Improving the Robustness of Fuzzy Trust Management System for WSNs

Seifi Mohammad¹
Yazdandoost Samane²

Paper Reference Number:  
Name of the Presenter: Seifi Mohammad

Abstract
Trust management system has gained world-wide attention in recent years [1, 17], particularly Fuzzy Trust Management System [19, 20, 21], because of uncertainty and ambiguity of trust nature [25, 26, 27]. Weakness of signal in surrounding environment lead to fail in communication, especially in adverse weather conditions. As a consequence nodes cannot communicate with each other that cause decreeing in trust values. While nodes are unable to trust each other, there will be no more cooperation thus environmental conditions should be included in trust calculation. In previous paper [28], a new way to calculate trust was introduced. In this paper environmental conditions are considered as an important factor in trust calculation. Simulation and analyze demonstrates that model is self-configurable and adaptive with environment and trust values are more scalable and robust.

Key words: Trust, Fuzzy, Sensor Network, Environment

1. Introduction
WSNs have a wide range of application in different environment e.g. health, military, security etc. that in most of them monitoring is being done. As noted before, many researchers are currently engaged in calculating trust and building trust management system specifically fuzzy methods owing to simplicity in calculation and uncertainty nature of fuzzy.

In previous paper, two types of factors are defined for calculating trust such as Status and Behavior of nodes. Status means information about the node itself such as power, memory etc. and behavior means information about communication of node with other nodes such as dropped packet, forwarding packet etc.

Main problem of above method is ignoring the surrounding environment and its effect on node communication for instance signal strength, signal propagation and packet delivery rates. Conditions are different in diverse environments thus signal propagation affects from the type and specification of environments. Parameters like humidity, temperature etc. may effect the signal propagation.

¹ M.tech Computer Network & Information Security-School of IT – JNTU Hyderabad, India- seifi.mohammad@gmail.com
² Master of Artificial Intellingence, Islamic Azad University of Mashad, s_yazdandoost@yahoo.com
Sensor networks use wireless communication and this type of communication is susceptible to environmental factors. Since WSNs may be deployed in a wide range of environments, it’s necessary for Trust calculation to be adaptive in any conditions. These physical effects are difficult to predict and may lead to weakness in signal propagation due to atmospheric conditions such as humidity, temperature, pollution, etc.

As a result of signal weakness, node communications will fail, and behavior features such as drop packet ratio significantly will increase and as a consequence Trust value will decrease. In this situation, nodes can’t trust each other and establish communication. Therefore, environmental conditions should be included in calculation. To do this a variety of sensors may be attached to the sensor nodes to measure properties of the environment.

As it comes from above, in addition to status and behavior of node, environmental conditions should be included in calculation of trust value that is done in this paper.

Rest of this paper is organized as follow. In section 2 related works are presented, and in section 3, system model is discussed. Trust calculation is proposed in section 4. The analyses and simulation results are provided in section 5.

2. Related work

Trust has been recognized as a prerequisite for cooperation in a distributed wireless sensor network.

There are many different papers proposed for Trust Management system in WSNs. Although there are a few comprehensive work such as [1,7,9,10,11,12]. Other papers proposed a partial solution or didn’t get involved in details such as [13,14]. In addition, some work has studied the issues and challenges such as [15],[16] and [17].

Main idea of these papers is reputation-based that use probability approach based on previous behavior of the node. [12] has defined eight parameters to calculate the trust. These parameters are limited to a cryptographic operation and interactive behavior, and they use a weighting mechanism for combining these parameters. [10] introduced the concept of Group-based trust for the clustered WSN, similar to [7]. They use monitoring technique and statistical information as a node reputation. Generally, this paper has improved the previous mathematical solution by calculating both direct and Indirect Trust. [17] is the best survey about trust that covers all the aspect of trust. It has studied trust in two levels of abstraction: Individual-Level and System-Level.

In contrast to all above papers, some papers introduce the concept of Fuzzy logic for trust calculation, such as [18,19,20]. [21,22,23] use the Fuzzy logic to calculate the trust value in WSN. [18] introduce the fuzzy logic as a suitable instrument for calculating the trust value. [19,23] suggests a set of parameters to calculate trust and uses the fuzzy logic as a tool for calculating trust based on the parameters for ad-hoc networks. These parameters are condition, history behavior, and environment of the node.
[21] has used an ANP method to reflect the relationship between nodes, and combined it with fuzzy because of the nature of trust to invent a new approach as Fuzzy-ANP method.

3. System model

In this model, it is assummed that node is new, and supposed to join to the network after deploying and communicate with other nodes. Therefore, it has no information about other nodes. Consequently, it doesn’t know to which node it can trust. Thus it’s necessary to have a knowledge base (KB) to assess each node to consider a rational trust value to this node.

All nodes are assigned an ID, trust calculation is done for all of its neighbors. For more illustration imagine that node i wants to calculate the trust value of node j. Node j sends its information to node i, the same will be done for the other neighbors.

Information is classified to three groups: (i) information about the status of nodes as power, memory, etc. (ii) information about the behavior of node in cooperation with other nodes such as the dropped packets, forwarding packet, etc. (iii) information about environment such as humidity, temperature etc.

There is no way to consider some pre-determined parameter for calculating trust, because it’s based on type of application. Some important factors are number of neighbors, Traffic input and output, Drop packet, Packet forwarded, Data rate, Error rate, Power consumption, Reliability, Competence .etc.

Next point is that these parameters have different level of importance Thus different weight should be assigned to these types of parameters. Another reason for classifying factors is to reduce the computation, by reducing the size of input as a divide and conquer solution.

This model is a symmetric 3-inputs-single-output fuzzy structure, that lead to reduce calculation and computation overhead. Model shown in “Figure 1”.

![Figure 1: Fuzzy trust model](image)

Second layer is a fuzzy system called T-Box that calculates the trust value based on the provided information from layer one by the two variable s and b that are outputs of S-Box and B-Box, respectively. Inputs of the T-Box are crisp value and the output t can be crisp or fuzzy variable, depend on the application requirement. Both of them as a tf and tc, are calculated in this paper.
In first layer, inputs are classified to the situational, behavioral and Environmental condition. S, B and E are fuzzy systems, inputs to this function are the data, provided by the neighbors. Each of the boxes has different number of inputs and single output, both inputs and output are crisp. For instance, for S-Box has three inputs and one output. Assigning different weight is done with using weighted averaging function (WA).

4. Trust Calculation

Because of the uncertainty and ambiguity of the trust nature, Fuzzy logic can be a good way for trust evaluation [18, 24]. Besides its flexibility, it reduces the complexity of calculation, has a fast response in output and is easy to implement.

All the fuzzy systems have the same structure, and as it can be seen in the blow figure, each fuzzy system consists of five components, such as Fuzzifier, Defuzzifier, Rule Base, Data Base and Inference Unit “Figure 2”.

Fuzzy system can take either fuzzy or crisp input, but here inputs are crisp, like the available energy percentage, thus a fuzzifier is required to convert it to a Linguistic variable such as low, medium or high. Defuzzifier is to extract the crisp value that best represent a fuzzy set. Centroid of area is the most widely adopted strategy defuzzification method. Other components are: A rule base contains a selection of fuzzy rules; A database which defines the membership functions used in the fuzzy rules; and An Inference engine, which performs the inference procedure upon the rules and given fact to derive a reasonable output or conclusion. In this section, the proposed fuzzy system will discuss in each layer.

Defining rules also depend on the scenario and application. The rule base is like the following:

If (Par3 is Low) and (Par2 is Medium) and (Par3 is High) then (Status is Good)

\[
trapezoid(x; a, b, c, d) = \begin{cases} 
  n & x \leq a, \\
  \frac{x-a}{b-a} & a \leq x \leq b, \\
  1 & b \leq x \leq c, \\
  \frac{d-x}{d-c} & c \leq x \leq d, \\
  0 & d \leq x.
\end{cases}
\]

\[
z_{\text{coA}} = \frac{\int_{x}^{c} \mu_{A}(z) \, dz}{\int_{x}^{d} \mu_{A}(z) \, dz}
\]
First Level
In first level, there are two types of input such as Status information and Behavior information. Inputs are weighted based on their importance.

For simulation, three parameters are considered as inputs for each box, which are listed as below: security level, remained power and Number of neighbors that are known as status information; drop percentage, routing table maintenance and Average latency as Behavior information; humidity and temperature are used for Environment information.

Input data are crisp, so Trapezoied function is selected as a fuzzification function. Three Membership function as Low, Medium and High is considered, and centroid of area has been used as a method for defuzzification.

Second level
In this level, trust value for each node will be calculated. It has 3 inputs such as status and behavior and environment. Gaussian function has been used as a fuzzification function. Five membership functions are assigned such as Very Low, Low, Medium, High and Very High and centroid of area has been used as a method for defuzzification.

5. Simulation
Simulation is done with MATLAB, a random network with 50 nodes is considered, and Dijkstra algorithm is selected as a rerouting algorithm.

One node is selected randomly to send a packet to the cluster-head. To do this, a routing through most trusted route will be done based on the trust value. Later the trust value will be updated, based on the result of this transaction. Fuzzy systems is shown in “Figure 5”, and shows how with using fuzzy approach results are became smooth.

Due to environment problem, rate of unsuccessful transactions may increased thus average trust value will be decreased and as a consequent nodes don’t trust to each other and cooperation goes down. Table 1 and Figure 4 are showing trust in different environment,
that is based on the percentage of unsuccessful transaction such as 0%, 10%, 20% till 100%. \( P^* \) is Percentage of unsuccessful transaction and \( N^* \) is Number of nodes.

<table>
<thead>
<tr>
<th>( P^* )</th>
<th>0</th>
<th>10</th>
<th>20</th>
<th>30</th>
<th>40</th>
<th>50</th>
<th>60</th>
<th>70</th>
<th>80</th>
<th>90</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>98</td>
<td>88</td>
<td>78</td>
<td>68</td>
<td>58</td>
<td>48</td>
<td>38</td>
<td>28</td>
<td>18</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>99</td>
<td>89</td>
<td>79</td>
<td>69</td>
<td>59</td>
<td>49</td>
<td>39</td>
<td>29</td>
<td>19</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>200</td>
<td>100</td>
<td>90</td>
<td>80</td>
<td>70</td>
<td>60</td>
<td>50</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>300</td>
<td>100</td>
<td>90</td>
<td>80</td>
<td>70</td>
<td>60</td>
<td>50</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>400</td>
<td>100</td>
<td>90</td>
<td>80</td>
<td>70</td>
<td>60</td>
<td>50</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>500</td>
<td>100</td>
<td>90</td>
<td>80</td>
<td>70</td>
<td>60</td>
<td>50</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>600</td>
<td>100</td>
<td>90</td>
<td>80</td>
<td>70</td>
<td>60</td>
<td>50</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>700</td>
<td>100</td>
<td>90</td>
<td>80</td>
<td>70</td>
<td>60</td>
<td>50</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>800</td>
<td>100</td>
<td>90</td>
<td>80</td>
<td>70</td>
<td>60</td>
<td>50</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>900</td>
<td>100</td>
<td>90</td>
<td>80</td>
<td>70</td>
<td>60</td>
<td>50</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>1000</td>
<td>100</td>
<td>90</td>
<td>80</td>
<td>70</td>
<td>60</td>
<td>50</td>
<td>40</td>
<td>30</td>
<td>20</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1: Trust values in diverse environment

Figure 4: Trust values in diverse environment

However, in this paper with considering the environment condition, in spite of bad environment, there will be a suitable trust value, which can keep cooperation on. This is shown in figure 5 and 6.
5. Conclusions
In this paper with considering environment conditions, in spite of bad environment, results are stable and smooth, therefore cooperation among nodes still keep up.

References


