Security Threats of Collusion-based Linguistic Fuzzy Trust Model for WSN

Firas Ali Al-Juboori, PhD.
Department of Computer Engineering
University of Baghdad
College of Engineering

Sura F. Ismail
Department of Computer Engineering
University of Baghdad
College of Engineering

ABSTRACT

In the last few years management of trust and reputation models over distributed systems has been proposed as a novel and accurate way of dealing with some security deficiencies which are inherent to distributed environments. Many models and theories have been designed in order to effective and accurately manage trust and reputation in those environments. Nevertheless, very few of them take into consideration all the possible security threats that can compromise the system. In this paper, an analysis of the effect of the security threats on the selection percentage of trustworthy servers (the accuracy) and average path length suggested by the Linguistic Fuzzy Trust Model over static Wireless Sensor Network are presented. It is observed that the accuracy of the model with collusion decreases as compared to the accuracy of the model without collusion while the results about the average path length suggested by the model are better and the change in it by varying the number of trustworthy servers is very low, so the average path length of the model with collusion is better than of it without collusion. Also it must be mentioned that the evaluation environment used in this paper is Trust and Reputation Model Simulator for Wireless Sensor Network.

General Terms

Linguistic Fuzzy Trust Model**,** Bio-inspired Trust and reputation Model**,** Trust and Reputation Model Simulator for Wireless Sensor Network.

Keywords

Collusion, Fuzzy, Security Threats, Sensor Networks.

1. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices called sensors which cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control. Individual sensor nodes posses limited processing, communicating and energy recourses. However, due to their important restrictions, they usually suffer from many security weaknesses, which make them often vulnerable to certain threats.

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). A malicious node could avoid reaching its benevolent neighbors, or leading to other malicious nodes, forming thus a collusion. Therefore it is necessary to accurately distinguish trustworthy nodes from fraudulent ones. This trustworthy nodes distinguishing can be achieved through a trust and reputation model [1,2].

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 studies works and models have been designed and developed in this direction. Many methods, technologies and mechanisms like fuzzy logic[3], bayesian networks [4] and bio-inspired algorithms [5] have been proposed in order to manage and model trust and reputation in systems such as P2P networks[6], ad-hoc ones [7], wireless sensor networks[8] (WSN) or even multi agent systems [9].Some of these models have been analyzed in [10,11], and realized that there are some security threats directly related to this specific kind of models. This paper shows the effect of the security threats on the performance of the Linguistic Fuzzy Trust Model (LFTM) and comparing the results of the model with and without collusion. The Linguistic Fuzzy Trust Model (LFTM) enhances the interpretability of the Bio-inspired Trust and Reputation Model (BTRM WSN) [5] 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) [12], 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 paths.

The rest of this paper is organized as follows :The Linguistic Fuzzy Trust Model (LFTM) is described in section 2 .In section 3, security threat will described .Simulations and results of experiments are discussed in section 4.In section 5 conclusion about the results is described. Section 6 describes the acknowledgment. Finally in section 7 lists of references is described.

2. LINGUISTIC FUZZY TRUST MODEL (LFTM)

This model is an enhancement for the pervious trust and reputation model, BTRM-WSN model [5] 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 Figure 1.

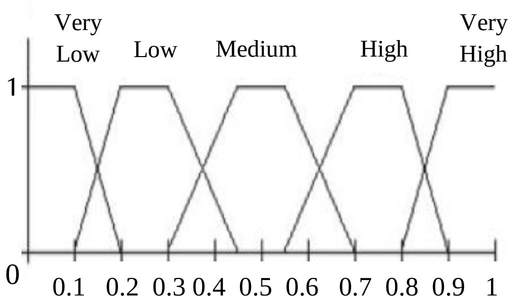


Figure 1. Linguistic labels and its defining fuzzy sets

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 [**13,14**].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 figure 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. The fact that every node maintains the pheromone traces of its neighbors can lead to some security threats that appear if a malicious server colludes with other malicious servers, because a sensor is only able to manage the pheromone traces of its neighbors, but by the same reason it cannot control the pheromone traces that its neighbors have associated with it.

The idea of collusion where malicious peers form a malicious collective by assigning the maximum trust value to other malicious peers in the network is showing in figure 3.

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.

The use of the different fuzzy grids in the Linguistic Fuzzy Trust Model is described in [**15**].

3. SECURITY THREATS

Every node maintains the pheromone traces of its neighbors and it is the only one who can manage, control and modifies them, this fact can lead to some security threats [**16**].

But the security threats can appear if a malicious server colludes with other malicious servers, because a sensor is only able to manage the pheromone traces of its neighbors, but it cannot control the pheromone traces that its neighbors have associated with it, and that collusion is only possible if the malicious sensors know each other and also know who the benevolent sensors are, and this assumption is not always feasible in every wireless sensor network.

The security threats that assumes here is that malicious sensors can praise their malicious neighbors by assigning them the maximum level of pheromone. Equally they can slander their benevolent neighbors by giving them the minimum value of pheromone.

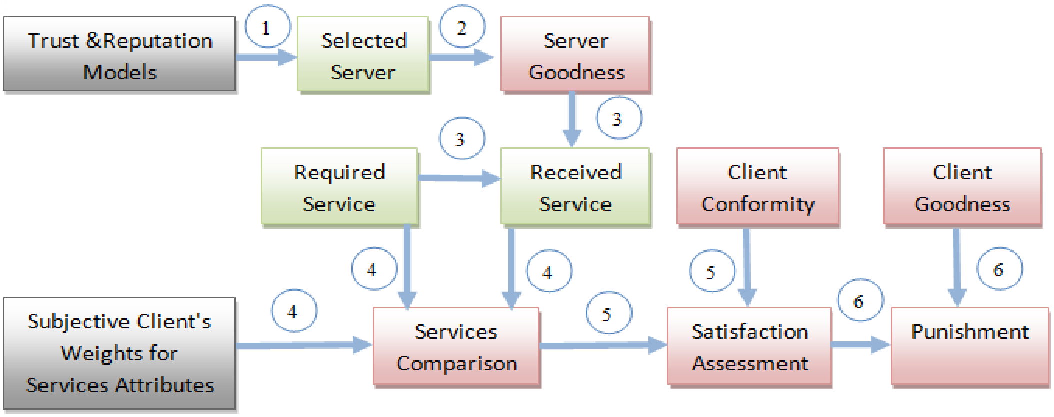


Figure 2. Linguistic Fuzzy Trust Model Steps

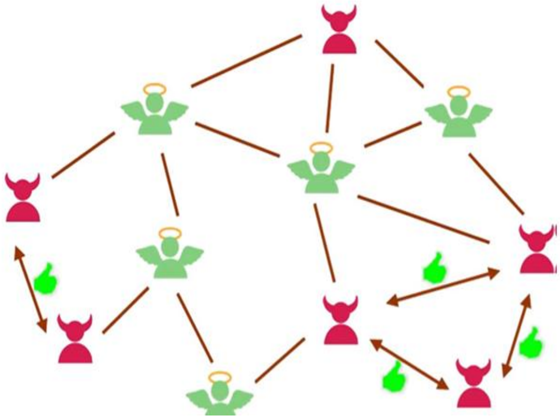


Figure 3. Malicious collectives

4. EXPERIMENTS AND RESULTS OF LINGUISTIC FUZZY TRUST MODEL OVER STATIC WSN WITH COLLUSION

The tested scenario is consisting of static wireless sensor networks where collusion among all malicious servers composing the network was built. As explained in Section 3, since every sensor is the only one who can manage the pheromone traces associated with its neighbors, malicious servers could collude an falsely praise themselves or slander benevolent servers. Here the worst situation is chooses, where every malicious server always had the maximum pheromone value for those of its neighbors who were also malicious, and the minimum pheromone value for those neighbors who were benevolent. How every sensor knows if its neighbors are malicious or benevolent is out of the scope of this paper.

The evaluation environment used in this paper is Trust and Reputation Model Simulator for WSN [17], 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 is calculated. Secondly, the average path length of the solutions found by the model is also calculated and in an environment with a lot of restrictions like WSNs, the shorter path is always preferred since it supposes less consumption of sensors' resources.

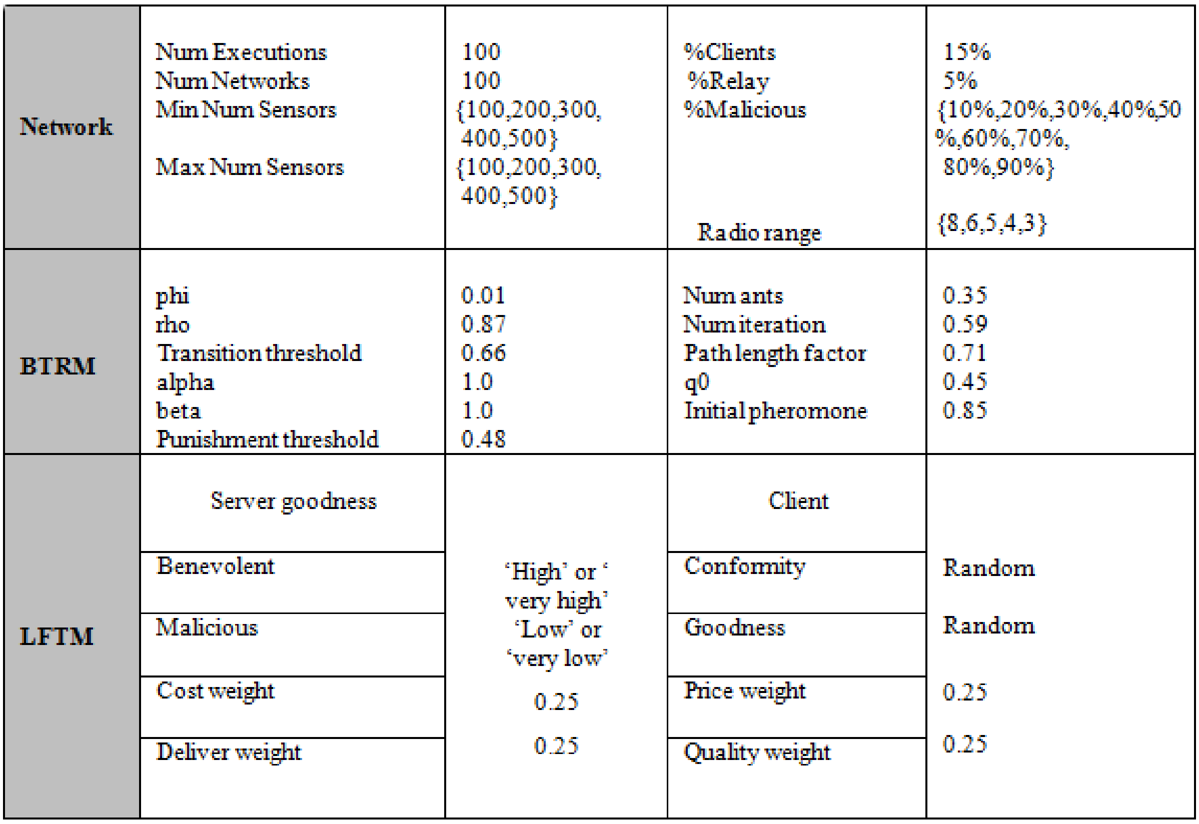
The experiments that carried out here had the following structure. The model is launched 100 times (i.e. each client applied for a service 100 times) over 100 WSNs randomly generated, each one composed of 100 sensors. On each network, the percentage of sensors acting as clients was always a 15%, 5% acts 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), and those experiments are repeated over WSNs composed of 200, 300, 400 and 500 sensors. These parameters and others used to perform the experiments are listed in table 1.

4.1 Selection Percentage of Trustworthy Servers

The results for the selection percentage of trustworthy servers achieved with LFTM over static network with and without collusion are listed in table 2. As it is observed from the results of the model without collusion 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%, 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 a high value. In general the selection percentage of trustworthy servers increases as the percentage of malicious servers increases regardless the size of the network, the reason for the increasing 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 the corresponding result for LFTM over static WSN with collusion gives the observation that when the percentage of malicious servers is less than or equal to 50% regardless the size of the network the accuracy is(less than 50%) which it is low value that make the model not useful at all because here assume that if the selection percentage is under the 50%,

Table 1. Experiment parameters



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

Then the model is completely useless. While the accuracy of the model increases(above 50%) when the percentage of untrustworthy servers increases above 50% and observes that in worse case when the percentage of malicious servers is 90% and the size of the network is 500 nodes then the accuracy is (82.67). And in general the accuracy of the model with collusion is less than the accuracy of the model without collusion that excepted as malicious server collude with other malicious servers and gives them the maximum pheromone value while gives the minimum pheromone value for those neighbors who were benevolent. The selection percentage of trustworthy servers increases as the percentage of malicious servers increases regardless the size of the network, the reason again for this increasing in 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. The results that obtained in table 2 are plotted in figure 4 .The selection percentage of trustworthy servers achieved by the LFTM model without collusion is showing in figure 4(a) and it is observed that when the percentage of malicious servers is greater than or equal to 80% the accuracy of the model is approximately equal and it is (above 98%) 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 accuracy is (greater than 96%). While the results obtained for the model with taking the effect of collusion is showing in figure 4(b), here the accuracy is deceased as compared with the accuracy of part (a) and the relationship between the accuracy of the model and the percentage of malicious servers is approximately linear. It is also observed that when the percentage of malicious serves is less than or equal to 30% the accuracy of the model is approximately the same for various sizes of network, and for the collusion-based model the maximum accuracy obtained is approximately (90%) when the percentage of malicious servers is 90%.

Table 2. Selection percentage of trustworthy servers

Static WSN with collusion					**Static WSN without collusion**					**%Malicious Servers**
500 nodes	400 nodes	300 nodes	200 nodes	100 nodes	500 nodes	400 nodes	300 nodes	200 nodes	100 nodes	
8.87	9.67	9.7	8.49	9.4	49.8	73.45	82.72	80.11	69.9	10
18.71	19.3	18.79	19.26	19.52	68.66	85.53	89.5	89.26	84.87	20
28.33	29.16	29.4	29.22	27.25	79.43	90.36	93.2	93.36	89.34	30
36.72	38.28	38.94	39.03	37.66	84.38	93.79	95.82	94.96	92.82	40
46.03	49.5	47	49.33	49.1	88.91	95.45	97.38	96.89	95.27	50
56.52	57.86	60.44	59.07	57.7	91.88	97.11	97.85	97.82	96.36	60
64.75	68.6	68.9	70.27	68.5	94.84	98.01	98.83	98.72	97.77	70
74.02	78.61	79.88	78.48	76.81	96.78	99.12	99.07	99.24	98.77	80
82.67	88.49	89.02	88.72	86.34	97.96	99.43	99.62	99.51	99.6	90

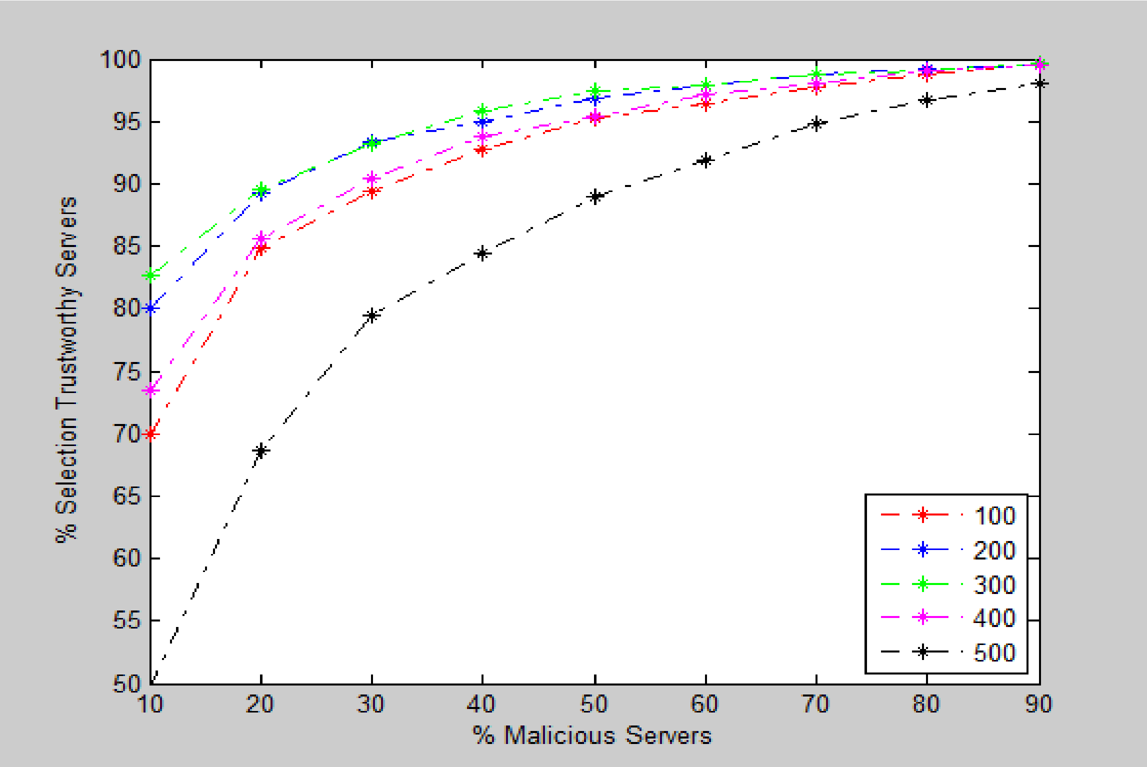


Figure 4(a).Selection percentage of trustworthy servers from Linguistic Fuzzy Trust Model over static WSN without collusion

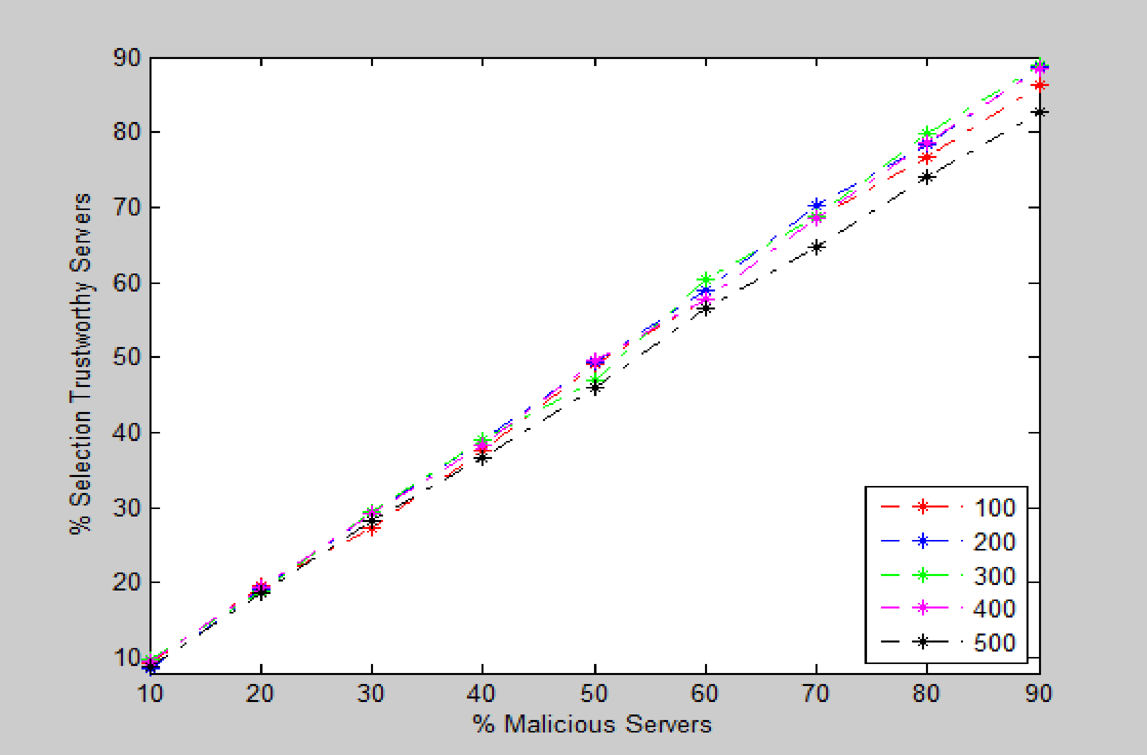


Figure 4(b). Selection percentage of trustworthy servers from Linguistic Fuzzy Trust Model over static WSN with collusion

4.2 Average Path Length Leading to Trustworthy Servers

Table 3 listed the results achieved with the LFTM model over static network with and without collusion-based. It is observed from the results obtained by applying LFTM model without collusion effect that the average path length decreases when the percentage of fraudulent servers increases regardless the size of the network and it is observed 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 from the results obtained from the collusion-based model shows the best results for the average path length that achieved by LFTM model over static WSN as compared to collusion-free model .Here the average path length never exceeds (2.8) hops. The results for the average path length for different percentage of malicious servers and for various size of network are near from each other, it is changes in low range. And in general also the average path length decreases as the number of good servers available decreases and as the size of the network increases. This means that most of the trustworthy servers found are very near to the client.

The results that obtained in table 3 are plotted in figure 5.The results achieved from the collusion-free model are showing in figure 5(a) ,here 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 5(b) show the results that achieved from LFTM model with collusion. When the percentage of malicious servers is greater than or equal to 40% the results here is between (2.76) to (2.64) which it is small range, while in the case of collusion-free model the average path length is between (5.28) to (2.56) .But when the percentage of malicious servers is above 40% then the average path length here is between (2.73) to (2.66) while in the case of collusion-free model the average path length is between (2.52) to (2.22), so in the case of collusion-based the results for all numbers of malicious servers and for all values of network size are approximately equal and small ,which meant that servers found are very near to the client. It can also mean that in such an adverse situation like this one (static WSNs with collusion), LFTM is unable to find benevolent servers which are too far from the clients. And it makes sense getting these values. If the proportion of malicious servers is low, it will be probable that some benevolent servers stay near the clients. And if that percentage is high, then malicious colluding servers will avoid clients’ ants to travel quite far in order to find benevolent servers.

Table 3. Average path length

Static WSN with collusion					Static WSN without collusion					%Malicious Servers
500 nodes	400 nodes	300 nodes	200 Nodes	100 nodes	500 nodes	400 nodes	300 nodes	200 nodes	100 nodes	
2.64	2.74	2.76	2.75	2.71	4.43	4.93	5.01	5.28	5.11	10
2.64	2.73	2.77	2.75	2.71	3.48	3.47	3.35	3.6	3.84	20
2.65	2.73	2.76	2.76	2.71	2.98	2.9	2.87	2.98	3.05	30
2.66	2.75	2.76	2.74	2.71	2.7	2.59	2.56	2.63	2.66	40
2.66	2.75	2.77	2.75	2.74	2.52	2.44	2.41	2.45	2.45	50
2.67	2.75	2.76	2.77	2.74	2.4	2.32	2.31	2.33	2.36	60
2.68	2.76	2.77	2.75	2.73	2.31	2.28	2.25	2.25	2.27	70
2.69	2.75	2.77	2.77	2.73	2.26	2.24	2.23	2.22	2.22	80
2.71	2.76	2.78	2.77	2.78	2.22	2.21	2.21	2.2	2.2	90

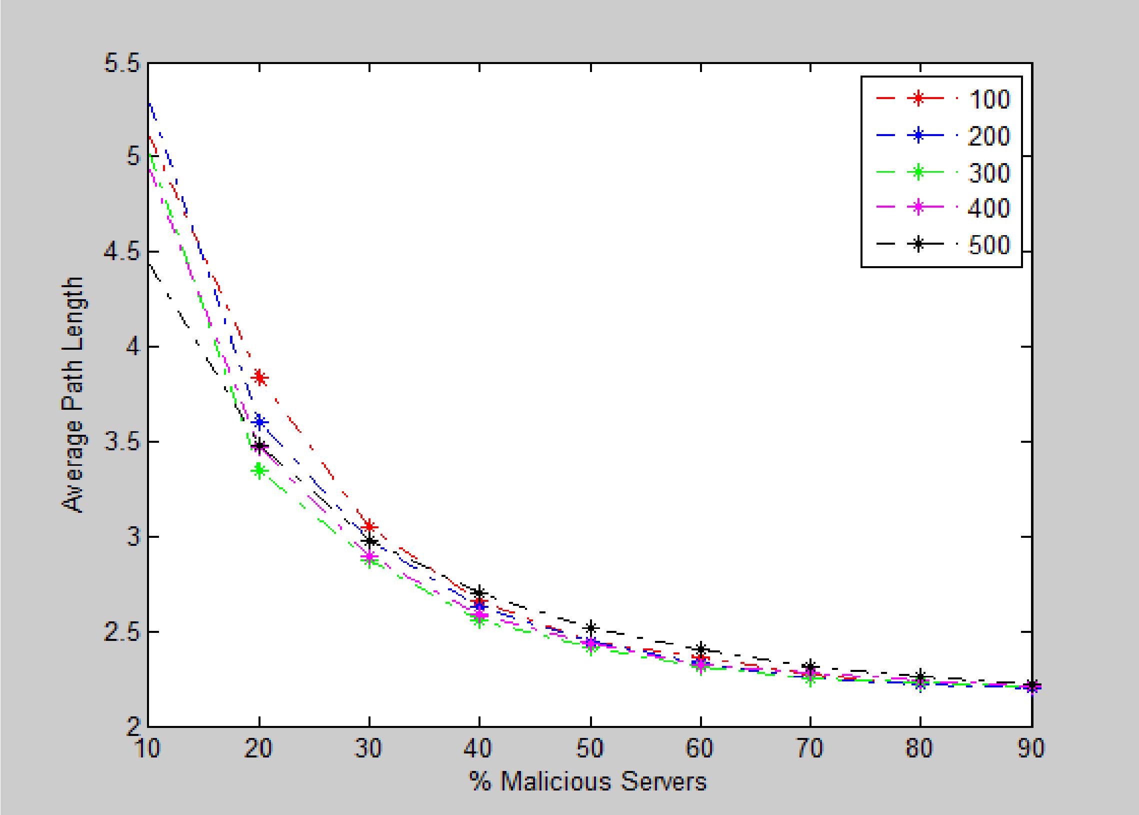


Figure 5(a). Path length from Linguistic Fuzzy Trust Model over static WSN without collusion

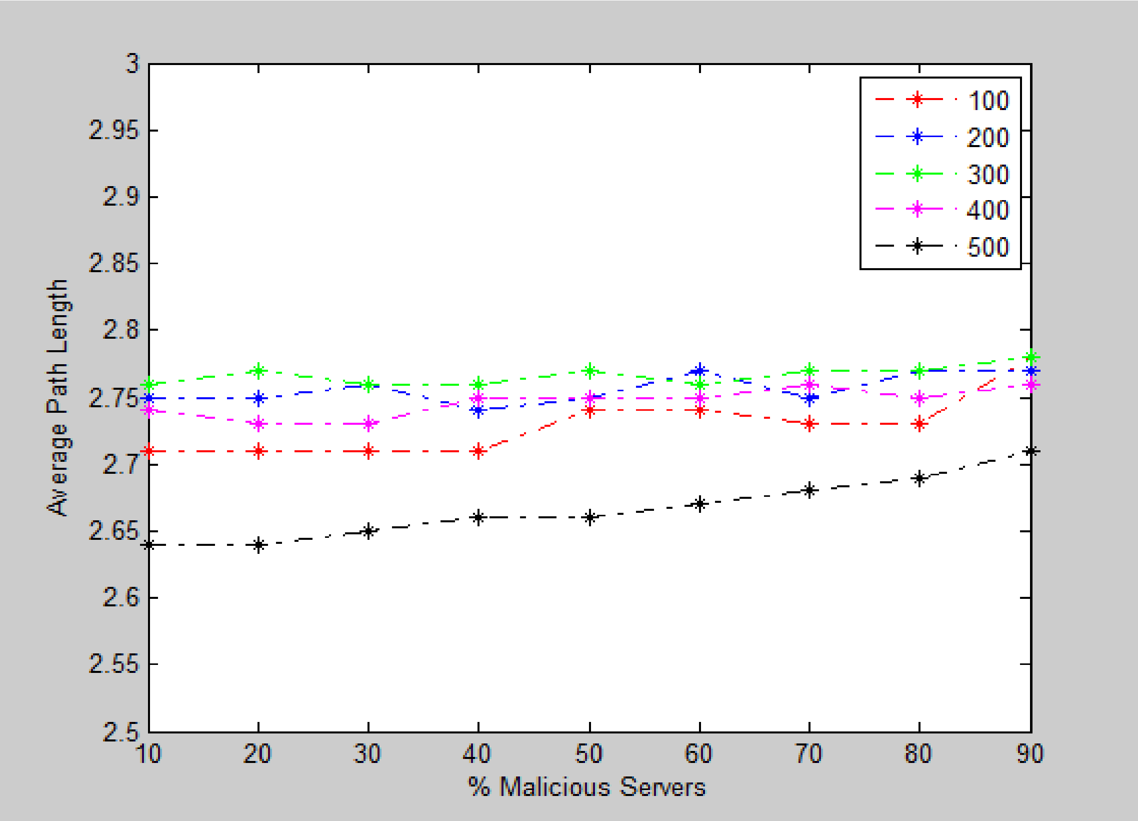


Figure 5(b). Path length form Linguistic Fuzzy Trust Model over static WSN with collusion

5. CONCLUSION

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.

This paper presented the effect of security threats that can appear if a malicious server colludes with other malicious servers. Here the worst case is taken, where malicious sensors can praise their malicious neighbors by assigning them the maximum level of pheromone. Equally they can slander their benevolent neighbors by giving them the minimum value of pheromone. In this paper the results that obtained by applying the LFTM model over static WSN with collusion are compare with the results achieved by the collusion-free model, and it is observed from the comparison that outcomes for the selection percentage of trustworthy servers are worse, as the number of good severs decreases while the results for the average path length are better which meant that good servers found are very near to the client but if the proportion of malicious servers is low, it will be probable that some benevolent servers stay near the clients, while if that percentage is high, then malicious colluding servers will avoid clients' ants to travel quite far in order to find benevolent servers.

6. ACKNOWLEDGMENTS

The authors would like to thank the reviewers for their detailed comments on earlier versions of this paper.

7. REFERENCES

[1] Marsh, S. P. 1994 Formalising Trust as a Computational Concept. Doctoral Thesis, Department of Computing Science and Mathematics, University of Stirling.

[2] Marti, S., and Garcia-Molina, H. 2006. Taxonomy of trust: categorizingP2P reputation systems. Computer Networks, 50(4):472–484.

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

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

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

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

[7] Moloney M, 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, p. 153–60, Athens,Greece.

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

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

[10] Josang A, Ismail R, Boyd C .2007. A survey of trust and reputation systems for online service provision. Decision Support Systems, 43(2):618–44.

[11] Sabater J, Sierra C. 2005. Review on computational trust and reputation models. Artificial Intelligence Review, 24(1): 33–60.

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

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

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

[15] GómezMármol F, Gómez Marín-Blázquez J, Martínez Pérez G. 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 (TSP-10), 838–845, DOI: 10.1109/CIT.2010.158, Bradford, UK.

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

[17] Gómez Mármol F, Martinez Pérez G. 2009. 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. DOI:10.1109/ICC.5199545,Dresden, Germany.