International Journal of International Journal of Control and Automation
Vol. 12, No. 4, (2019), pp. 134-150

A Fuzzy and Trust based Routing in Wireless Sensor Networks

Radhika Gupta[1], Sahil Verma[2], Kavita[3],Atul Malhotra[4]
[1]M.Tech Student, Lovely Professional University
Email:radhikagupta.0202@gmail.com[2]Associate Professor,Lovely Professional University Email:sahilkv4010@yahoo.co.in
[3]Associate Professor,Lovely Professional University
Email:dhullkavita@yahoo.co.in
[4]Assistant Professor,Lovely Professional University Email:atul.18011@lpu.co.in
*Corresponding Author: sahilkv4010@yahoo.co.in **

Abstract

Mobile ad hoc networks is a prominent research topic and wireless sensor networks are one of the category of these types of networks. Sensor networks are challenged due to their ad hoc nature, they are prone to security attacks and their reliance on battery power. To meet these challenges, clustering is a traditional technique aiding to improve network lifetime by preserving the node's energies. The clustering schemes used show a few downsides which confine their use for functional systems. In the first place, cluster heads are ordinarily chosen from all sensor nodes present in the system, and therefore, unequal groups might be produced and secondly, manual definition of controllable parameters. Another area of concern is protection of network from security attacks which can be from insider nodes or outsiders. Therefore, the concept of trust is proposed along with the adaptive neuro fuzzy logic for a secure and energy efficient network. Trust is used to provide security from hostilesensors in the network andneuro fuzzy logic for selecting a competent head for a cluster based routing. Adaptive neuro fuzzy logic rules are fired according to node's energy, trust values and transmission distance to choose cluster head.

Keywords: *Wireless sensor networks, adaptive neuro fuzzy logic, trust management, security, performance analysis*

1. Introduction

Sensors are seen as a powerful and computational devices used for different automotive purposes, reducing the human work. Wireless sensor network (WSN) is a collection of these powerful sensors working collectively to make things better and easy. Sensor networks is a popular class of mobile ad hoc networks used for different purposes to control and produce a proper scope of justifications and needs. Like other hot research topics [19] in ad hoc field for example, vehicular ad hoc networks (VANET), wireless mesh networks (WMNs), WSNs are also being studied widely for research works and their use in industries is obvious one. WSNs work in a manner that they sense the data in the environment field they are deployed through remote connections, gather it and communicate it following different sensors and associate with different systems like remote Ethernet.

Consequently, the deployment of these systems strictly and heavily depends upon the particular execution situation and the needs of the application regarding credibility, ease of use. These days, sensors are widely used [16] from industry to medical and agricultural areas. Few of the application areas include various medical treatments and patient health monitoring, in defence sector to monitor the enemy or attacks. In agriculture field to monitor crop health and with the help of satellites to figure out the environmental conditions and accordingly suitable crops to grow.

Security of a communication is always been a big concern. In case of wireless communication it becomes more necessary as well as difficult to prevent the security breach. An ad hoc network is prone [18] to outsider as well as insider attacks. Sensors are used in battlefields and in many security related applications. Therefore, this becomes utmost important to provide a secure data transfer within sensors to give accurate results. Trust is a traditional term [5] used as a factor to rely upon something. Trust, in general terms is the degree of belief [4] of social behaviour of an entity. In terms of networks, trust fits in the way nodes initiating the communication with other nodes, without having any prior interaction or knowledge about them. It has been said that [1] there is a need for best trust management schemes to relate and analyse the ways trust can be used for WSN. Best trust management scheme here can draw a meaning that based on one's requirement, trust type needs to be identified. As mentioned in the [2] trust can be used to avoid different types of attacks and more importantly for which area. In most of the works given on trust, it's been said that trust is proactively used for the detection and segregation [3] of flawed nodes which apparently consume more energy and ultimately die, degrading overall performance of network.

Fuzzy logic is a branch of artificial intelligence to handle the uncertainty in decisions. Fuzzy inference system [10,12] draws outputs from fuzzy inputs i.e. parameters which are not certain. The data sets whose values are not crisp (exactly clear) forms fuzzy data set. Unlike an exact value which can be true/false, yes/no, 0/1 fuzzy values are multiple values under a certain possible range. Like in the case of 0 and 1 fuzzy values can take multiple decimal values starting from 0 till 1. Therefore, fuzzy logic is used to handle partial truth. Adaptive neuro fuzzy inference system is a type of artificial neural network (ANN) and is also called as adaptive network based fuzzy inference system. Neuro-adaptive learning techniques [4] provide a medium for the fuzzy modelling mechanism to learn information about a data set. The ANN learning algorithm [6] plays its role in the process of changing the parameters and the value in the system to adjust its condition. It is basically tuning of one of the type of fuzzy inference system, Sugeno type [20] by using training data. The anfis command produces a single output fuzzy inference system (FIS) and attunes the system parameters using the specified input/output training data. The training algorithm uses combination of least-squares and back-propagation gradient descent methods to model the training

data set. This paper proposes a trust and neuro fuzzy based solution for providing the security and optimizing the network efficiency parameter. The rest of the paper consists of the study of the previous work done on trust and sensor networks, proposed solution with results of different scenarios and conclusion and future scope.

2. Related Work

K. P. Rama Prabha, N. Jeyanthi (2018) have proposed a fuzzy logic andtrust based technique for dynamic secure routing [15] in mobile ad-hoc networks. Three parameters form trust metrics, historical trust, behaviour trust and neighbour trust. The main purpose of applying trust is to segregate the malicious nodes in the network. The fuzzy logic is used to form the cluster of nodes in the network, providing network energy efficiency. The work gives better results for delay and packet delivery ratio.

V. Ram Prabha P. Latha (2017) have proposed a fuzzy and trust solutionfor refining malicious node detection precision.Initially, a multiple value trust is inputted for fuzzification. Types of trust models considered are, communication behaviour trust (CBT) and social behaviour trust (SBT) [14].

Yuxin Liu, Mianxiong Dong (2016) gave a secure and trustable routing scheme [13]. The active trust method comprises active detection routing and data detection routing protocol and detects malicious nodes and trust values. The calculated results show that the scheme proves to give high security, scalability and energy efficiency.

Harold et al. (2016) proposed an improved cluster based key management (ECBK) protocol [17] for safecommunication by evaluating node's degree of trust. The protocol also provide load balancing among clusters. However, mobility of nodes and sink is another factor not considered in this work.

Hui Xia, ZhipingJia, Edwin H.-M. Sha (2014) have put forwarded a trust-based multicast routing protocol (FAPTrust) [8]. Here, the trust parameters are calculated by using fuzzy logic. Fuzzy logic rules prediction is used to predict updated trust value of node and entropy method based fuzzy AHP theory to weight the decision factors. The proposed solution has improved quality of network interactivity, trust credibility, spiteful node detection and enhancement of system security. However environmental factors for trustcalculation are not considered.

Li Yu et al. (2012) say that trust frameworks [11] evaluate trustworthiness between nodes by figuring out every single node's behaviour. Based on fuzzy fundamentals, three-dimensional classifier is used to find trust. The classification is based on behaviour space namely direct, indirect and neighbour trust. Inclusion of more behavioural aspects like past behaviour analysis of nodes, can give more accurate results which was not covered in this work.

FenyeBao et al. (2012) have considered extensibility and re-configurability, to handle the hostile sensor nodes and scan attacks [9] on the network.Extensive

work is done on trust and a research scope is given to test environment with autonomous nodes without sink node.

Tajeddine et al. (2011) proposed a fuzzy incorporated reputation based trust [21] for a distributive network. Fuzzy logic is included, so as to take decisions on current state of data i.e. a decision subsystem which decides whether to place an interaction/transmission or not. The reputation index (RI) value of the systems is dependent on three factors, which are correctness of result, time of interaction and monetary value of the interaction. The model is built for a distributed system not exactly for sensor networks where network's energy, transmission power along with the trust metrics can form an energy efficient solution for sensor networks.

Ameer Ahmed Abbasi et al. (2010) have given taxonomy [7] and a general review of clustering schemes. Important parameters considered for a wireless sensor network in this paper, mainly include energy efficiency, scalability, cluster stability, overlapping, convergence time, location awareness and node mobility. Main purpose behind clustering is for the balancing of load, increased connectivity, minimal cluster count and reduced delay.

3. Proposed Work

In this work, a network is deployed in an area of *a by a* dimensions in metres with varying *n* nodes. The aim is to test performance metric packet delivery ratio and security level by using the algorithm to form clusters and select cluster heads from candidate cluster heads. The selection is done by using trust value and adaptive neuro fuzzy logic. The algorithm for the proposed technique is as follow:

Algorithm

Updating the node's energy and check for dead node

```
For n iterations
    For all nodes
            E=E+S(i).E          where E initially = 0 and S(i).E is
node's energy
    End For
    For all nodes
        If S(i).E<=0
            Mark node as dead
        End If
    End For
    If total nodes-dead <=10
        Break
```

Clustering process

```
    For k clusters
      For all nodes
        If c(node) <=
```

(Probl/(1-Probl*mod(r,round(1/Probl)))))

incrementCHcount *where c(node) is random probable value (0 to 1), Prob1 is probability of head=.05 and CHcount is initialized to 1*

Calculate energy and distance of nodes from sink

If CHcount>k

Break

End if

End if

End for

End for

anfis();

End for

Anfis algorithm

For all CHcount

Calculate minimum distance among cluster nodes

If minimum distance < threshold distance(d)

Store the coordinates of cluster and that node of cluster.

Trust is calculated as the exponential function of the packet loss ratio.

packet loss ratio (p) =

1-(10 * log10(diss.^alpha*))* *(where alpha=0.1 and diss is distance from nearest node)*

Trust = sin(2*p)/exp(p/5)

n= anfis(distance, trust, energy, epochs)

end if

end for

Simulation Results

For simulation of the proposed work Matrix Laboratory (MATLAB) has been used. Table 1 represents the parameters used for simulation. Here, experiment is repeated with different number of nodes like 50, 75 and 100 at different iterations of 30 and 50. Initially each node is assigned with 1J of energy and minimum distance for communication is 50m.

Table 1 Simulation Parameters

Simulation Parameters	
Parameter	**Values**
Area	200m *200m
Energy Level	1J
Nodes deployment	Random way point
Number of Nodes	Varied
Threshold distance	50m
Number of iterations	Varied

Scenario 1: 50 nodes were deployed and simulation was run for 30 iterations.

Figure 1 represents the energy consumption graph for 50 nodes for 30 iterations at 1J of energy.

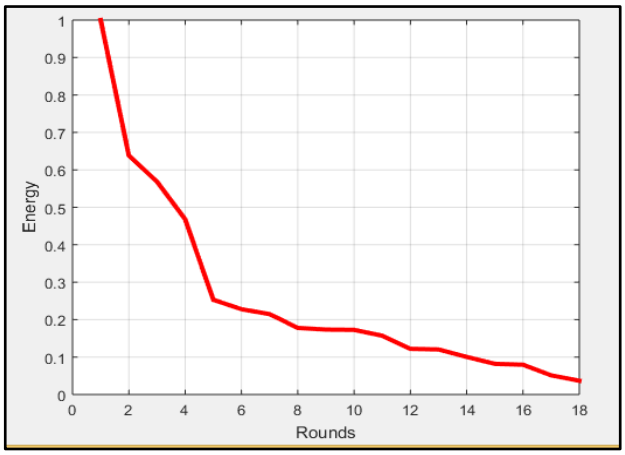

Fig 1 Energy consumption graph for scenario 1

Figure 1 shows that till last iteration almost energy of network is consumed. The corresponding collected values of packet delivery ratio are shown in table 2. Based on these values graph is plotted, represented in figure 2. The graph shows that average packet delivery ratio for this scenario is 98.6%.

Table 2 Packet delivery ratio for scenario 1

Rounds	Values of packet delivery ratio
1	1
2	1
3	1
4	.998
5	.998
6	.994
7	.994
8	.989
9	.986
10	.983
11	.978
12	.975
13	.972
14	.969
15	.965

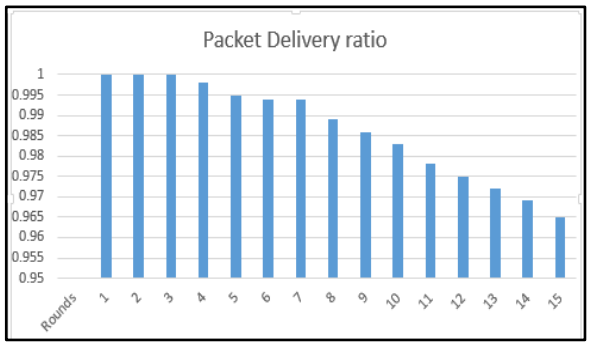

Fig 2Packet delivery ratio graph, scenario 1

For the same scenario, security level is also tested as a network performance parameter. Table 3 shows the obtained values for security and figure 3 represents the plotted graph. It is found that average security level obtained for this scenario is 87.8%.

Table 3 Security level for scenario 1

Rounds	Values of Security level
1	1
2	.998
3	.996
4	.985
5	.953
6	.906
7	.876
8	.867
9	.853
10	.832
11	.815
12	.798
13	.776
14	.765
15	.754

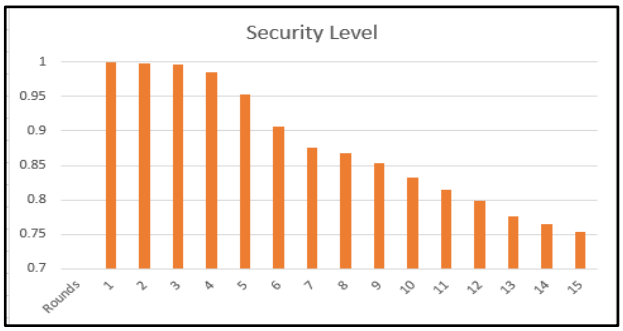

Fig 3 Security level for scenario 1

For the same number of nodes, simulation was run for 50 iterations. 50 nodes with same initial parameters tested for 50 iterations forms scenario 2. Figure 4 represents the energy consumption graph for this scenario.

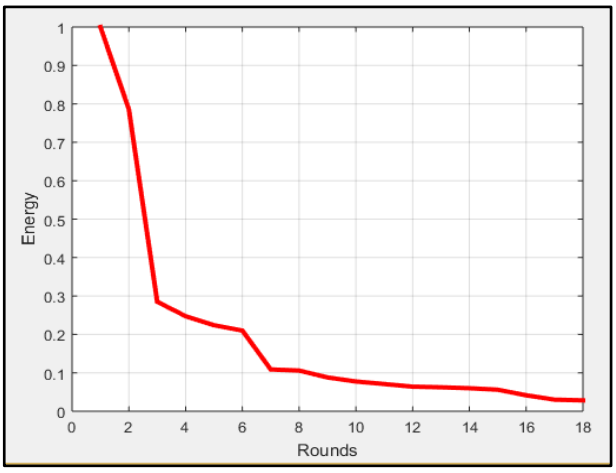

Fig 4 Energy consumption graph for scenario2

The corresponding collected values of packet delivery ratio are shown in table 4.

Table 4 Packet delivery ratio for scenario 2

Rounds	Values of Packet Delivery Ratio
1	1
2	1
3	.999
4	.999
5	.996
6	.993
7	.993
8	.993
9	.983

10	.99
11	.99
12	.988
13	.988
14	.985
15	.982

Based on these values graph is plotted in figure 5. The graph shows that average packet delivery ratio for this scenario is 99.25%.

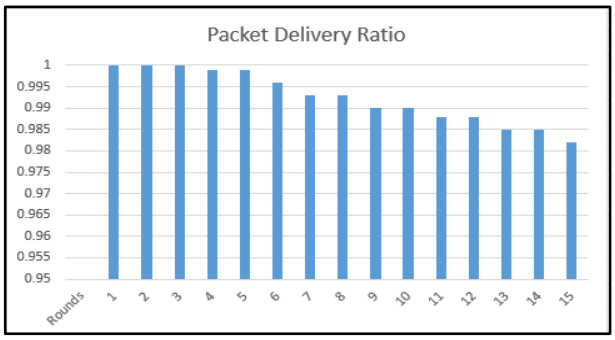

Fig 5 Packet delivery ratio, scenario 2

Similarly, security level values are shown in table 5 and corresponding graph in figure 6. The average value obtained from graph for security is 88.12%.

Table 5 Security level for scenario 2

Rounds	Values of security level
1	1
2	.999
3	.987
4	.978
5	.963
6	.958
7	.921
8	.9
9	.876
10	.843
11	.8
12	.786
13	.754
14	.733
15	.72

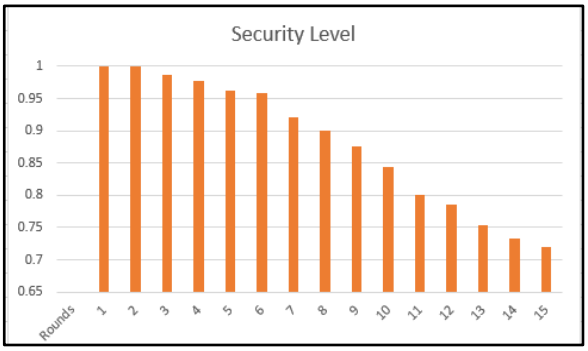

Fig 6 Security level for scenario 2

Next case considered was testing network on 75 nodes for 30 iterations. The initial parameters were kept same as in table 1. This case forms the scenario 3. The energy consumption graph is represented by figure 7.

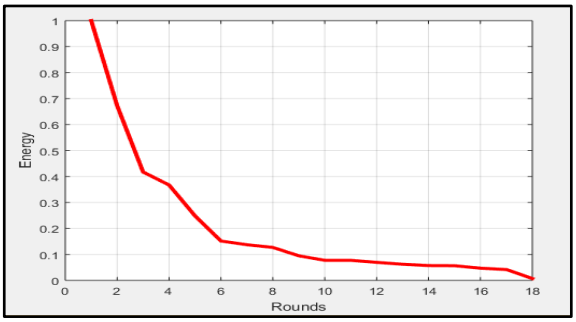

Fig 7 Energy consumption for scenario 3

The packet delivery ratio and security level values were noted for this scenario and are shown in table 6 and table 7 respectively.

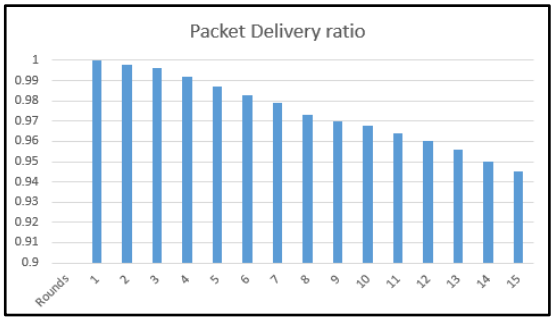

Fig 8 Packet delivery ratio, scenario 3

Table 6 Packet delivery ratio for scenario 3

Rounds	Values of packet delivery ratio
1	1

2	.998
3	.996
4	.992
5	.987
6	.983
7	.979
8	.973
9	.97
10	.968
11	.964
12	.96
13	.956
14	.95
15	.945

The average results obtained for packet delivery ratio is 97.4% and security is 80.8%. The plotted graphs are shown in figure 8 and figure 9 respectively.

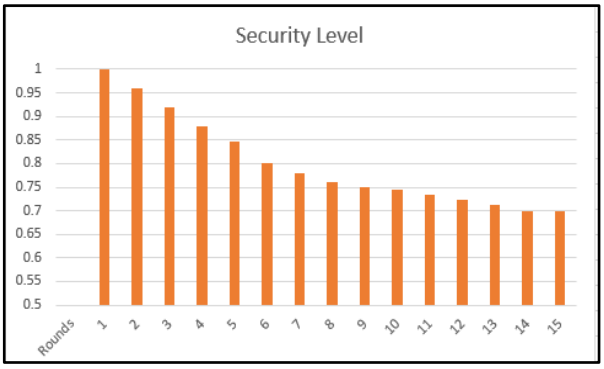

Fig 9 Security level for scenario 3

Table 7 Security level for scenario 3

Rounds	Values of security level
1	1
2	.96
3	.92
4	.88

5	.846
6	.8
7	.78
8	.76
9	.75
10	.745
11	.734
12	.723
13	.712
14	.7
15	.72

Scenario 4: Same network, with 75 nodes and 1 sink node was deployed to test for 50 iterations with initial parameters. The energy consumption graph is shown in figure 10.

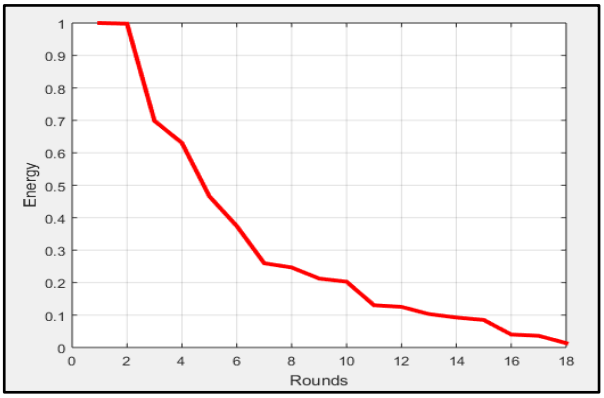

Fig 10 Energy consumption for scenario 4

Packet delivery ratio values and security values obtained for this scenario are listed in table 8 and table 9 respectively.

Table 8 Packet delivery ratio for scenario 4

Rounds	Values of packet delivery ratio
1	.999
2	.998
3	.996

4	.993
5	.987
6	.984
7	.977
8	.972
9	.966
10	.962
11	.958
12	.955
13	.945
14	.941
15	.938

The values are plotted on graph, shown in figure 11 and 12 respectively for both parameters. The average value obtained for packet delivery ratio for scenario 4 is 97.1% and security is 81.6%.

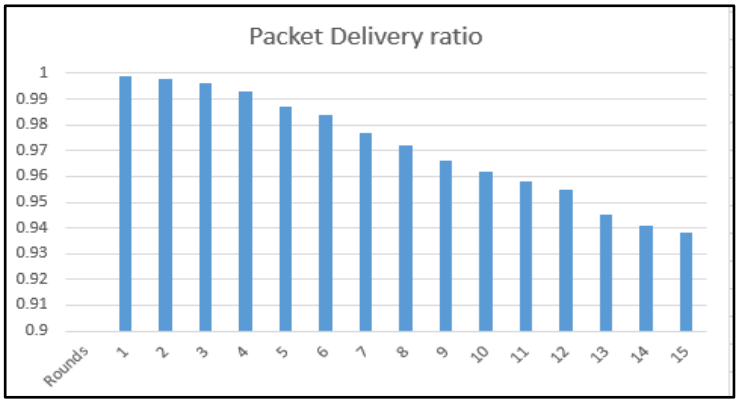

Fig 11 Packet delivery ratio for scenario 4

Table 9 Security level for scenario 4

Rounds	Values of security level
1	1
2	.997
3	.965
4	.942
5	.9

6	.875
7	.834
8	.8
9	.783
10	.765
11	.721
12	.7
13	.68
14	.65
15	.63

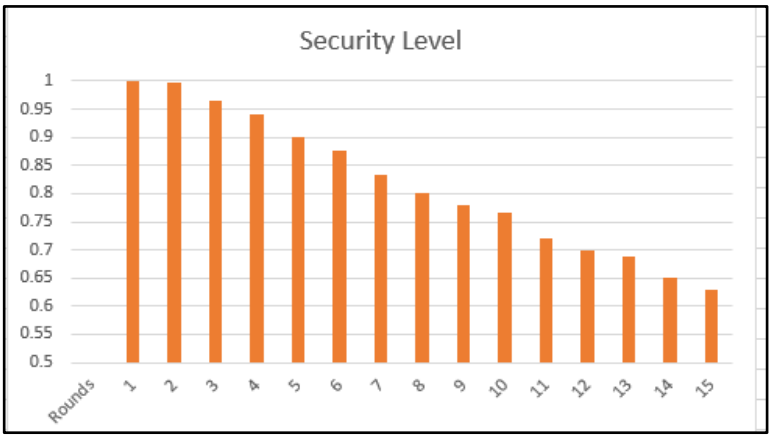

Fig 12 Security level for scenario 4

The graphs and average values obtained for performance parameters shows that with 1J of energy maximum performance is obtained for 50 nodes at 50 iterations that is 99.25% for packet delivery ratio and 88.12% for security. The performance metrics tables are given below for 50 nodes and 75 nodes respectively in table 10 and table 11.

Table 10 Performance parameters for 50 nodes

Number of Nodes = 50		
Number of iterations	Packet Delivery Ratio (%)	Security Level (%)
30	98.6	87.8
50	99.25	88.12

Table 11 Performance parameters for 75 nodes

Number of Nodes = 75

Number of iterations	Packet Delivery Ratio (%)	Security Level (%)
30	97.4	80.2
50	97.1	81.6

When compared with the existing work done for mobile ad hoc networks using trust and mamdani fuzzy logic, better results are obtained for packet delivery ratio. The paper has proposed a trust and fuzzy logic based solution for mobile ad hoc networks. The concept of trust with neuro fuzzy logic is applied in this work. Table 12 depicts the packet delivery ratio when compared.

Table 12 Performance comparison

Packet Delivery Ratio (%)	
Proposed Work	99.25
Existing work for MANETs	99.2

Conclusion and Future Scope

The proposed scheme for wireless sensor networks is an effort to contribute as a solution for ad hoc networks problematic areas. Sensors being running on batteries face energy consumption problems. The benefit of using neuro fuzzy logic eliminated the concept of random selection of cluster head.The proposed algorithm was executed for different number of nodes against different iterations. Better results are obtained in terms of packet delivery ratio when compared with existing work. It is seen from results that the given algorithm could not achieve the security as was expected. This can contribute as a cause of further research to extend this work. Also, inclusion of more parameters to neuro fuzzy will form good set of training data so that system can give more refined results. Optimization techniques can also be applied to further improve the network performance efficiency.

References

[1] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, “Trust management systems for wireless sensor networks: Best practices,” *Comput. Commun.*, vol. 33, no. 9, pp. 1086–1093, 2010.

[2] R. Gupta, D. Sahil Verma, D. Kavita, and A. Ial Yadav, “A Comparative Analysis of Trust Based Applications in Wireless Sensor Networks,” *Int. J. Eng. Technol.*, vol. 7, no. 4.12, pp. 73–77, 2018.

[3] G. V. Crosby, L. Hester, and N. Pissinou, “Location-aware, trust-based

detection and isolation of compromised nodes in wireless sensor networks," *Int. J. Netw. Secur.*, vol. 12, no. 2, pp. 107–117, 2011.

[4] A. P. Markopoulos, S. Georgiopoulos, M. Kinigalakis, and D. E. Manolakos, "Adaptive neuro-fuzzy inference system for end milling," *J. Eng. Sci. Technol.*, vol. 11, no. 9, pp. 1234–1248, 2016.

[5] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Commun. Surv. Tutorials Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

[6] E. K. Eldhose and G. Jisha, "Active Cluster Node Aggregation Scheme in Wireless Sensor Network Using Neural Network," *Procedia Technol.*, vol. 24, pp. 1603–1608, 2016.

[7] O. Boyinbode, H. Le, A. Mbogho, M. Takizawa, and R. Poliah, "A survey on clustering algorithms for wireless sensor networks," *Proc. - 13th Int. Conf. Network-Based Inf. Syst. NBiS 2010*, vol. 30, pp. 358–364, 2010.

[8] H. Xia, Z. Jia, L. Ju, X. Li, and Y. Zhu, "A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules," *Proc. - 2011 IEEE/ACM Int. Conf. Green Comput. Commun. GreenCom 2011*, vol. 2, pp. 124–130, 2011.

[9] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," *IEEE Trans. Netw. Serv. Manag.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.

[10] J.-S. Lee and W.-L. Cheng, "Fuzzy-Logic-Based Clustering Approach for Wireless Sensor Networks Using Energy Predication," *IEEE Sens. J.*, vol. 12, no. 9, pp. 2891–2897, Sep. 2012.

[11] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, 2012.

[12] H. Xia, E. H.-M. Sha, and Z. Jia, "Research of trust model based on fuzzy theory in mobile ad hoc networks," *IET Inf. Secur.*, vol. 8, no. 2, pp. 88–103, 2014.

[13] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 2013–2027, Sep. 2016.

[14] V. Ram Prabha and P. Latha, "Fuzzy Trust Protocol for Malicious Node

Detection in Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol. 94, no. 4, pp. 2549–2559, 2017.

[15] K. P. Rama Prabha and N. Jeyanthi, "A Trust and Fuzzy Cluster Based Dynamic Secure Routing Algorithm for Mobile Ad Hoc Networks," *Wirel. Pers. Commun.*, vol. 98, no. 3, pp. 2959–2974, 2018.

[16] M. Shokouhifar and A. Jalali, "Optimized sugeno fuzzy clustering algorithm for wireless sensor networks," *Eng. Appl. Artif. Intell.*, vol. 60, no. July 2015, pp. 16–25, 2017.

[17] Y. H. Robinson, S. Balaji, and M. Rajaram, "ECBK: Enhanced Cluster Based Key Management Scheme for Achieving Quality of Service," *Circuits Syst.*, vol. 07, no. 08, pp. 2014–2024, 2016.

[18] E. G. Julie, S. Tamilselvi, and Y. H. Robinson, "Performance Analysis of Energy Efficient Virtual Back Bone Path Based Cluster Routing Protocol for WSN," *Wirel. Pers. Commun.*, vol. 91, no. 3, pp. 1171–1189, Dec. 2016.

[19] I. Chlamtac, M. Conti, and J. J. N. Liu, "Mobile ad hoc networking: Imperatives and challenges," Ad Hoc Networks, vol. 1, no. 1, pp. 13–64, 2003.

[20] https://in.mathworks.com/help/fuzzy/neuro-adaptive-learning-and-anfis.html

[21] A. Tajeddine, A. Kayssi, A. Chehab, and H. Artail, "Fuzzy reputation-based trust model," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 345–355, Jan. 2011.