VOL. 12, NO. 13, JULY 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

DESIGN AND ANALYSIS OF CROSS LAYER APPROACH IN THE DETECTION OF BLACKHOLE ATTACKS USING ADAPTIVE NEURO-FUZZY INFERENCE SYSTEM

Vydeki Dharmar[1] and Bhuvaneswaran Raghuvel Subramanian[2]
[1]School of Electronics Engineering, VIT University, Chennai, India
[2]Ramajunan Computing Centre, Anna University, Chennai, India
E-Mail: vydeki.d@vit.ac.in

ABSTRACT

Blackhole attack is considered to be a virulent attack in mobile ad hoc networks (MANETs) that operate on reactive routing protocols. This paper presents an efficient cross layer approach to detect the malicious node that launches the blackhole attack. The proposed scheme uses Adaptive Neuro- Fuzzy Inference System (ANFIS), which combines the benefits of neural networks and fuzzy logic, in the detection process. Experimental results prove that the cross layer approach using ANFIS outperforms the scheme using single layer approach. The proposed scheme produces 100% true detection when Fuzzy C-means (FCM) clustering is used and 95.9% for subtractive clustering. The detection time has also been comparatively reduced.

Keywords: blackhole attack, clustering, cross layer, MANET, Neuro-fuzzy, soft computing.

1. INTRODUCTION

A decade of exponential growth in wireless networks has profoundly impacted our lifestyle, from cellular telephones to wireless Internet access. A wireless network without any fixed infrastructure is referred to as a mobile ad hoc network (MANET), as the wireless nodes are capable of moving freely. It is a mobile, wireless, multi-hop network that operates without the benefit of any existing infrastructure, except for the nodes themselves [1]. Such networks are assumed to be self-forming and self-healing. These unique characteristics allow them to be used in special applications such as the army, emergency/ rescue operations, habitat monitoring etc. Routing in such networks is challenging because typical routing protocols do not operate efficiently in the presence of frequent movements, intermittent connectivity, and network splits/joints. Moreover, the use of wireless links makes these networks very vulnerable to security attacks, ranging from passive eavesdropping to active interfering. Attacks against the network may come from malicious nodes that are not part of the network and are trying to join the network without authorization. Such nodes are typically called outsiders. Networks are protected from malicious outsiders through the use of cryptographic techniques. Such techniques allow nodes to securely verify the identity of other nodes, and can therefore; try to prevent any harm being caused by the malicious outsiders. Attacks also come from nodes that are authorized to be part of the network and are typically called insiders. Insider nodes may launch attacks because they have been compromised by an unauthorized user (e.g. hacker) through some form of remote penetration, or have been physically captured by a malicious user.

Blackhole attack is such an insider attack which aims at degrading the performance of the network. There are mechanisms listed in literature to detect blackhole attacks. This paper proposes the design of a novel cross layer approach in the ANFIS based blackhole detection scheme. The Adaptive Neuro-Fuzzy Inference System combines the benefits of the Fuzzy Inference System (FIS) and neural network paradigms [2]. An ANFIS functions by applying neural learning rules to identify and tune the parameters and structure of an FIS. The proposed scheme also uses a hybrid credit allocation process to improve the detection efficiency of the scheme.

Section 2 presents the related works in the chosen field. The background for the proposed work is discussed in Section 3. The design of credit based hybrid blackhole detection scheme using ANFIS framework with cross layer approach is dealt in detail in Section 4. Section 5 provides the experimental results of the proposed work and its comparative analysis with the single layer approach. Performance analysis of the proposed techniques is discussed on detail in Section 6. Comparison of the proposed cross layer ANFIS scheme with the single layer ANFIS scheme is presented in Section 7. In Section 8, the proposed method is compared with the existing cross layer scheme. Conclusion and future scope of the work are presented in Section 9.

2. RELATED WORKS

Ping Yi, Ting Zhu, Ning Liu, Yue Wu, Jianhua Li adopted a cross layer approach to detect the gray and blackhole nodes in MANETs [3]. A MAC layer parameter, namely, the collision rate has been included in the detection process. Each node operates on a promiscuous mode and computes the forwarding rate of the next-hop node. If it is lesser than a threshold value, the next-hop node is considered a gray/blackhole node, and is avoided in further communication. The MAC layer collision rate is used to compute the threshold dynamically and reduce the false positive. Despite the fact that this scheme was successful in reducing the false alarms, it had produced less accurate detection.

D. Vydeki and R. S. Bhuvaneswaran have developed a single layer blackhole detection scheme using

ANFIS. The design involves the selection of appropriate parameters from network layer and an ANFIS structure trained using a known data set to detect the malicious nodes. A detection accuracy of 96.4% was produce by this approach [4]. The proposed work using cross layer has proven to outperform the existing scheme in detecting the blackhole attack.

Vimal Kumar and Rakesh Kumar [27] have presented a solution for AODV based MANETs infected with blackhole attack. This algorithm makes few changes in the routing protocol and improves the throughput and packet delivery ratio. However, it does not declare the malicious nodes to the network.

3. BLACKHOLE ATTACK

The impact of blackhole attack is high in MANETs operating on reactive routing protocols. In classic reactive routing protocols, such as ad hoc on-demand distance vector (AODV) routing, the malicious node targets the route discovery process to launch the blackhole attack. Vulnerable fields, such as the hop count and sequence number in the route reply (RREP) packets are exploited by the adverse node. As soon as the blackhole node receives a route request (RREQ), it generates a RREP with the least hop count and highest sequence number, without checking its routing table. This RREP is sent to the source in a fast manner, using high transmission power. Moreover, it does not forward the RREQ to the neighbouring nodes, even if it does not have a path to destination. In this way, it makes the source node to select it in the path from the source to the destination. When it has made itself available as part of a communication path, the blackhole node does not forward the data packets to the intended destination, but drops them.

Figure-1 illustrates the blackhole attack.

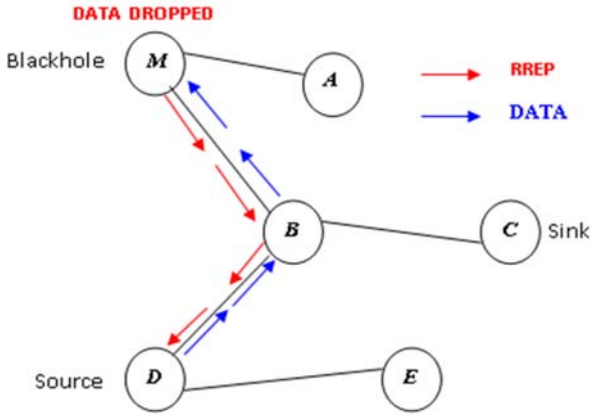

Figure-1. Blackhole attack.

The nodes labelled A to E in the illustration are genuine nodes, and the one labelled M is the adverse node that launches the blackhole attack. The links shown between the wireless nodes A to E and M are logical links. When the source node D tends to communicate with the sink node C, it starts the route discovery process by flooding the RREQ packets. The blackhole node M replies to D with the shortest and fresh route through fake RREP. This makes D to send the packets to M, where they are dropped.

The proposed cross layer design effectively detects the node that launches the blackhole attack in comparatively lesser duration

4. PROPOSED CROSS LAYER SCHEME

This paper presents the design of credit based hybrid blackhole detection scheme using ANFIS on cross layer approach. The specification and anomaly detection techniques are combined to increase the detection accuracy of the proposed scheme. The model specifying the normal behaviour of a node is defined in terms of fields belonging to routing protocol, as in specification method [5] and the threshold value to determine the malicious behaviour is computed automatically as given in anomaly technique. The number of packets dropped (PD), number of route replies sent (SREP) and RREQ forwarding rate (RFR) are the network layer parameters derived from the simulated MANETs. These parameters indicate the behaviour of blakchole node.

A loosely-coupled cross layer approach is adopted by considering a physical layer parameter, residual energy (RE). A credit allocation process is used to improve the detection of blackhole node. The data set consisting of cross layer parameters and credits is conditioned using two types of clustering mechanisms: FCM and subtractive clustering. The conditioned data set is presented as input to a Sugeno type-2 FIS, which is the first step in modelling the ANFIS. The Sugeno FIS is configured with suitable membership functions to represent input and output parameters. The algorithm of the detection scheme is given below.

Credit based cross layer detection algorithm:
//PD: No. of Packets Dropped; SREP: No. of RREPs sent; RFR: Route request forwarding rate; RE: Residual energy; IC: Initial credit; FC: Final Credit
// PDTH, STH, RTH-Threshold of PD, SREP, RE respectively; SD: Standard deviation
Get network layer parameters PD, SREP, RFR and physical layer parameter RE
2. Assign IC = RFR
3. Find threshold value for each parameter as:
PDTH=Mean (PD);
STH=Mean (SREP);
RTH=Mean (RE)
4. At each node compute the individual parameter credit as:
a. If PD<PDTH
IC1=IC+1
Else IC1=0
b. If SREP<STH
IC2=IC+1
Else IC2=0
c. If RE<RTH
IC3=IC+1
Else IC3=0

5. Compute final credit as:

FC=IC1+IC2+IC3

6. Set input parameters as PD, SREP, RFR, RE and FC
7. Use the FCM/Subtractive clustering technique to condition the parameters and generate the input data set to FIS
8. Generate the Sugeno-Type 2 FIS with input/output membership functions and fuzzy rules
9. Evaluate the FIS using the parameters and fuzzy rules and produce the defuzzified output for each node.
10. Compute the SD of the FIS output
11. Detect the blackhole node as:

If node's FIS output< SD, it is a black hole.
Else it is a normal node.

The algorithm starts with data collection from the simulated MANET. The parameter extraction process filters the network layer parameters such as PD, SREP and physical layer parameter RE from the log file of ns2. The metric RFR is computed as the ratio of number of RREQs forwarded by a node to number of RREQs received by that node. The extracted parameters and the derived metric form the initial data set. The initial credit for the algorithm is assigned the value of RFR, which closely reflects the behaviour of a blackhole node. The credit for each parameter is computed by comparing it to its mean value for the given scenario. If the parameter value is less than its mean value, the credit is incremented; else, zero credit is assigned. The final credit of a node is the sum of all parameters' credit.

The credit allocation process leaves the data set for further conditioning through clustering. Clustering partitions a data set into several groups, such that the similarity within each group is larger than that among groups. There are two major clustering algorithms: FCM and subtractive clustering. In FCM, each data point belongs to a cluster to a degree specified by a membership grade. The FCM partitions the input vectors into a number of fuzzy groups and finds a cluster center in each group, such that the dissimilarity is minimized. In subtractive clustering, each data point is considered as the candidate for the cluster center. Consider a collection of data points $\{x_1, x_2, \ldots, x_n\}$. A density measure ($D_i$), that reflects the density of the neighbouring data points, is expressed as the sum of exponential of the negative ratio of square distances between the i^{th} data point and the neighbouring points to half of the square radius, i.e, D_i given in (1),

$$D_i = \sum_{j=1}^{n} \exp\left(- \frac{\left\| x_i - x_j \right\|^2}{\left(r_a / 2 \right)^2} \right) \quad (1)$$

Where, r_a defines the radius of the neighbourhood. A data point will have a high density value if it has many neighbouring data points. After calculating the D_i of each data point, the one with the highest density measure is selected as the cluster center.

The proposed cross layer algorithm has been tested with both types of clustering and the results are discussed in the next section. The clustered data set is fed to the ANFIS for detecting the blackhole nodes.

The Adaptive Neuro-Fuzzy Inference System combines the benefits of the FIS and neural network paradigms into a single capsule. An ANFIS functions by applying neural learning rules to identify and tune the parameters and structure of a Fuzzy Inference System. In the ANFIS structure, the functions used at all the nodes are differentiable; thus the backpropagation algorithm can be used to learn the premise parameters [6]. The training of the network is carried out using a forward pass and a backward pass. The ANFIS based detection scheme starts with defining the structure of the neuro-fuzzy system. A Sugeno type fuzzy inference system is generated, as the first step in modelling the ANFIS, with suitable membership functions. The membership function for the input data set comprising of the clustered data set is modelled as Gaussian. In FIS, the parameters of the input membership functions have fixed values. The neural like connectionist structure and learning to make the FIS's membership function parameters to vary dynamically, results in the integrated system, ANFIS. The structure has to be suitably trained for this purpose.

A training data set is rendered to the ANFIS model to enable the learning process. A part of the input data set serves as the training data. Proper selection of the training data implies faster learning and convergence. Hence, the data set consisting of the protocol-specific features such as the PD, SREP and RFR, from each of the traffic scenarios is used to form the training data set. This is selected in such a way as to reduce the error, and maximize the performance of the system. The hybrid learning rule is used to dynamically vary the linear and nonlinear parameters of the ANFIS depending upon the total number of nodes in the network and the input membership functions. The number of training epochs is given as 10, which is a trial and error value. During the training process, the ANFIS model modifies the various linear and nonlinear parameters to reduce the error in every training epoch. At the end of 10 epochs, the error is minimized, which allows the structure to be tested with the other data set.

A trained ANFIS is able to assess the given data set, and indicate the performance of every node, in terms of the defuzzified value in the range of [-2,6]. The defuzzified output value indicates the behaviour of the wireless nodes. Lesser is its value, the more genuine is the node. The detection of blakchole nodes is carried out by defining a reference/ boundary value of the defuzzified values. The boundary value is computed as the standard deviation of the output values of all traffic cases. The nodes that have output values lesser than this, are considered to be blackhole nodes.

5. RESULTS OF CROSS LAYER DETECTION SCHEME USING THE ANFIS

The following plots portray the experimental results of the cross layer design in the hybrid detection scheme using ANFIS with both clustering techniques. The X-axis displays the respective node id and the Y-axis gives

the output of the proposed scheme in the range (-3,9). Whenever the node has an output value lesser than the boundary value, it is declared as blackhole node. The nodes having output value well above the boundary line are treated as benign nodes.

Figure-2 depicts the result for the network with 15 nodes having two blackhole nodes (13,14), and when the communication occurs between more numbers of nodes. The ANFIS model that produced the output displayed in Figure-2 uses subtractive clustering. It is clear from this figure that the nodes 13 and 14 are correctly decided as blackhole nodes by the proposed scheme. A closer look on Figure-2 reveals that one benign node with id 1 is identified as malignant node, leading to false positive. Hence, for the scenario indicated by blue coloured line, the scheme is producing 100% true positive rate and 7% false positive rate.

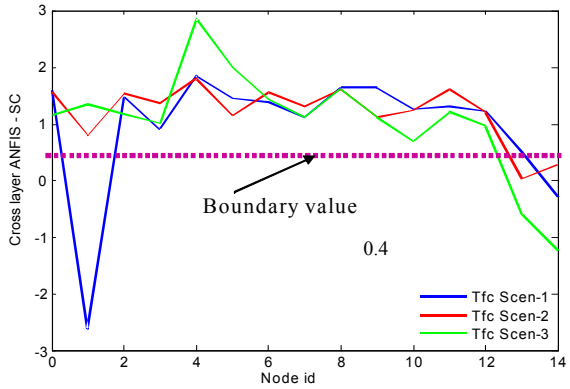

Figure-2. ANFIS cross layer detection scheme with subtractive clustering for 15-node MANET.

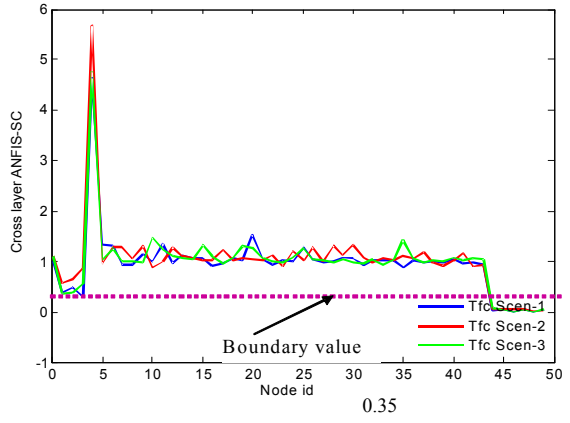

Figure-3. ANFIS cross layer detection scheme with subtractive clustering for 50-node MANET.

The output of the proposed cross layer detection scheme using ANFIS with subtractive clustering for 50-node MANET with 6 blackhole nodes (44 to 49) and low traffic is shown in Figure-3. It is noted from this figure that the malicious nodes are rightly identified by the system for all traffic cases without any false alarms.

The performance of the proposed cross layer scheme using ANFIS with FCM clustering is illustrated in the following figures. Similar to any other cross layer system, this design also improves the detection efficiency of the single layer detection scheme using neuro-fuzzy method with FCM clustering. Figure-4 depicts the detection output of the cross layer scheme using ANFIS for a 25-node MANET with 5 blackhole nodes (20 to 24) and medium traffic. This figure clearly shows that the output values of the nodes 2,20,21,22,23 and 24 are lesser than the boundary value for all cases of communication. Out of the 6 nodes that have been declared as blackhole nodes, the node 2 is a genuine node, which is improperly detected as a malicious node. Other five nodes 20 to 24 are rightly identified. This proves that the cross layer scheme is capable of detecting the malignant nodes very efficiently with few false alarms.

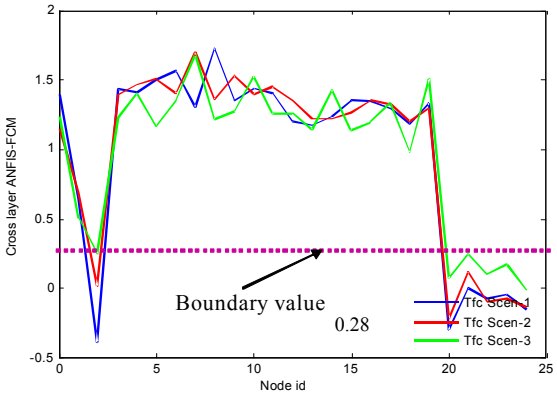

Figure-4. ANFIS cross layer detection scheme with FCM clustering for 25-node MANET.

This inference is supported by Figure-5 that displays the result of this scheme for a 50-node MANET with 6 blackhole nodes (44 to 49) and low traffic.

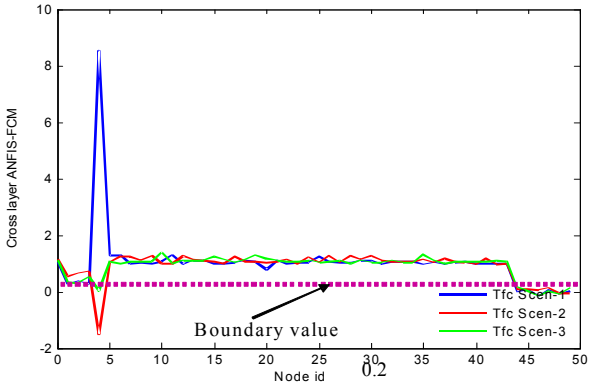

Figure-5. Result of ANFIS cross layer detection scheme with FCM clustering for 50-node MANET.

It can be seen from Figure-5 that except for communication case-3, which generates a false alarm for node with id 4, the proposed scheme is able to detect all the adverse nodes perfectly. Thus, the hybrid cross layer detection scheme using ANFIS with FCM clustering performs better than its single layer counterpart.

6. PERFORMANCE ANALYSIS

The experimental studies show that the cross layer design in the implementation of detection scheme using ANFIS performs better than that of the single layer scheme, except for very few cases. Table I elucidates theperformance of this scheme in terms of the following measures:

a) True Positive Rate (TPR) - is the measure of the number of black hole nodes correctly identified

b) False Positive Rate (FPR) - is the measure of the number of normal nodes identified as adversary nodes, and

c) False Negative Rate (FNR) - indicates the number of blackhole nodes being detected as normal nodes

The computation of these performance parameters is carried out, using Equations (2), (3) and (4).

$$TPR = \frac{TP}{TP + FN} \quad (2)$$

$$FPR = \frac{FP}{n} \quad (3)$$

$$FNR = \frac{FN}{TP + FN} \quad (4)$$

where,

TP: number of true positives
FN: number of false negatives
FP: number of false positives, and
'n': total number of nodes in the network (size of network).

Table-1. Performance analysis of cross layer detection scheme using the ANFIS.

Network size	No. of blackhole nodes	Traffic intensity	TPR (SC) (%)	TPR (FCM) (%)	FNR (SC) (%)	FNR(FCM) (%)	FPR (SC) (%)	FPR (FCM) (%)
15	1	Low	100	100	0.00	0.00	2.33	2.33
		Med	100	100	0.00	0.00	7.00	2.33
		High	100	100	0.00	0.00	2.33	2.33
15	2	Low	83.33	100	16.67	0.00	4.67	2.33
		Med	83.33	100	16.67	0.00	4.67	4.67
		High	100	100	0.00	0.00	2.33	2.33
15	3	Low	89.00	100	11.00	0.00	2.33	4.67
		Med	55.67	100	44.33	0.00	2.33	4.67
		High	78.00	100	22.00	0.00	2.33	2.33
25	1	Low	100	100	0.00	0.00	1.33	0.00
		Med	100	100	0.00	0.00	2.67	0.00
		High	100	100	0.00	0.00	4.00	0.00
25	2	Low	100	100	0.00	0.00	5.33	0.00
		Med	100	100	0.00	0.00	1.33	0.00
		High	100	100	0.00	0.00	6.67	0.00
25	5	Low	100	100	0.00	0.00	4.00	4.67
		Med	100	100	0.00	0.00	2.67	7.00
		High	100	100	0.00	0.00	4.00	4.67
50	3	Low	100	100	0.00	0.00	2.00	9.00
		Med	100	100	0.00	0.00	2.00	6.67
		High	100	100	0.00	0.00	2.67	4.67
50	6	Low	100	100	0.00	0.00	0.00	11.33
		Med	100	100	0.00	0.00	0.00	11.33
		High	100	100	0.00	0.00	0.00	17.67
50	10	Low	100	100	0.00	0.00	0.67	2.33
		Med	100	100	0.00	0.00	0.00	4.67
		High	100	100	0.00	0.00	0.00	4.67

It is very clear from Table-1 that the cross layer hybrid detection scheme using ANFIS structure with FCM clustering produces 100% accurate detection for all network scenarios and blackhole densities. The scheme using subtractive clustering offers good detection, except for few cases. The cross layer scheme has effectively reduced the false alarms compared to the single layer approach.

The detection time of this scheme is presented in Table-2. When the traffic is less in the network, the schemes using both the clustering techniques take larger time to detect the blackhole nodes. This is similar to the performance of the single layer schemes. The information available on a smaller network is lesser and hence the structure of the ANFIS requires time to learn the underlying relationship between the inputs and output. However, the speed of detection with respect to the network size varies linearly in the cross layer schemes, whereas, it showed a non-linear pattern in the single layer schemes. Due to the addition of the cross layer parameter, the speed of detection is proportional to the network size. Moreover, it can be inferred from this table that time taken by the scheme with FCM clustering is more compared to the one with subtractive clustering. This clearly indicates the impact of clustering technique in the detection performance. In applications where fast detection with good accuracy is required, the ANFIS scheme with subtractive clustering may be used, whereas, for applications demanding maximum accuracy, the scheme with FCM may be suitable.

Table-2. Detection time of ANFIS based cross layer scheme.

Network size	Traffic intensity	Detection time of cross layer ANFIS (FCM) (in seconds)	Detection time of cross layer ANFIS (SC) (in seconds)
15	Low	0.130203	0.051946
	Medium	0.125200	0.056639
	High	0.182485	0.050841
25	Low	0.171740	0.074347
	Medium	0.152883	0.075647
	High	0.155403	0.082449
50	Low	0.205264	0.097834
	Medium	0.189885	0.097446
	High	0.199128	0.110289

7. COMPARATIVE ANALYSIS WITH THE ANFIS SINGLE LAYER SCHEME

The performance of the cross layer detection scheme using ANFIS is compared with its single layer counterpart and the results are plotted in Figure-6 and Figure-7.

The comparison of single and cross layer schemes using ANFIS with subtractive clustering is shown in Figure-6. The three major performance measures; detection accuracy in terms of TPR, false alarm rate in terms of FPR and the speed of detection are presented in the three subplots, respectively. It can be seen from the first subplot of this figure that the TPR of the ANFIS based cross layer scheme with subtractive clustering performs better for medium and large networks, whereas the performance of the single layer scheme is marginally better in small networks.

When considering the false alarm rate of the single and cross layer schemes, which is presented in the subplot-2, it is understood that the cross layer design has reduced the false alarms effectively compared to its single layer counterpart. The detection speed of the cross layer scheme is slightly higher compared to that of the single layer scheme.

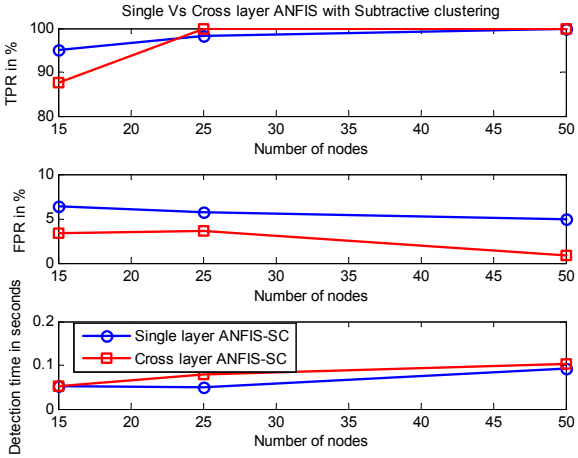

Figure-6. Comparison of single and cross layer ANFIS schemes with subtractive clustering.

The performance comparison of the ANFIS based cross layer detection scheme using FCM clustering with that of the single layer approach is depicted in Figure-7. It can be seen from this figure that the cross layer design produces 100% true detection for all network sizes, as illustrated in the subplot-1 of this figure. Further, the speed of detection is less when the network is small or large, and it is slightly higher than that of the single layer scheme, for medium sized network. However, it generates higher false positives for large networks, as given in the subplot-2. The minor reduction in the performance of the cross layer schemes is due to the effect of clustering techniques.

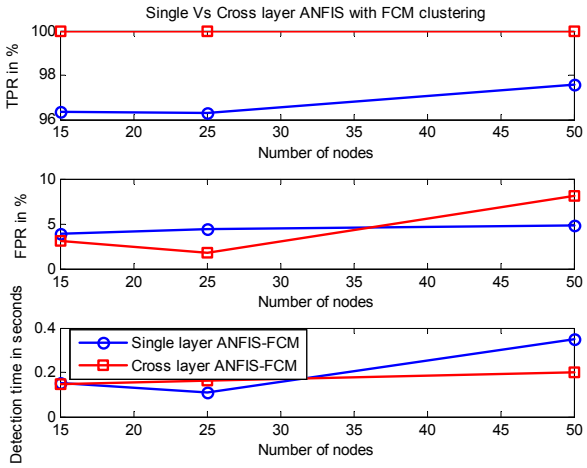

Figure-7. Comparison of single and cross layer ANFIS schemes with FCM clustering.

8. COMPARISON WITH EXISTING SCHEME

The cross layer based detection scheme is compared with the existing scheme proposed by Ping Yi *et al* (2012). The authors had developed a scheme using parameters from the network and MAC layers to detect blackhole attack. It's a path-based scheme in which each node observes the behaviour of the neighbouring node in one-hop distance and maintains a buffer to store its activities such as packet forwarding rate, and MAC layer collision rate. When these values are higher compared to a predefined threshold value, the next-hop node is considered as the blackhole node and avoided in the future communication. This monitoring and detection process, using a dynamically changing threshold value, is carried out periodically in order to ensure secure communication. This scheme has been tested with the user-generated data for 50 nodes, simulation duration of 100s and the performance has been evaluated using detection probability (DP) and false positive probability (FPP), expressed in percentage is presented in Table-3. It can be inferred from this table that, the proposed cross layer detection schemes using fuzzy and neuro-fuzzy approaches with both type of clustering perform better than the existing scheme. The detection probability of the existing scheme is comparatively lesser and it produces more false alarm.

Table-3. Performance comparisons of proposed cross layer scheme with existing scheme.

Performance measure	Existing scheme	Proposed schemes			
		Cross layer FIS		Cross layer ANFIS	
		FCM	SC	FCM	SC
Detection probability	0.693	0.945	0.982	1.00	0.959
False positive probability	0.136	0.041	0.050	0.043	0.026

9. CONCLUSIONS

A cross layer detection scheme to detect the virulent blackhole attack in mobile ad-hoc network was discussed in this paper. The design was tested with adaptive neuro-fuzzy inference system and its performance was evaluated with various metrics. Its performance is also compared with a single-layer scheme and from the results it's proven that the cross layer scheme performs better in terms of true positive rate, false positive rate and detection speed. Both the single and cross layer schemes were tested with two types of clustering: subtractive and fuzzy c-means. In future, more parameters from other layers can be included to reduce the false alarms and to improve the speed. Moreover, the proposed algorithm may be modified appropriately to detect other routing layer attacks such as gray hole and worm hole attacks.

REFERENCES

[1] Charles E Perkins. 2001. Ad hoc networking. Addison Wesley.

[2] Jang J.S.R., Sun C.T. and Mizutani E. 2010.Neuro-fuzzy and soft computing - a computational approach to learning and machine intelligence. PHI.

[3] Ping Yi, Ting Zhu, Ning Liu, Yue Wu, Jianhua Li. 2012. Cross-layer detection for blackhole attack in wireless Network. Journal of Computational Information Systems. 8(10): 4101-4109.

[4] Vydeki D. and Bhuvaneswaran R.S. 2012. Design of wireless IDS using adaptive neuro-fuzzy inference system. European Journal of Scientific Research. 90(1): 149-156.

[5] FarooqAnjum. 2007. Security for wireless ad hoc networks. John Wiley and Sons.

[6] Yue Wu, Biaobiao Zhang, Jiabin Lu and Du, K. L. 2011. Fuzzy logic and neuro-fuzzy systems: a systematic introduction. International Journal of Artificial Intelligence and Expert Systems (IJAE). 2(2): 47-80.

[7] AikateriniMitrokotsa, ManolisTsagkaris and Christos Douligeris. 2008. Intrusion detection in mobile ad hoc networks using classification algorithms. 7th IFIP Annual Mediterranean Ad Hoc Networking Workshop, MedHocNet.

[8] Amir AbolfazlSuratgar, Mohammad BagherTavakoli and Abbas Hoseinabadi. 2008. Modified Levenberg-Marquardt method for neural networks training. World Academy of Science, Engineering and Technology. 6: 46-48.

[9] Amitabh Mishra, KetanNadkarni and AnimeshPatcha. 2004. Intrusion detection in wireless ad hoc networks. IEEE Wireless Communications. 11(1): 48-60.

[10] Anil Kumar, K.S and Nandamohan,V. 2008. Novel anomaly intrusion detection using neuro-fuzzy inference system. International Journal of Computer Science and Network Security. 8(8).

[11] Chin-Yang Tseng, PoornimaBalasubramanyam and Calvin Ko. 2003. A specification-based intrusion detection system for AODV. Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks.

[12] Huang Y.A. and Lee W. 2004. Attack analysis and detection for ad hoc routing protocols. 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera. pp. 125-145.

[13] Joseph, J. F. C., Das, A., Seet, B.C. and Bu Sung Lee. 2007. Cross layer versus single layer approaches for intrusion detection in MANETs. ICON, 15th IEEE International conference on Networks. pp. 194-199.

[14] Kurosawa S., Nakayama H., Kato N., Jamalipour A. andNemoto Y. 2007. Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. International Journal of Network Security. 5(3): 338-346.

[15] Ali AbdulrahmanMahmood, Taha Mohammed Hasan, Dhiyab Salman Ibrahim. 2015. Modified AODV Routing Protocol to Detect the Black Hole Attack in MANET. International Journal of Advanced Research in Computer Science and Software Engineering. 5(7): 173-178.

[16] Ming-Yang Su. 2011. Prevention of selective black hole attacks on mobile attack networks through IDS. Computer Communications, l.34: 107-117.

[17] MonitaWahengbam and NingrinlaMarchang. 2012. Intrusion detection in MANET using fuzzy logic. Proceedings of 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS). pp. 189-192.

[18] Muna Muhammad, Jawhar, T. and Monica Mehrotra. 2010. Design network intrusion detection system using hybrid fuzzy-neural network. International Journal of Computer Science and Security. 4(3): 295-307.

[19] Poojitha G., Naveen Kumar, K. and Jayarami Reddy, P. 2010. Intrusion detection using artificial neural network. Proceedings of IEEE Second International conference on Computing, Communication and Networking Technologies.

[20] Sivaram Murthy C. and Manoj B.S. 2001. Ad hoc wireless networks, protocols and architecture.Pearson Education.

[21] Stamouli I., Argyroudis P.G. and Tewari H. 2005. Real-time intrusion detection for ad hoc Networks. Sixth IEEE Intl Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05). pp. 374-380.

[22] Nitesh A. Funde, P. R. Pardhi. 2103. Detection and Prevention Techniques to Black &GrayHole Attacks In MANET: A Survey. International Journal of Advanced Research in Computer and Communication Engineering. 2(10): 4132-4136.

[23] Carlos Gershenson. 2011. Artificial neural networks for beginners. arxiv.org/pdf/cs/0308031.

[24] VineetSrivastava and MehulMotani. 2005. Cross-layer design: A survey and the road ahead. IEEE Communications Magazine. pp. 112-119.

[25] V. ThiruppathyKesavan and S. Radhakrishnan. 2012. Multiple Secret Keys based Security for Wireless Sensor Networks. International Journal of Communication Networks and Information Security. 4(1).

[26] Vimal Kumar and Rakesh Kumar. 2015. An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network. Procedia Computer Science. 48(2015):472-479.