Linguistic Fuzzy Trust Model over Oscillating Wireless Sensor Networks

Firas Ali Al-Juboori
Ph. D.
College of Engineering - University of Baghdad
Email: firasaljuboori@yahoo.com

Sura Fawzi Ismail
M.Sc. Student
College of Engineering - University of Baghdad
Email: surafawzi7789@yahoo.com

ABSTRACT

Simulation of the Linguistic Fuzzy Trust Model (LFTM) over oscillating Wireless Sensor Networks (WSNs) where the goodness of the servers belonging to them could change along the time is presented in this paper, and the comparison between the outcomes achieved with LFTM model over oscillating WSNs with the outcomes obtained by applying the model over static WSNs where the servers maintaining always the same goodness, in terms of the selection percentage of trustworthy servers (the accuracy of the model) and the average path length are also presented here. Also in this paper the comparison between the LFTM and the Bio-inspired Trust and Reputation Model for Wireless Sensor Networks (BTRM-WSN) in terms of the accuracy and the average path length suggested by each model is presented. Both models give quite good and accurate outcomes over oscillating WSNs. Also it must be mentioned that the evaluation environment used here is Trust and Reputation Model Simulator for WSN.

Key words: oscillating WSN, linguistic fuzzy trust model, bio-inspired trust and reputation model for wireless sensor networks, trustworthy servers, and malicious servers.

اختبار نموذج ضبابي الثقة على شبكات الاستشعار الاسلكية المتأرجحة

فراس علي الجبوري
مدرس
كلية الهندسة - جامعة بغداد

سرى فوزي اسماعيل
طالبة ماجستير
كلية الهندسة - جامعة بغداد

الخلاصة

هذا البحث يتناول برنامج محاكاة بالحاسبة لنموذج ضبابي الثقة على شبكة استشعار لاسلكية متأرجحة حيث كفاءة الخوادم التابعة لها متغيرة مع الزمن وايضا هذا البحث يتناول المقارنة بين النتائج المكتسبة من تطبيق النموذج على شبكة استشعار لاسليكة متأرجحة مع النتائج التي حصل عليها من التطبيق على شبكة استشعار لاسلكية ثابتة حيث كفاءة الخوادم ثابتة والمقارنة هنا من ناحية دقة النموذج ومتوسط طول المسار .هذا البحث يتناول أيضا المقارنة بين النتائج من تطبيق النموذج ضبابي الثقة مع نموذج ذو استيحاء حيوي لقياس الثقة من حيث دقة وطول الطريق وكلا النموذجين يعطي نتائج جيدة جدا ودقيقة على شبكات الاستشعار اللاسلكية المتأرجحة.

1. INTRODUCTION

Wireless sensor networks or sensor networks are composed of a large number of sensor nodes deployed densely in a closed proximity to collect data to a specific function. Sensors have limited memory, computational capability, and limited transmission capacity. The sensors primarily preprogrammed to collect the data and forward to the base station through defined communication path. If the information is sensitive, the nodes and communication path must be trustworthy. The sensor network possesses the self-organizing capability if the positions of nodes are not predetermined. Irrespective of the topology, each node must trust the successive node in the path. If any node in the path is suspicious, the decision node must calculate the alternative path.

This paper take the scheme that assumes some nodes of the network request some services (and act, therefore, as clients) and some others provide those services (thus acting as servers or services providers). Here suppose that every sensor is only able to communicate with its direct neighbors (that is, it cannot establish a direct communication with a node more than one hop ahead. They are, however, susceptible to a large number of security threats, **Mármol**, and **Pérez**, **2009a**, some of which might be effectively mitigated with an accurate trust and reputation management, **Marsh**, **1994**, **Marti**, and **Garcia-Molina**, **2006**. Many researches about trust and reputation management models have been recently proposed as an innovative solution for guaranteeing a minimum level of security between two entities belonging to a distributed system that want to have a transaction or interaction. Thus, many models have been designed and developed in this direction.

Many methods, technologies and mechanisms like fuzzy logic, **Tajeddine**, **et al.**, **2006**, bayesian networks, **Wang**, **et al.**, **2006**, or even bio-inspired algorithms, **Mármol**, and **Pérez**, **2011**, have been proposed in order to manage and model trust and reputation in systems such as P2P networks, **Almen´arez**, **et al.**, **2004**, ad-hoc ones, **Moloney**, and **Weber**, **2005**, wireless sensor networks, **Boukerche**, **et al.**, **2007**, or even multi-agent systems, **Sabater**, and **Sierra**, **2001**.

The simulation of the trust model, Linguistic Fuzzy Trust Model (LFTM) over oscillating Wireless Sensor Networks is presented here. This model enhances the interpretability of previous model, BTRM-WSN (Bio-inspired Trust and Reputation Model for Wireless Sensor Networks), **Mármol**, and **Pérez**, **2011**, and makes it closer to the final user with relatively improvement in the accuracy of it. BTRM-WSN is a model based on a bio-inspired algorithm called ant colony system (ACS), **Dorigo**, and **Gambardella**, **1997**, where ants build paths fulfilling certain conditions in a graph. These ants leave some pheromone traces that help next ants to find and follow those routes.

The simulation of the BTRM-WSN model over oscillating WSNs is presented in paper, **Mármol**, and **Pérez**, **2011**, while in this paper the simulation of the LFTM model over oscillating WSNs is presented, and the comparison between the simulations of the two models over oscillating Wireless Sensor Networks is also presented here. Here the simulation is focused in two targets. First, interesting in finding out how many times a model is able to select the right benevolent server to interact with. In other words, the selection percentage of trustworthy servers is calculated; Second, in calculating the average path length suggested by a model. The rest of this paper is organized as follows: An overview of the Linguistic Fuzzy Trust model is presented in section 2. In section 3 simulation results of experiments and comparison between simulation of the BTRM-WSN and LFTM models over oscillating Wireless Sensor Networks are discussed. In section 4 conclusions is described.

2. LINGUISTIC FUZZY TRUST MODEL

This model is an enhancement for the pervious trust and reputation model, BTRM-WSN model, **Mármol**, and **Pérez**, **2011**, which uses linguistic fuzzy sets and fuzzy logic for the enhancement. On one hand, it will be enjoyed the representation power of linguistically labeled fuzzy sets, as is the case, for instance, of 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.

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 **Fig. 1**.

Fuzzy rules can be expressed in several forms. 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. 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:(**If *quality* is Good AND *price* is Low THEN *satisfaction* is Very High)**

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. 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, defuzzified back into a numerical value. Details of how fuzzification, fuzzy inference, aggregation, and defuzzification work can be found in, **Pedrycz**, and **Gomide**, **1998**, **Jang**, **et al.**, **1997**. The defuzzification method chosen to be used in this paper is Center of Gravity.

The flow of the Linguistic Fuzzy Trust Model is depicted in **Fig. 2**, emphasizing those steps where it actually applied linguistic fuzzy sets and fuzzy logic. Such steps are:

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 weights for the services attributes.
5) The client satisfaction is assessed by means of the services comparison performed in previous step, and the client conformity.
6) Finally, the punishment level is determined by the client satisfaction with the received service, together with his/her goodness.
More detailed about the use of linguistic fuzzy sets in the Linguistic Fuzzy Trust Model is described in, **Mármol**, **et al.**, **2011**.

3. EXPERIMENTS AND RESULTS

The tested scenario consisted of Wireless Sensor Networks where the goodness of the servers belonging to them could change along the time. How a sensor decides to be benevolent or malicious at each time is out of scope of this paper.
The following proposal takes in this paper: after every 20 transactions are carried out (i.e., after every client has had 20 transactions) all the benevolent servers composing the Wireless Sensor Network become malicious. **Fig. 3** shows this proposal.
In **Fig. 3** when the peer behavior is 1, the server is benevolent server but when the peer behavior is 0, then the server is malicious server. In order to preserve the same percentage of malicious servers, the number of previous benevolent servers, say *nb*, is kept. Then *nb* random servers are selected (note that all of them will be malicious) and their goodnesses are swapped so they become benevolent and the percentage of malicious servers remains equal to the stage previous the oscillation. With an oscillation scheme like this a benevolent server could maintain its positive goodness since it could be randomly selected to become benevolent when it indeed previously was benevolent.
The evaluation environment used is Trust and Reputation Model Simulator for WSN, **Mármol**, and **Pérez**, **2009b**, which is a generic framework serving as an assistant tool to easily implement trust and reputation mechanisms in distributed environments and to compare between them.
Here the experiments focused on two main targets. First, interesting in finding out how many times the model is able to select the right benevolent server to interact with. In other words, the selection percentage of trustworthy servers or the accuracy of the model is calculated. In order to consider a trust and reputation model as acceptable (with a minimum quality level), it is assumed that the model is not useful at all if the selection percentage of the trustworthy servers is less than 50%, since a smaller percentage would result in a model with certain security deficiencies. Secondly, it is aimed to find the closest benevolent servers to the client requesting the service. On the one hand it is more secure and robust if the lesser number of intermediaries present in a transaction. On the other hand, due to the specific restrictions related to Wireless Sensor Networks, the resources consumption saving is a critical issue. Therefore, a shorter path leading to the final trustworthy server implies less involved sensors and, consequently, less global utilization of resources such as energy or bandwidth.
The experiments that carried out here had the following structure. The model is launched 100 times (i.e. each client applied for a service 100 times) over 100 WSNs randomly generated, each one composed of 100 sensors. On each network, the percentage of sensors acting as clients was always a 15%, 5% acts as relay servers (those that not providing the service requested by the clients) and the 80% left were, therefore, sensors acting as trustworthy or malicious servers. With tried the model over 100 random WSNs having a 10% (over the 80% left) of malicious servers.

100 with 20%, other 100 with 30%, and so on until a 90% of malicious servers (the worst simulated situation). But even more, those experiments are repeated over WSNs composed of 200, 300, 400 and 500 sensors. This parameters and others used to perform the experiments are listed in **Table 1**.

3.1 Experiments and Results of Linguistic Fuzzy Trust Model over Oscillating Wireless Sensor Networks

3.1.1 Selection percentage of trustworthy servers

Fig. 4 shows the results achieved with LFTM model over static and oscillating WSNs. It is observed from **Fig. 4(a)** which is outcomes achieved with LFTM model over static networks that the selection percentage of trustworthy servers is quite high (above the 90%) when the percentage of malicious servers is greater than or equal to 60% regardless the size of the networks. And the maximum accuracy reached when the percentage of malicious servers is 90% and the size of the network is 300 nodes which it is (99.62%), and even in the worst case when the percentage of malicious servers is 90% and the size of the networks is 500 nodes, the accuracy is (97.96%) which it is still a high value. In general the selection percentage of trustworthy servers increases as the percentage of malicious servers increases regardless the size of the networks; the reason for the increase in the accuracy of the model as the number of malicious servers increases 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.

While it is observed from **Fig. 4(b)** which is the corresponding result for LFTM over oscillating WSNs that the selection percentage of trustworthy servers is (less than 50) when the percentage of malicious servers is 10% regardless the size of the network, which makes the model not useful at all, because here assume that if the selection percentage of trustworthy servers is under the 50%, then the model is completely useless, and the accuracy began to increase by increasing the percentage of the malicious servers. The selection percentage of trustworthy servers is quite high (above the 90%) when the percentage of malicious servers is greater than or equals to 70% regardless the size of the networks. The maximum accuracy reached here, when the percentage of malicious servers is 90% and the size of the network is 300 nodes which it is (99.13%), and even in the worst case when the percentage of malicious servers is 90% and the size of the networks is 500 nodes, the accuracy is (97.03%) which it is still high value. The selection percentage of trustworthy servers increases as the percentage of malicious servers increases regardless the size of the network, the reason again for the increase in the accuracy by increasing the number of malicious servers 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. And in general the accuracy of the model over oscillating WSNs are slightly less than the accuracy of the model over static WSNs and this differences in the accuracy achieved with the model over static WSNs and over oscillating WSNs decreases as the percentage of malicious servers increases.

It is observed from the two figures **Fig. 4(a)** and **Fig. 4(b)** that for a certain percentage of malicious servers the results about the selection percentage of trustworthy servers is close to each other when the size of the network is less than or equal to 400 nodes while when the size of

the network is 500 nodes the outcomes about the selection percentage of trustworthy servers is different from each other.

3.1.2 Average path length leading to trustworthy servers

The results achieved with LFTM model over static and oscillating Wireless Sensor Networks are shown in **Fig. 5**. It is observed from **Fig. 5(a)** which is the results achieved with LFTM model over static WSNs that the average path length decreases as the percentage of fraudulent servers increases regardless the size of the network, and it is also observed that when the percentage of malicious servers is greater than or equal to 80% the average path length is approximately equal to (2.2) which it is small value.

While it is observed from the simulation of the model over oscillating WSNs, **Fig. 5(b)** that the average path length decreases as the percentage of malicious servers increases regardless the size of the network, it is also observed that when the percentage of malicious servers is greater than or equal to 80% the average path length is never exceed (2.5) which it is still small value. But for a certain percentage of malicious servers and a certain size of network the average path length suggested by LFTM model over oscillating WSNs is longer than the average path length suggested by the model over static WSNs, such as for example when the percentage of malicious servers is 10% and the size of network is 300 nodes then the average path length suggested by the model over static WSNs is (5.01) while the average path length suggested by the model over dynamic WSNs is (10.68) and this differences between the average path length suggested by the model over static WSNs and the average path length suggested by the model over oscillating WSNs decreases as the percentage of malicious servers increases.

Finally, the appreciation that can be given from the results of the average path length together with the selection percentage of trustworthy servers constitute the proof that LFTM obtains quite good, accurate outcomes with slight differences in outcomes over oscillating Wireless Sensor Networks as compared with static scenario, since with an oscillation scheme the same percentage of malicious servers remains equal to the stage previous the oscillation. And also the outcomes in general slightly differ from one set of random WSNs to another when the percentage of malicious servers fixed and vary the size of the Wireless Sensor Networks, which constitutes a demonstration of the scalability of the model.

3.2 Comparison between Simulation of Bio-inspired Trust and Reputation Model and Linguistic Fuzzy Trust Model over Oscillating WSNs

In this section, the comparison between the two models, BTRM-WSN and LFTM according to the selection percentage of trustworthy servers and the average path length suggested by each model is described.

3.2.1 Selection percentage of trustworthy servers

Fig. 6 shows the selection percentage of trustworthy servers achieved with BTRM-WSN over oscillating WSNs composed of 100 to 500 sensors with a percentage of malicious servers from 10% to 90%.

It can be checked that the selection percentage of trustworthy servers is greater than 90% if the percentage of malicious servers is approximately less than or equal to 40%, regardless the size of the Wireless Sensor Network. Moreover, reasonably good outcomes (those with a selection percentage above the 60%) are obtained when the proportion of fraudulent servers is less than or

equal to 80%. But the selection percentage of trustworthy servers decreases as the percentage of malicious servers increases, so when the percentage of malicious servers is equal to 90% the outcomes began to be (less than 50%) which makes the system not useful at all because here it is assumed that if the selection percentage of trustworthy servers is under the 50%, then the model is completely useless.

While the corresponding results obtains for the LFTM model over oscillating WSNs are shown in **Fig. 4(b)**, here the selection percentage of trustworthy servers is (less than 50) when the percentage of malicious servers is 10% which makes the model not useful at all. The accuracy began to increase by increasing the percentage of the malicious servers. The selection percentage of trustworthy servers is quite high (above the 90%) when the percentage of malicious servers is greater than or equals to 70% regardless the size of the networks.

The comparison between the two figures **Fig. 6** and **Fig. 4(b)** gives the conclusion that in the case of the BTRM-WSN model, the selection percentage of trustworthy servers decreases as the percentage of malicious servers increases while in the case of LFTM model, the selection percentage of trustworthy servers increases as the percentage of untrustworthy servers increases. This means that BTRM-WSN model gives higher accuracy in Wireless Sensor Networks with small number of malicious servers while LFTM model gives higher accuracy in Wireless Sensor Networks with large number of malicious servers.

Also it can be observes from the comparison, that the selection percentage of the trustworthy servers of the two models is slightly different from one set of random WSNs to another when the percentage of malicious servers fixed and vary the size of the Wireless Sensor Network, which constitutes a demonstration of the scalability of the two models.

3.2.2 Average path length leading to trustworthy servers

In this work, the measuring of the length (number of hops) of those paths found by BTRM-WSN and LFTM models leading to trustworthy servers is presented.

Fig. 7 shows the outcomes achieved with BTRM-WSN model over oscillating WSNs, here when the percentage of malicious servers is less than or equal to 40%, the results about the average path length is small and the differences between results when varying the size of tested networks are also small but when the percentage of untrustworthy servers is greater than 40% then the results about the average path length began to increase and the differences between results when varying the size of the networks also began to increase. It is also observes that whatever the size of the network and the number of malicious servers can reach high values the average path length never exceeds (8.5) hops in any case, which is still a good outcome for Wireless Sensor Networks, and in general when the percentage of malicious servers composing the network is greater, then the average path length also increases regardless the size of the networks.

The outcomes in **Fig. 5(b)** shows the results that achieved with LFTM model over oscillating WSNs, here the differences in the average path length suggested by the model when varying the size of the tested networks decreases as the percentage of malicious servers increases, so when the percentage of malicious servers is 10% the differences is very high but when the percentage is 90% the differences is very small and it is approximately equal. And also here in general, the average path length decreases as the percentage of malicious servers increases regardless the size of the network.

In the comparison between the two figures **Fig. 7** and **Fig. 5(b)**, it can be observed that in the case of the BTRM-WSN model, the average path length leading to trustworthy servers increases

as the percentage of malicious servers increases while in the case of LFTM model, the average path length leading to trustworthy servers decreases as the percentage of untrustworthy servers increases. This means that BTRM-WSN model gives shorter path length in Wireless Sensor Networks with small number of malicious servers while LFTM model gives shorter path length in Wireless Sensor Networks with large number of malicious servers.

Also it can be observed from the comparison, that the average path length leading to trustworthy servers suggested by the two models is slightly different from one set of random WSNs to another with varying in the size of the Wireless Sensor Networks when the percentage of malicious servers is less than 50% in the case of BTRM-WSN model and when the percentage of malicious servers is greater than or equal to 50% in the case of LFTM model, which gives an evidence about the scalability of the two models.

4. CONCLUSION

Trust and reputation management over distributed systems has been proposed in the last few years as a novel and accurate way of dealing with some security deficiencies which are inherent to those environments. Tackling those risks not fully covered by traditional network security scheme.

In this paper the effect of one of these risks was shown, this risk is the oscillating behavior of the server nodes where the goodness of the servers could change along the time. The results is about the selection percentage of trustworthy servers and the average path length achieved with Linguistic Fuzzy Trust Model over oscillating WSNs. The experiment of the LFTM model over oscillating WSNs gives the proof that LFTM obtains quite good and accurate outcomes over oscillating Wireless Sensor Networks, with a low influence from the size of the networks and the percentage of malicious servers, which makes LFTM therefore presents a technique to identify trustworthy servers that is suitable for oscillating Wireless Sensor Networks.

Also, a comparison between BTRM-WSN and LFTM models over oscillating WSNs is presented. The results achieved by both models are slightly differ from one set of random WSNs to another when the percentage of malicious servers fixed and vary the size of the Wireless Sensor Network, which gives a confirmation about the scalability of the two models.

REFERENCES

- Almen´arez, F., Marı´n, A., Campo, C., and Garcı´a, C., 2004, *PTM: A Pervasive Trust Management Model for Dynamic Open Environments*, First Workshop on Pervasive Security and Trust, Boston, USA.

- Boukerche, A., Xu, L., and El-Khatib, K., 2007, *Trust-Based Security for Wireless Ad Hoc and Sensor Networks*, Computer Communications, Vol. 30, PP. 2413-2427.

- Dorigo, M., and Gambardella, L. M, 1997, *Ant Colony System: A Cooperative Learning Approach in the Traveling Salesman Problem*, IEEE Transaction on Evolutionary Computing, Vol. 1, Issue 1, PP. 53-66.

- Jang, J. S. R., Sun, C. T., and Mizutani, E., 1997, *Neuro-Fuzzy and Soft Computing*, Prentice Hall: Upper Saddle River, New Jersey, USA.

- Mármol, F. G, and Pérez, G. M, 2009a, *Security Threats Scenarios in Trust and Reputation Models for Distributed Systems*, Elsevier Computers & Security, Vol. 28, Issue 7, PP. 545-556.

- Mármol, F. G, and Pérez, G. M, 2009b, *TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks*, Proceedings of the IEEE International Conference on Communications, Communication and Information Systems Security Symposium, PP. 1-5, Dresden, Germany.

- Mármol, F. G, and Pérez, G. M., 2011, *Providing Trust in Wireless Sensor Networks Using A Bio Inspired Technique*, Telecommunication Systems Journal, Vol. 46, Issue 2, PP. 163-180.

- Mármol, F. G, Marín-Blázquez, J. G, and Pérez, G. M, 2011, *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, PP. 838-845, Bradford, UK.

- Marsh, S. P., 1994, *Formalising Trust As A Computational Concept*, Ph.D. Dissertation, Department of Computing Science and Mathematics, University of Stirling.

- Marti, S., and Garcia-Molina, H., 2006, *Taxonomy of Trust: Categorizing P2P Reputation Systems*, Computer Networks, Vol. 50, Issue 4, PP. 472-484.

- Moloney, M., and Weber, S., 2005, *A Context-Aware Trust-Based Security System for Ad Hoc Networks*, In Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, PP. 153-160, Athens, Greece.

- Pedrycz, W., and Gomide, F., 1998, *An Introduction to Fuzzy Sets: Analysis and Design*, The MIT Press: Cambridge, Masssachusetts, USA.

- Sabater, J., and Sierra, C., 2001, *REGRET: Reputation in Gregarious Societies*, Proceedings of the Fifth International Conference on Autonomous Agents, ACM Press, PP. 194-195, Montreal, Canada.

- Tajeddine, A., Kayssi, A., Chehab, A., and Artail, H., 2006, *PATROL-F- A Comprehensive Reputation-Based Trust Model with Fuzzy Subsystems*, Third International Conference, ATC, LNCS, Wuhan, China: Springer, Vol. 4158, PP. 205-216.

- Wang, Y., Cahill, V., Gray, E., Harris, C., and Liao, L., 2006, *Bayesian Network Based Trust Management*, Third International Conference, ATC, LNCS, Wuhan, China: Springer, Vol. 4158, PP. 246-257.

Table 1. Experiment parameters.

Network	NumExecutions NumNetworks MinNumSensors MaxNumSensors	100 100 {100,200,300, 400,500} {100,200,300, 400,500}	%Clients %Relay %Malicious Radio range	15% 5% {10%,20%,30%,40%, 50%,60%,70%,80%, 90%} {8,6,5,4,3}
BTRM	phi rho Transition threshold alpha beta Punishment threshold	0.01 0.87 0.66 1.0 1.0 0.48	Num ants Num iteration Path length factor q0 Initial pheromone	0.35 0.59 0.71 0.45 0.85
LFTM	Server goodness	‘High’ or ‘ very high’	Client	Random
	Benevolent		Conformity	
	Malicious	‘Low’ or ‘very low’	Goodness	Random
	Cost weight	0.25	Price weight	0.25
	Deliver weight	0.25	Quality weight	0.25

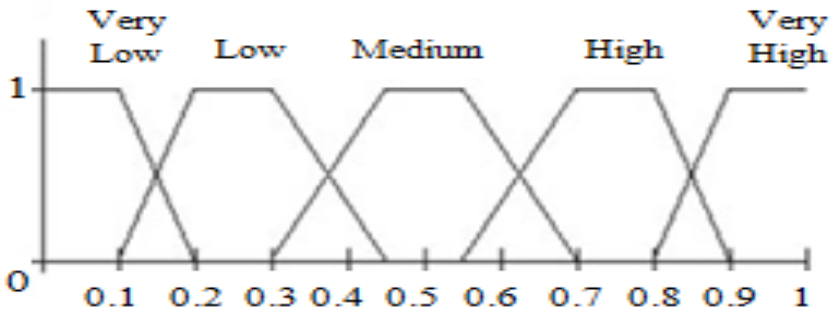

Figure 1. Linguistic labels and its defining fuzzy sets.

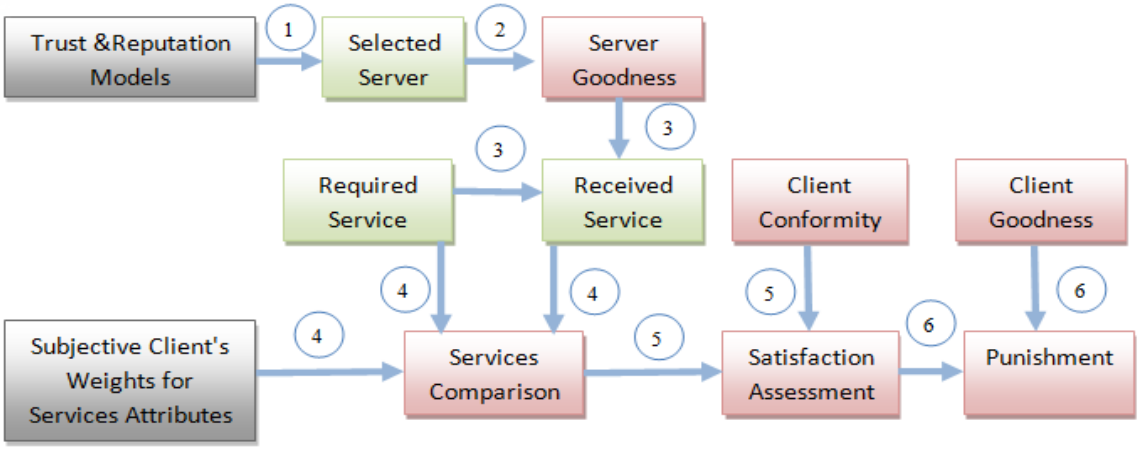

Figure 2. Linguistic fuzzy trust model steps.

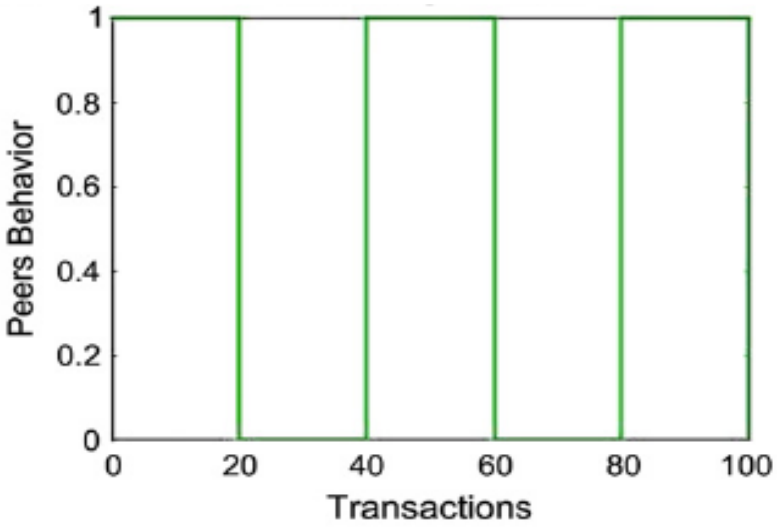

Figure 3. Oscillating behavior.

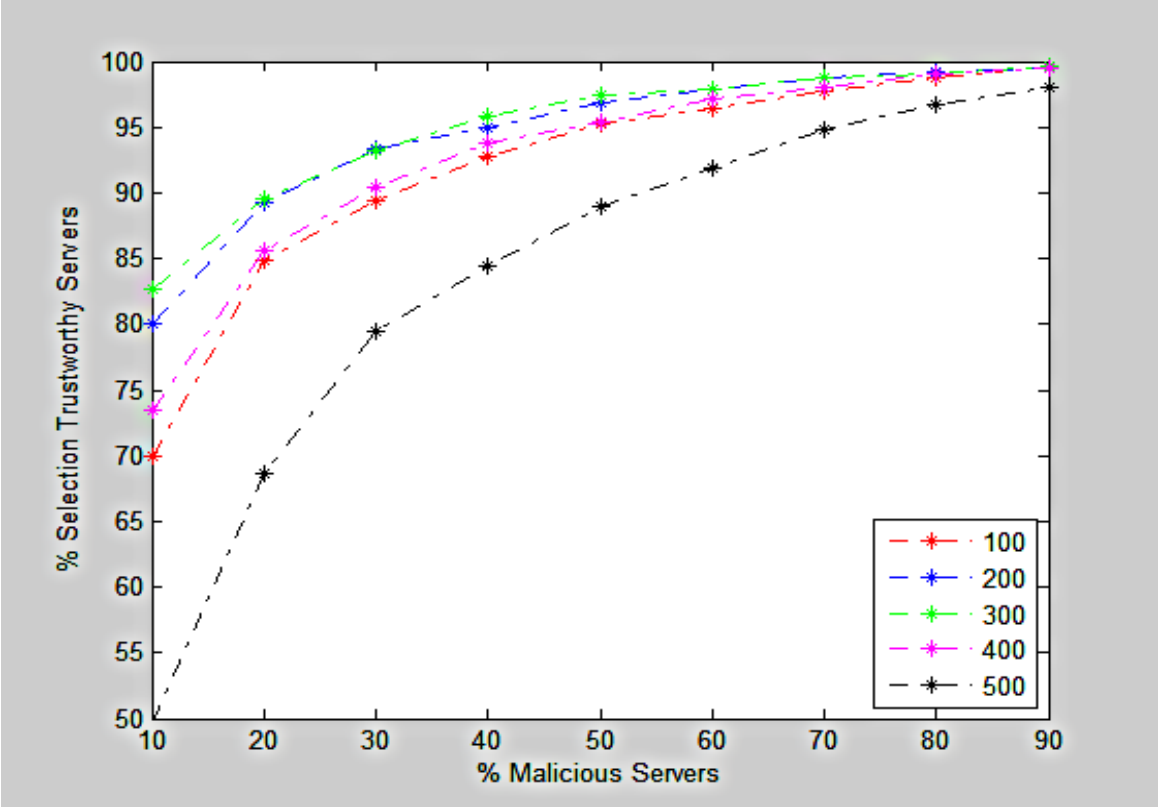

Figure 4(a). Selection percentage of trustworthy servers from linguistic fuzzy trust model over static WSNs.

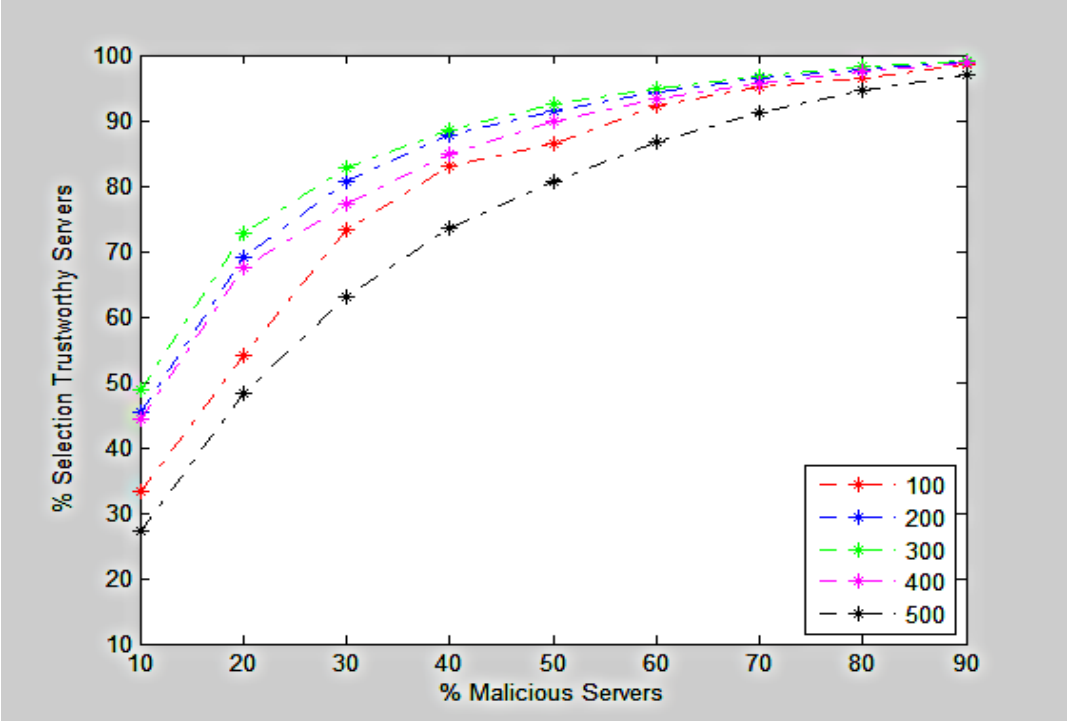

Figure 4(b). Selection percentage of trustworthy servers from linguistic fuzzy trust model over oscillating WSNs.

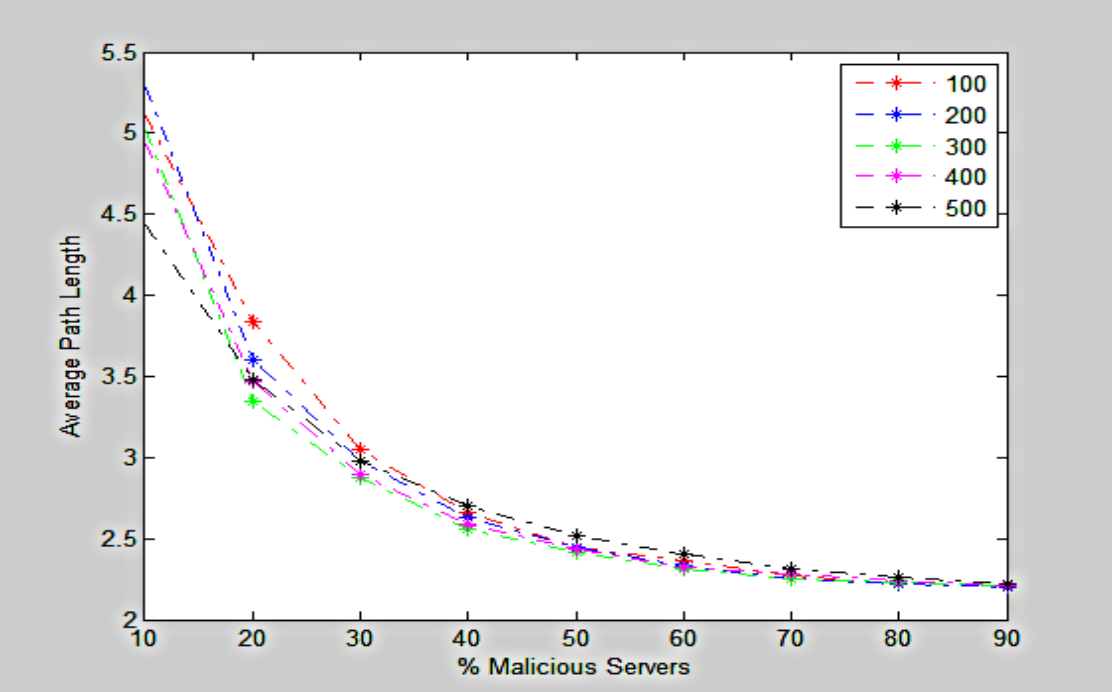

Figure 5(a). Average path length leading to trustworthy servers from linguistic fuzzy trust model over static WSNs.

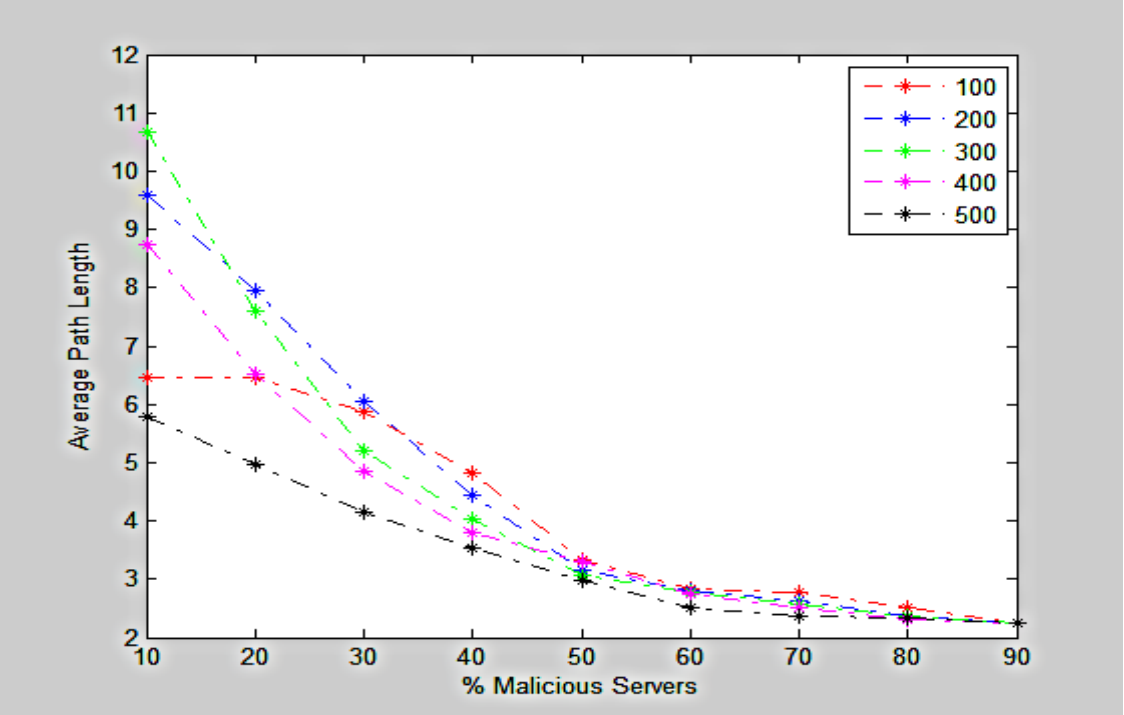

Figure 5(b). Average path length leading to trustworthy servers from linguistic fuzzy trust model over oscillating WSNs.

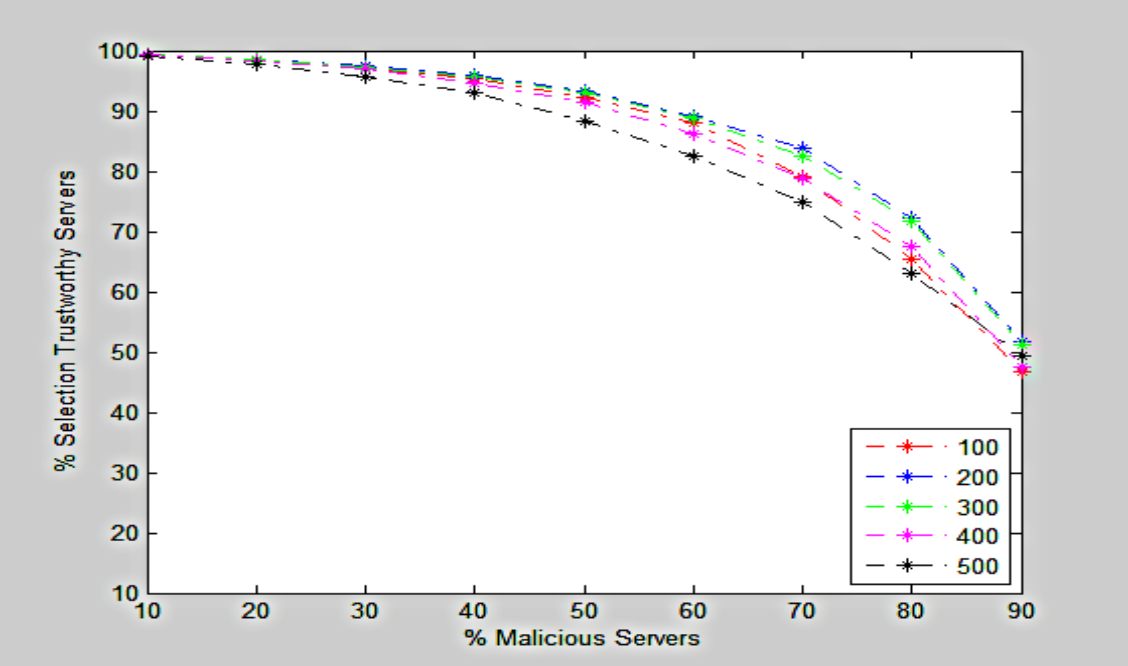

Figure 6. Selection percentage of trustworthy servers form bio-inspired trust and reputation model over oscillating WSNs.

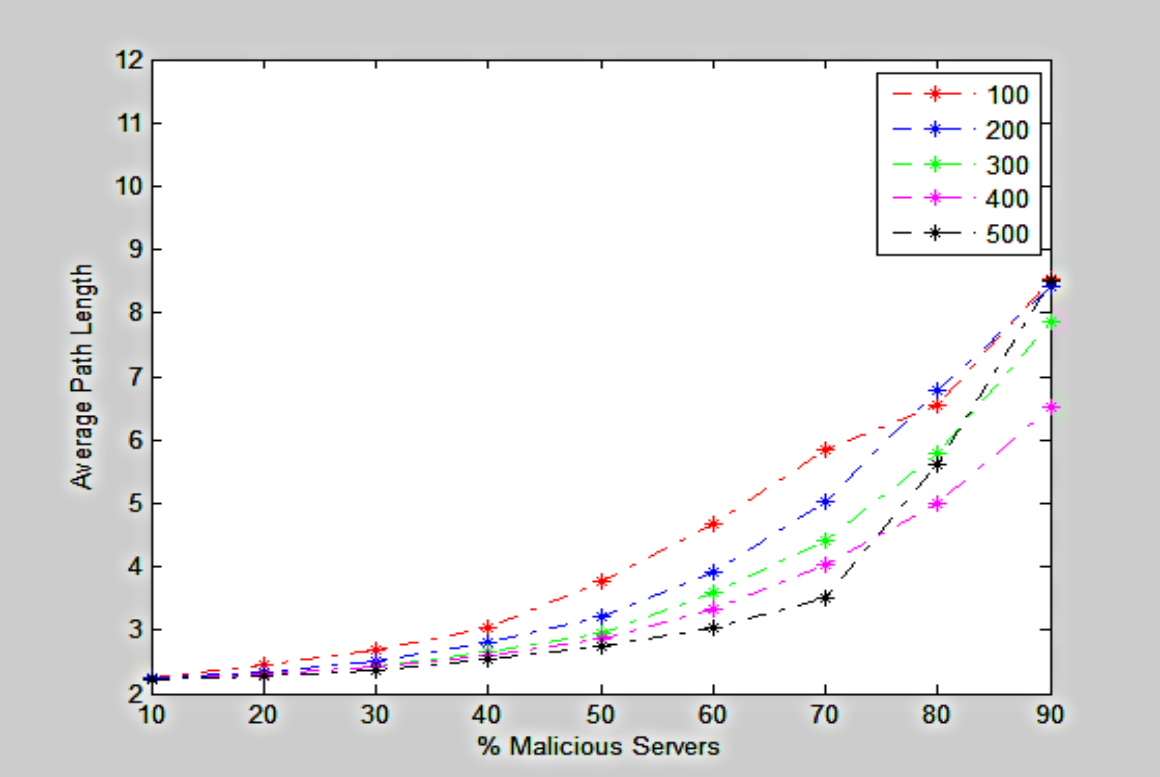

Figure 7. Average path length leading to trustworthy servers form bio-inspired trust and reputation model over oscillating WSNs.