Performance Analysis of Dynamic Wireless Sensor Networks using Linguistic Fuzzy

Zainab Hassan Fakhri
University of Baghdad/ College of Engineering

ABSTRACT
Wireless sensor networks (WSNs) are becoming very popular due to their large use in many of applications such as monitoring and collecting data from undisturbed dangerous environments. But the nodes in a sensor network are severely affected by energy. Reducing energy consumption of nodes to increase the network lifetime is considered as a most important challenge, so this paper will simulate the Linguistic Fuzzy Trust Model (LFTM) over dynamic Wireless Sensor Networks to save energy and shows the effect of dynamics in the performance of the model. A comparison in terms of the selection percentage of trustworthy servers (the accuracy of the model) and the average path length is also presented between LFTM model over dynamic WSNs and LFTM model over static WSNs. Also in this paper, a comparison between the Linguistic Fuzzy Trust Model (LFTM) and the Bio-inspired Trust and Reputation Model for Wireless Sensor Networks (BTRM-WSN) is achieved in terms of the accuracy and the average path length. Both models will give quite good and accurate outcomes over dynamic Wireless Sensor Networks.

Keywords
Dynamic, Fuzzy, Bio-inspired, Sensor networks

1. INTODUCTION
Wireless Sensor Network comprises of hundreds to thousands of small nodes employed in a wide range of data gathering applications such as military, environmental monitoring and many other fields [1]. Due to limited energy and the difficulty in recharging a large number of sensor nodes, energy efficiency and maximizing the network lifetime are the most important design goals of a sensor network. This paper 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). Also, it is assumed that every sensor is only able to communicate with its direct neighbors, that it cannot establish a direct communication with a node more than one hop ahead. However, they are susceptible to a large number of security threats [2], some of them might be effectively mitigated with an accurate trust and reputation management [3,4]. Trust and reputation models have been recently suggested by many researches as an creative solution for guaranteeing a minimum level of security between two entities belonging to a distributed system that want to have a transaction or interaction. Many methods, technologies and mechanisms like fuzzy logic[5], Bayesian networks [6] or even bio-inspired algorithms [7] have been proposed in order to manage and model trust and reputation in systems such as P2P networks[8], ad-hoc ones [9], wireless sensor networks[10] (WSNs) or even multi-agent systems [11].

WSNs composed of sensors with restrictions in energy consumption, bandwidth, storage capacity, etc. In dynamic environment, some nodes switch off for awhile saving amount of energy. In this paper the simulation of the trust model, Linguistic Fuzzy Trust Model (LFTM) [12] over dynamic Wireless Sensor Networks is presented. This model enhances the interpretability of previous model, BTRM-WSN (Bio-inspired Trust and Reputation Model for Wireless Sensor Networks) and making 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) [13], 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 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 dynamic Wireless Sensor Networks are discussed. In section 4, conclusions are mentioned.

2. LINGUISTIC FUZZY TRUST MODEL
This model is considered an improvement for the trust and reputation model, BTRM-WSN model [7] which uses linguistic fuzzy sets and fuzzy logic for the enhancement. 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 shown in Figure 1.

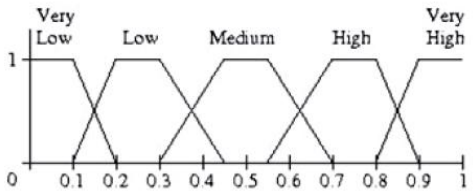

Fig 1: Linguistic labels and its defining fuzzy sets

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 are so evaluated. As can be guessed, the truth value of the consequent part is precisely that one achieved by the whole antecedent logic expression. The de-fuzzification method chosen in this paper is Center of Gravity. Linguistic Fuzzy Trust Model is shown in figure 2, emphasizing 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.

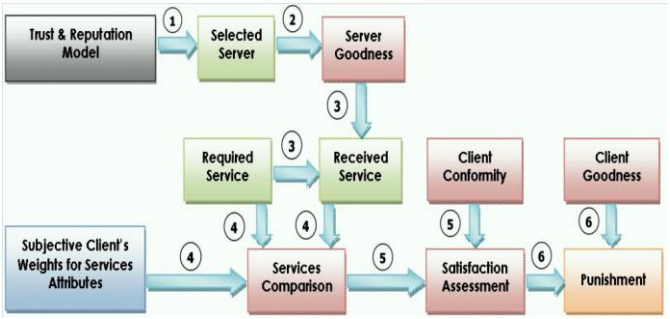

Fig 2: Linguistic Fuzzy Trust Model Steps.

3. EXPERIMENTS AND RESULTS

The simulated scenario consists of dynamic Wireless Sensor Networks with nodes continuously entering and leaving the environment .The decision scheme of when to switch off and switch on is as follows: when a server receives and supplies 20 requests it automatically switches off during a certain timeout. On the other hand, if a server does not receive at least 20 requests within a time interval, it also switches off during another timeout.

The evaluation environment used in this paper is Trust and Reputation Model Simulator for WSN [16], 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. It is assume 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, also, it is aimed to find the closest benevolent servers to the client requesting the service. 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%, while 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. The experiments are repeated over WSNs composed of 200, 300, 400 and 500 sensors. Simulation parameters used to perform the experiments are listed in table 1.

3.1 Experiments and Results of LFTM over Dynamic Wireless Sensor Networks

3.1.1 Selection Percentage of Trustworthy Servers

Table 2 shows the results achieved with LFTM model over static and dynamic WSNs. It is observed from the 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 equals to 60% regardless of 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 100 nodes which it is (99.6), 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 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 While the corresponding result for LFTM over dynamic WSNs gives the observation that when the percentage of malicious servers is less than or equal to 20% regardless of the size of the network, the accuracy is (less than 37%) which is very low value that makes the model not useful at all because it is assumed that if the selection percentage of trustworthy servers is under the 50%, then the model is completely useless. And the accuracy continues in increase, so when the percentage of malicious servers is greater than or equal to 60% regardless of the size of the network the accuracy is (above 70%) which is quite good. The maximum accuracy reached when the percentage of malicious servers is 90% and the size of the network is 100 nodes which is (96.77), 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 (90.3) which is still quite 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. In general the accuracy of the model over dynamic WSNs is less than the accuracy of the model over static WSNs.

Table 1. Simulation 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 Benevolent Malicious Cost weight Deliver weight	‘High’ or ‘ very high’ ‘Low’ or ‘very low’ 0.25 0.25	Client Conformity Goodness Price weight Quality weight	 Random Random 0.25 0.25

Table 2. Selection percentage of trustworthy servers

Dynamic WSN					**Static WSN**					**%Malicious Servers**
500 nodes	**400 nodes**	**300 nodes**	**200 nodes**	**100 nodes**	**500 Nodes**	**400 nodes**	**300 nodes**	**200 nodes**	**100 nodes**	
14.69	17.11	19.42	17.99	19.25	49.8	73.45	82.72	80.11	69.9	10
28.6	32.93	35.54	36.16	35.68	68.66	85.53	89.5	89.26	84.87	20
40.23	47.36	50.1	55.5	49.69	79.43	90.36	93.2	93.36	89.34	30
52.6	58.34	62.08	61.93	62.43	84.38	93.79	95.82	94.96	92.82	40
62.05	69.59	72.06	74.23	73.53	88.91	95.45	97.38	96.89	95.27	50
70.17	77.82	81.69	81.32	80.6	91.88	97.11	97.85	97.82	96.36	60
78.79	85.45	87.69	87.89	87.69	94.84	98.01	98.83	98.72	97.77	70
85.02	90.44	92.7	93.02	93.04	96.78	99.12	99.07	99.24	98.77	80
90.3	94.98	96.75	96.62	96.77	97.96	99.43	99.62	99.51	99.6	90

The selection percentage of trustworthy servers achieved with LFTM model over static WSNs is shown in figure 3(a) and it is observed that when the percentage of malicious servers is greater than or equal to 80% and the size of the network is less than or equal to 400 nodes the accuracy of the model is approximately equal and it is (above 98%) while when the

percentage of malicious servers is greater than or equal to 80% and the size of the network is 500 nodes the accuracy is (greater than 96%).While the results obtained for the model over dynamic WSNs are shown in figure 3(b), it is observed that the selection percentage of trustworthy servers increases as the percentage of untrustworthy servers increases regardless of the size of the network, it is reached to (96.77) but the accuracy here is less than the accuracy of figure 3(a).

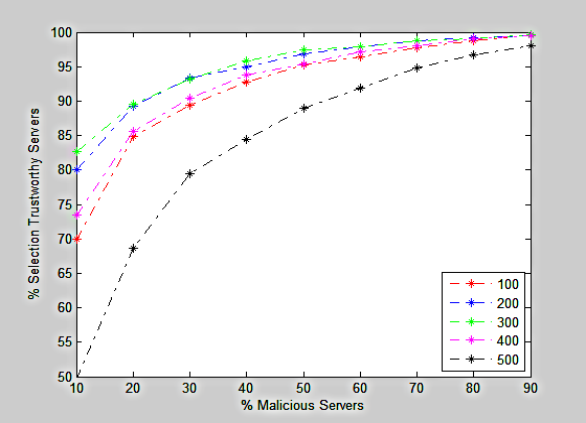

Fig 3(a): Selection percentage of trustworthy servers from Linguistic Fuzzy Trust Model over static WSNs.

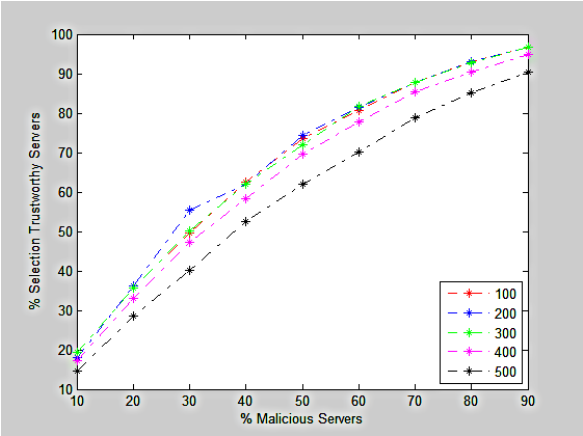

Fig 3(b): Selection percentage of trustworthy servers from Linguistic Fuzzy Trust Model over dynamic WSNs.

3.2 Comparison between Bio-Inspired Trust and Reputation Model for Wireless Sensor Networks Linguistic Fuzzy Trust Model over Dynamic 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 simulated and modeled.

3.2.1 Selection Percentage of Trustworthy Servers

Figure 5 shows the selection percentage of trustworthy servers achieved with BTRM-WSN and LFTM over dynamic WSNs composed of 100 to 500 sensors with a percentage of malicious servers from 10% to 90%. As it is observed from figure 5(a) which shows the outcomes achieved with BTRM-WSN that the selection percentage is nearly greater than 90% when the percentage of malicious servers is less than or equal to 40%, regardless of the size of the WSN. It remains qualified outcomes (above the 60%) when the percentage of malicious servers is less than or equal to 80%. Selection percentage gets worse when the percentage of malicious servers increases and even worse if the size of the Wireless Sensor Network is greater. Nevertheless, it can state that BTRM-WSN is running if the percentage of fraudulent sensors is less than 80%. While figure 5(b) shows the corresponding results achieved with LFTM, it is observed that when the percentage of malicious servers is less than or equal to 20% regardless the size of the network the accuracy is(less than 37%) which it is very low value that make the model not useful at all because it is assumed that if the selection percentage of trustworthy servers is under 50%, then the model is completely useless. The accuracy continues in increase by increasing the percentage of the malicious servers. When the percentage of malicious servers is greater than or equal to 60% regardless the size of the network the accuracy is (above 70%) which it is quite good .And the maximum accuracy reached when the percentage of malicious servers is 90% and the size of the network is 100 nodes which it is (96.77), 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 (90.3) which it is still quite high value.

3.1.2 Average Path Lengths Leading to Trustworthy Servers

The results obtained with LFTM model over static and dynamic Wireless Sensor Networks are listed in table 3. It is observed from the results achieved with LFTM model over static WSNs that the average path length decreases as the percentage of fraudulent servers increases regardless of 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 dynamic WSNs that the average path length decreases as the percentage of malicious servers increases regardless of the size of the network, but for a certain percentage of malicious servers and a certain size of network the average path length suggested by LFTM model over dynamic 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 (10.61).The results achieved with LFTM model over static networks are shown in figure 4(a) , the average path length is greater than or equal to (2.5) when the percentage of malicious servers is less than or equal to 50% ,while when the percentage of malicious servers is greater than 50% the average path length decreases and the change in average path length that obtained by varying the network size is very small, it is between (2.4) to (2.21) which it is small range. The outcomes in figure 4(b) shows the results that achieved with LFTM model over dynamic WSNs, here when the percentage of malicious servers is less than or equal to 70%, the results about the average path length is high and the differences between the results when varying the size of tested networks are also high, but when the percentage of untrustworthy servers is greater than 70% then the results about the average path length is small and the differences are quite small.

Table 3. Average path length leading to trustworthy servers

Dynamic WSN					Static WSN					%Malicious Servers
500 Nodes	400 nodes	300 nodes	200 Nodes	100 Nodes	500 nodes	400 nodes	300 nodes	200 nodes	100 nodes	
5.69	8.7	10.61	8.77	6.06	4.43	4.93	5.01	5.28	5.11	10
5.18	7.54	9.04	7.52	5.76	3.48	3.47	3.35	3.6	3.84	20
4.71	6.6	7.58	6.46	5.21	2.98	2.9	2.87	2.98	3.05	30
4.25	5.92	6.69	6.02	4.74	2.7	2.59	2.56	2.63	2.66	40
3.88	5.22	5.93	5.27	4.28	2.52	2.44	2.41	2.45	2.45	50
3.7	4.56	5.14	4.66	4	2.4	2.32	2.31	2.33	2.36	60
3.35	3.92	4.29	4.17	3.62	2.31	2.28	2.25	2.25	2.27	70
3.06	3.42	3.53	3.55	3.1	2.26	2.24	2.23	2.22	2.22	80
2.77	2.91	2.96	2.94	2.67	2.22	2.21	2.21	2.2	2.2	90

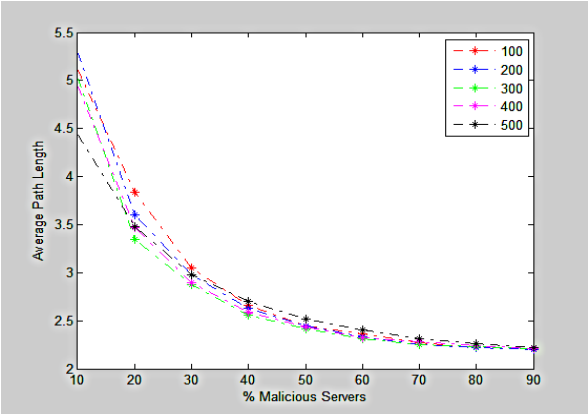

Fig 4(a): Average path length leading to trustworthy servers from Linguistic Fuzzy Trust Model over static WSNs

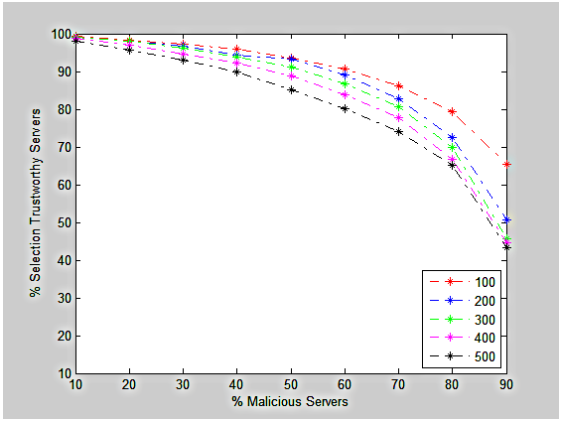

Fig 5(a): Selection percentage of trustworthy servers from Bio-inspired Trust and Reputation Model over dynamic WSNs

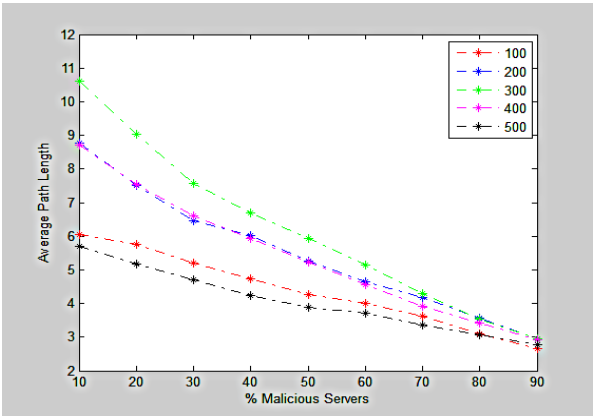

Fig 4(b): Average path length leading to trustworthy servers from Linguistic Fuzzy Trust Model over dynamic WSNs

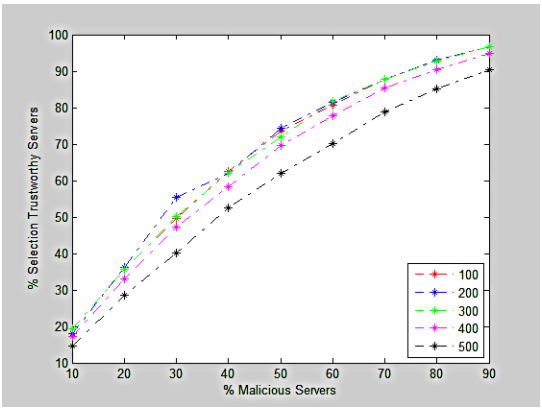

Fig 5(b): Selection percentage of trustworthy servers from Linguistic Fuzzy Trust Model over dynamic WSNs

The comparison between the two figures 5(a) and 5(b) gives the conclusion that in the case of simulation 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 since 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.

3.2.2 Average Path Length Leading to Trustworthy Servers

In this developed experiment, the measuring of the length (number of hops) of those paths found by BTRM-WSN and LFTM models leading to trustworthy servers presented and it is plotted as shown in figure 6. It is shown due to outcomes achieved with BTRM-WSN model over dynamic WSNs, when the percentage of malicious servers is less than or equal to 70%, the results about the average path length is small and the differences between the results when varying the size of tested networks are also small but when the percentage of untrustworthy servers is greater than 70%, then the results about the average path length is high and the differences are quite high. It is also observed that whatever the size of the network and the number of malicious servers, the average path length never exceeds 8.66 hops in any case, which is still a good outcome for Wireless Sensor Networks. Figure 6(b) shows the results that achieved with LFTM model over dynamic WSNs, as compared with the outcomes of figure 6(a), when the percentage of malicious servers is less than or equal to 70%, the results about the average path length is high and the differences between the results when varying the size of tested networks are also high but when the percentage of untrustworthy servers is greater than 70% then the results about the average path length is small and the differences are quite small . When the percentage of malicious servers is greater, then the average path length decreases regardless of the size of the networks.

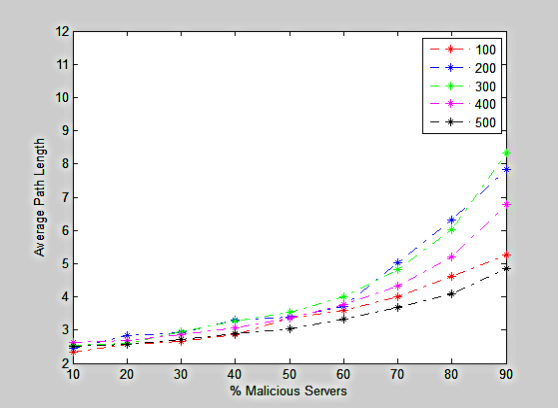

Fig 6(a): Average path length leading to trustworthy servers form Bio-inspired Trust and Reputation Model over dynamic WSNs

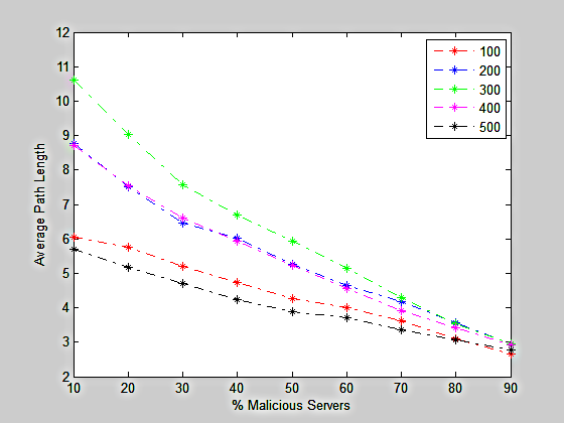

Fig 6(b): Average path length leading to trustworthy servers from Linguistic Fuzzy Trust Model over dynamic WSNs.

In the comparison between the two figures 6(a) and 6(b), it can be shown that in the case of simulation the BTRM-WSN model over dynamic WSNs, 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. Also the average path length leading to trustworthy servers suggested by the two models is slightly differ from one set of random WSNs to another when the percentage of malicious servers is less than or equal to 70% in the case of BTRM-WSN model and when the percentage of malicious servers is greater than or equal to 70% in the case of LFTM model with varying in the size of the wireless sensor networks, which gives an evidence about the scalability of the two models.

4. CONCLUSION

It is observed from the obtained results that the model gives higher accuracy and shorter path length in static environments, but significantly decreasing in accuracy and increase in the average path length when simulate the model over dynamic WSNs but with more saving in energy. The experiment of the LFTM model over dynamic WSNs gives the proof that LFTM obtains quite good and accurate outcomes over dynamic Wireless Sensor Networks, with a low influence from the size of the networks and the percentage of malicious servers. It is also observed that as number of malicious servers increases the selection percentage of trustworthy servers decreases in the case of BTRM-WSN while increases in the case of LFTM and the average path length suggested by BTRM-WSN increases while decreases in the case of LFTM. Also 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.

5. REFERENCES

[1] L. Akyildiz, W. Su, Y. Sankarasubramanian and E. Cayirci, “A survey on sensor networks”, IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, 2002.

[2] GómezMármol F, Martínez Pérez G ,"Security threats scenarios in trust and reputation models for distributed systems" ,Elsevier Computers & Security,28(7),545–556,2009.

[3] Marsh, S. P. , "Formalising trust as a computational concept", Ph.D. thesis, Department of Computing Science and Mathematics, University of Stirling,1994.

[4] Marti, S., & Garcia-Molina, H. ,"Taxonomy of trust: categorizing P2P reputation systems", Computer Networks, 50(4), 472–484,2006.

[5] Tajeddine A, Kayssi A, Chehab A, Artail H," PATROL-F- a comprehensive reputation-based trust model with fuzzy subsystems", Third international conference, ATC,LNCS, Wuhan, China: Springer, vol. 4158, p. 205–17, 2006.

[6] Wang Y, Cahill V, Gray E, Harris C, Liao L ,"Bayesian network based trust management", Third international conference, ATC, LNCS, Wuhan, China: Springer, Vol. 4158, p. 246–57, 2006.

[7] Gómez Mármol F, Martínez Pérez G ," Providing trust in wireless sensor networks using a bio inspired technique", Telecommunication Systems Journal, 46(2),163–180,2011.

[8] Almena´ rez F, Marı´n A, Campo C, Garcı´a C , "PTM: a pervasive trust management model for dynamic open environments", First workshop on pervasive security and trust, Boston , USA, Aug 2004.

[9] Moloney M, Weber S, "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, p. 153–60 ,Athens, Greece, Sep 2005.

[10] Boukerche A, Xu L , El-Khatib K ,"Trust-based security for wireless ad hoc and sensor networks", Computer Communications,30(11–12),2413–27,2007.

[11] Sabater J, Sierra C , "REGRET: reputation in gregarious societies", Proceedings of the fifth international conference on autonomous agents ,ACM Press, p.194–5, Montreal, Canada, 2001.

[12] GómezMármol 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), 838–845, DOI: 10.1109/CIT.2010.158, Bradford, UK, 2011.

[13] Dorigo, M. , & Gambardella, L., "Ant colony system: a cooperative learning approach in the traveling salesman problem", IEEE Transaction on Evolutionary Computing, 1(1), 53 66,1997.

[14] Pedrycz W, Gomide F," An Introduction to Fuzzy Sets: Analysis and Design", the MI Press: Cambridge, Masssachusetts, USA, 1998.

[15] Jang JSR, Sun CT, Mizutani E, "Neuro-Fuzzy and Soft Computing", Prentice Hall: Upper Saddle River, New Jersey, USA, 1997.

[16] 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, DOI:10.1109/ICC.5199545, Dresden, Germany, 2009.