007; **18**(4):460–473.
20. Boukerche A, Xu L, El-Khatib K. Trust-based security for wireless ad hoc and sensor networks. *Computer Communications* 2007; **30**(11–12):2413–2427.
21. Dhurandher SK, Misra S, Obaidat MS, Gupta N. An ant colony optimization approach for reputation and quality-of-service-based security in wireless sensor networks. *Security and Communication Networks* 2009; **2**(2):215-224.
22. Kim TK, Seo HS. A trust model using fuzzy logic in wireless sensor network. *Proceedings of World Academy of Science, Engineering and Technology, vol. 32*, 2008; 69–72.
23. Zhang Z, Ho PH, Nat-Abdesselam F. RADAR: A reputation-driven anomaly detection system for wireless mesh networks. *Wireless Networks* 2010; **16**:2221–2236.
24. Omar M, Challal Y, Bouabdallah A. Reliable and fully distributed trust model for mobile ad hoc networks. *Computers and Security* 2009; **28**(3–4):199–214.
25. Buchegger S, Le Boudec JY. A robust reputation system for P2P and mobile ad-hoc networks. *Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems*, Cambridge MA, USA, 2004.
26. Almenárez F, Marín A, Campo C, García C. PTM: a pervasive trust management model for dynamic open environments. *Privacy and Trust, First Workshop on Pervasive Security and Trust*, Boston, USA, 2004.
27. Sabater J, Sierra C. REGRET : reputation in gregarious societies. In *Proceedings of the Fifth International Conference on Autonomous Agents*, Müller JP, Andre E, Sen S, Frasson C (eds). ACM Press: Montreal, Canada, 2001; 194–195.
28. Songsiri S. MTrust: a reputation-based trust model for a mobile agent system. In *Autonomic and Trusted Computing, no.4158 in LNCS Third International Conference, ATC 2006*. Springer: Wuhan, China, 2006; 374–385.
29. Breuer J, Held A, Leinmller T, Delgrossi L. Trust issues for vehicular ad hoc networks. *67th IEEE Vehicular Technology Conference (VTC2008-Spring)*, Singapore, 2008.
30. Raya M, Papadimitratos P, Gligor V, Hubaux JP. On data-centric trust establishment in ephemeral ad hoc networks. *Proceedings of IEEE INFOCOM*, Phoenix, AZ, USA, 2008.
31. Lo NW, Tsai HC. A reputation system for traffic safety event on vehicular ad hoc networks. *EURASIP Journal on Wireless Communications and Networking* 2009; **2009**:1–10.
32. Takabi H, Joshi JBD, Ahn GJ. Security and privacy challenges in cloud computing environments. *IEEE Security and Privacy* 2010; **8**:24–31. DOI: 10.1109/MSP.2010.186.
33. Wang S, Zhang L, Wang S, Qiu X. A cloud-based trust model for evaluating quality of Web services. *Journal of Computer Science and Technology* 2010; **25**(6):1130-1142. DOI: 10.1007/s11390-010-9394-1.
34. Hwang K, Kulkarni S, Hu Y. Cloud security with virtualized defense and reputation-based trust mangement. *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, Chengdu, China, 2009; 717–722, DOI: 10.1109/DASC.2009.149.
35. Gómez Mármol F, Girao J, Martínez Pérez G. TRIMS, a privacy-aware trust and reputation model for identity management systems. *Elsevier Computer Networks Journal* 2010; **54**(16):2899–2912. DOI: 10.1016/j.comnet.2010.07.020.
36. Mohan A, Blough DM. AttributeTrust - a framework for evaluating trust in aggregated attributes via a reputation system. In *Proceedings of the 2008 Sixth Annual Conference on Privacy, Security and Trust*, 2008; 201–212. DOI: 10.1109/PST.2008.28.
37. Windley PJ, Daley D, Cutler B, Tew K. Using reputation to augment explicit authorization. In *Proceedings of the 2007 ACM workshop on Digital identity management, DIM '07*, 2007; 72–81.
38. Conner W, Iyengar A, Mikalsen T, Rouvellou I, Nahrstedt K. A trust management framework for service-oriented environments. *Proceedings of the 18th International Conference on World Wide Web, WWW '09*, 2009; 891–900, DOI: 10.1145/1526709.1526829.
39. Malik Z, Bouguettaya A. RATEWeb: Reputation Assessment for Trust Establishment among Web services. *The VLDB Journal* 2009; **18**(4):885–911. DOI: 10.1007/s00778-009-0138-1.
40. Bianculli D, Jurca R, Binder W, Ghezzi C, Faltings B. Automated dynamic maintenance of composite services based on service reputation. *Proceedings of the 5th International Conference on Service-Oriented Computing, ICSOC '07*, 2007; 449–455. DOI: 10.1007/978-3-540-74974-5_42.
41. Sachin B, Parikshit M, Antonietta S, Neeli P, Ramjee P. Proposed security model and threat taxonomy for the Internet of Things (IoT). In *Recent Trends in Network Security and Applications, Third International Conference, CNSA 2010, Communications in Computer and Information Science vol. 89*, Natarajan M, Selma B, Nabendu C, Dhinaharan N (eds): Chennai, India, 2010; 420–429.
42. Wang W, Zeng G, Yuan L. Ant-based reputation evidence distribution in P2P networks. In *GCC, Fifth International Conference on Grid and Cooperative Computing*. IEEE Computer Society: Changsha, Hunan, China, 2006; 129–132.
43. Zhuo T, Zhengding L, Kai L. time-based dynamic trust model using ant colony algorithm. *Wuhan University Journal of Natural Sciences* 2006; **11**(6):1462–1466.
44. Dorigo M, Stützle T. *Ant Colony Optimization*. Bradford Book: Cambridge, MA, 2004.
45. Cordón O, Herrera F, Stützle T. A review on the ant colony optimization metaheuristic: basis, models and new trends. *Mathware and Soft Computing* 2002; **9**(2–3):141–175.
46. Gómez Mármol F, Martínez Pérez G. Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication Systems Journal* 2011; **46**(2):163–180.

DOI: 10.1002/cpe

47. Tajeddine A, Kayssi A, Chehab A, Artail H. PATROL-F- a comprehensive reputation-based trust model with fuzzy subsystems. In *Autonomic and Trusted Computing, no.4158 in LNCS Third International Conference, ATC 2006*. Springer: Wuhan, China, 2006; 205–217.
48. Carbó J, Molina JM, Dávila J. Trust management through fuzzy reputation. *International Journal of Cooperative Information Systems* Mar 2003; **12**:135–155.
49. Gómez Mármol F, Gómez Marín-Blázquez J, Martínez Pérez G. Linguistic fuzzy logic enhancement of a trust mechanism for distributed networks. *Proceedings of the Third IEEE International Symposium on Trust, Security and Privacy for Emerging Applications (TSP-10)*, Bradford, UK, 2010; 838–845. DOI: 10.1109/CIT.2010.158.
50. Marti S, Garcia-Molina H. Taxonomy of trust: categorizing P2P reputation systems. *Computer Networks* Mar 2006; **50**(4):472–484.
51. Pedrycz W, Gomide F. *An Introduction to Fuzzy Sets: Analysis and Design*. The MIT Press: Cambridge, Masssachusetts, USA, 1998.
52. Jang JSR, Sun CT, Mizutani E. *Neuro-Fuzzy and Soft Computing*. Prentice Hall: Upper Saddle River, New Jersey, USA, 1997.
53. Gómez Mármol F, Martínez Pérez G. TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. *Proceedings of the IEEE International Conference on Communications (IEEE ICC 2009), Communication and Information Systems Security Symposium*, Dresden, Germany, 2009. DOI: 10.1109/ICC.2009.5199545.

DOI: 10.1002/cpe