Journal of Computer Science, 9 (4): 521-525, 2013
ISSN 1549-3636

doi:10.3844/jcssp.2013.521.525 Published Online 9 (4) 2013 (http://www.thescipub.com/jcs.toc)

EFFECT OF CLUSTERING IN DESIGNING A FUZZY BASED HYBRID INTRUSION DETECTION SYSTEM FOR MOBILE AD HOC NETWORKS

[1]Vydeki, D. and [2]R.S. Bhuvaneswaran

[1]Department of Electronics and Communication Engineering, Easwari Engineering College, Chennai, India
[2]Ramanujan Computing Centre, College of Engineering Guindy, Anna University, Chennai, India

Received 2012-08-10, Revised 2012-08-12; Accepted 2012-05-14

ABSTRACT

Intrusion Detection System (IDS) provides additional security for the most vulnerable Mobile Adhoc Networks (MANET). Use of Fuzzy Inference System (FIS) in the design of IDS is proven to be efficient in detecting routing attacks in MANETs. Clustering is a vital means in the detection process of FIS based hybrid IDS. This study describes the design of such a system to detect black hole attack in MANET that uses Adhoc On-Demand Distance Vector (AODV) routing protocol. It analyses the effect of two clustering algorithms and also prescribes the suitable clustering algorithm for the above-mentioned IDS. MANETs with various traffic scenarios were simulated and the data set required for the IDS is extracted. A hybrid IDS is designed using Sugeno type-2 FIS to detect black hole attack. From the experimental results, it is derived that the subtractive clustering algorithm produces 97% efficient detection while FCM offers 91%. It has been found that the subtractive clustering algorithm is more fit and efficient than the Fuzzy C-Means clustering (FCM) for the FIS based detection system.

Keywords: IDS, Routing Attack, Subtractive Clustering, FCM

1. INTRODUCTION

Securing a MANET is a challenging and intricate due to lack of infrastructure, vulnerable medium, mobile nodes and resource constraints. Moreover, choice of suitable routing protocol is the key factor in determining the proper operation of any MANET. AODV is a reactive routing protocol (Perkins, 2008), which establishes paths on request from the source. It follows a Route Discovery Process (RDP) that involves the transmission of Route Request (RREQ) packet from the source node to all the neighbouring nodes. Any intermediate node or the destination node itself generates a Router Reply (RREP) packet, indicating the path to destination and sends back to the source. The hop count and sequence number are used to select the shortest and fresh path when the source receives multiple RREPs. However, due to the inherent nature of MANET and some vulnerability in AODV, the RDP is prone to various routing attacks. Many authentication and security protocols have been developed for providing secure routes to such networks. An IDS (Anjum and Mouchtaris, 2007) is a second line of defence in MANETs to mitigate security attacks. Based on how it is implemented, IDS can be classified into three types: signature detection, anomaly detection and specification based detection. Signature detection aims at identifying the known attacks. Anomaly detection defines the normal behavior of any node and if a node's behavior deviates from that of the normal, it is detected as malicious node. Specification based approach defines the normal behavior in terms of protocol parameters. Several approaches are followed to detect routing attacks using any or combination of the mentioned techniques. Clustering the

Corresponding Author: Vydeki, D., Department of Electronics and Communication Engineering, Easwari Engineering College, Chennai, India

data set is the most important process in developing fuzzy-based IDS. This study aims at analyzing the effect of two fundamental clustering algorithms, namely, subtractive clustering and FCM, in the design of a FIS based hybrid IDS, which combines specification and anomaly based approaches. The proper selection of clustering algorithm is critical to improve the detection rate of such a system to detect the routing attack; especially black hole attack in an AODV based MANET.

2. MATERIALS AND METHODS

2.1. Black Hole Attack in AODV

MANET is a collection of wireless and mobile nodes operating collaboratively to communicate with each other (Murthy and Manoj, 2004). The routing protocol establishes the route from source to destination for successful communication. The adversaries tend to exhibit a compromised behavior by tampering the RREP or RREQ packets used in the RDP of AODV routing protocol. One such routing attack is the black hole attack, in which, the adversary node behaves in the following way:

- Does not forward the RREP to the neighbouring nodes, even when it does not have the path information requested in the received RREQ
- It generates an RREP by making the hop count value to be equal to one, so that the source node may select the adversary node in the path to destination
- Also it modifies the sequence number to be of high value in order to project the false route as the fresh route

These actions will make the malicious node to be selected by the source node for the communication between it and the destination. Upon receiving the data packets from source node, the attacker simply drops it and does not forward in the right direction. This attack is difficult to be handled by authentication protocols as the attack is performed after authentication process is over.

2.2. IDS

An intrusion detection system is capable of detecting such routing attack, when the sufficient data set is provided to it. A hybrid IDS has been developed as represented in **Fig. 1**.

The details of the proposed system are as below: MANETs are simulated in ns2 with varying number of nodes (15, 25 and 50) and traffic intensity (no. of simultaneous communications).

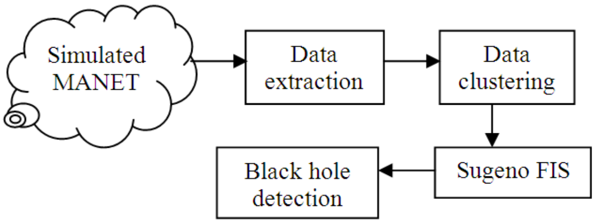

Fig. 1. FIS based IDS

The black hole nodes are simulated in appropriate positions by making suitable modifications listed previously. The density of black hole nodes is also varied from 1% to 5% of the total nodes. The nodes move with a maximum velocity of 200 m sec^{-1} in a 1000×1000 sq.m simulated geographic area. Communication between a pair of nodes use Constant Bit Rate (CBR) type of application and the number of simultaneous communications is varied from low to high, in order to verify the operation of the proposed IDS in various traffic cases. Two-ray ground model is used to approximate the channel behaviour. Single path AODV establishes the path from the different sources to various destinations. The simulation scenarios of MANETs are carried out in the network simulator ns2.

The parameters necessary for the specification-based IDS are extracted from the simulated networks' log file. To define the normal behaviour in terms of the routing protocol, anomaly approach is followed, in which the network is run for several traffic cases.

The threshold for each protocol-specific parameter is defined manually (Tseng *et al*., 2003) in specification-based technique, whereas it is computed from the data set in the anomaly-based approach. The proposed hybrid IDS combines these two mechanisms and the threshold values for each AODV-specific parameter are computed as the average of each nodes value from the simulated networks. Following parameters are used for the detection purpose: Number of Packets Dropped (PD), number of RREPs sent back to the source node (SREP), RREQ Forwarding Rate (RFR) which is computed as a ratio of number of RREQs forwarded to the number of RREQs received. A credit allocation scheme allots an initial credit equal to the RFR to every node and the credits are incremented if the node's parameter value is less than the threshold value. It is decremented otherwise and the final credit is the sum of all individual parameter credits. These parameters and the credits form the data set for the FIS based hybrid IDS.

2.3. Clustering Algorithms

Clustering partitions (Jang *et al*., 1997) a data set into several groups such that the similarity within each group is larger than that among groups. Proper selection of clustering algorithm improves the detection efficiency in the fuzzy-based IDS. The proposed system considers two major clustering algorithms: FCM and subtractive clustering. In FCM, each data point belongs to a cluster to degree specified by a membership grade. FCM partitions the input vectors into 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 cluster center. Consider a collection of data points $\{x_1, x_2, …., x_n\}$. A density measure (D_i) that reflects the density of neighbouring data points is defined as given in Equation 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 first cluster center. If D_{c1} is the density measure of the selected data point x_{c1}, the density measure of each data point x_i is revised by the formula given in Equation 2:

$$D_i = D_i - D_{c1} \exp\left(\frac{\left\| x_i - x_{c1} \right\|^2}{\left(r_b / 2 \right)^2} \right) \quad (2)$$

where, r_b is a positive constant.

The choice of proper clustering algorithm has a greater impact in the detection process of a fuzzy based hybrid IDS in detecting the black hole attack. The system is tested with both the FCM and subtractive clustering algorithms and the results are discussed in the next session. After clustering the input parameters, a Sugeno FIS is generated with Gaussian function as the membership function for the input and output. Membership function maps each point in the input data set to a membership value that defines the degree of membership. With the clustered input and membership functions, the 'genfis' function in Matlab generates a FIS. The output of the FIS is an indication about the FIS is computed and set as threshold. Each node's FIS output is compared with this threshold and the detection of black hole is carried out as follows:

- If the FIS output of each node is lesser than the overall threshold value, it is considered as a normal and genuine node
- If it is greater, the node is detected as a black hole node

3. RESULTS

The following figures illustrate the output generated by FIS based hybrid IDS. In the following plots, X-axis represents the number of nodes, which is also the node id. Y-axis represents the FIS output, in an approximate range [-0.5, 2]. More the output value more is the genuineness of the node. Hence, nodes with lesser output value represent the black hole node.

4. DISCUSSION

The efficiency of any IDS may be defined in terms of True Positive Rate (TPR), which indicates the number of correctly identified black hole nodes, False Positive Rate (FPR), which is the measure of genuine nodes being incorrectly identified as black holes and True Negative Rate (TNR), which gives the number of black hole nodes not identified by the system.

Figure 2 illustrates the comparison of FIS based hybrid IDS with subtractive clustering as well as FCM for a network of 15 nodes. In the simulated network, node id 14 is simulated as black hole node. As mentioned earlier, the nodes with lesser value are identified as black hole nodes. It is evident from **Fig. 2** that the two clustering algorithms detect node with id 14 as black hole node, which produces 100% TPR. However, FCM detects node with id 1 as a black hole, producing a false positive. Subtractive clustering algorithm does not give any false alarm in the given case.

From **Fig. 3**, it is understood that FCM detects nodes 1,2 and 24 as black hole nodes, among which only node 24 is a black hole node. Output of subtractive clustering yields nodes 1 and 24 as malicious nodes, thus reducing the number of false positives.

Similarly, it is clear from **Fig. 4** that the subtractive clustering produces more accurate detection than that done by the FCM.

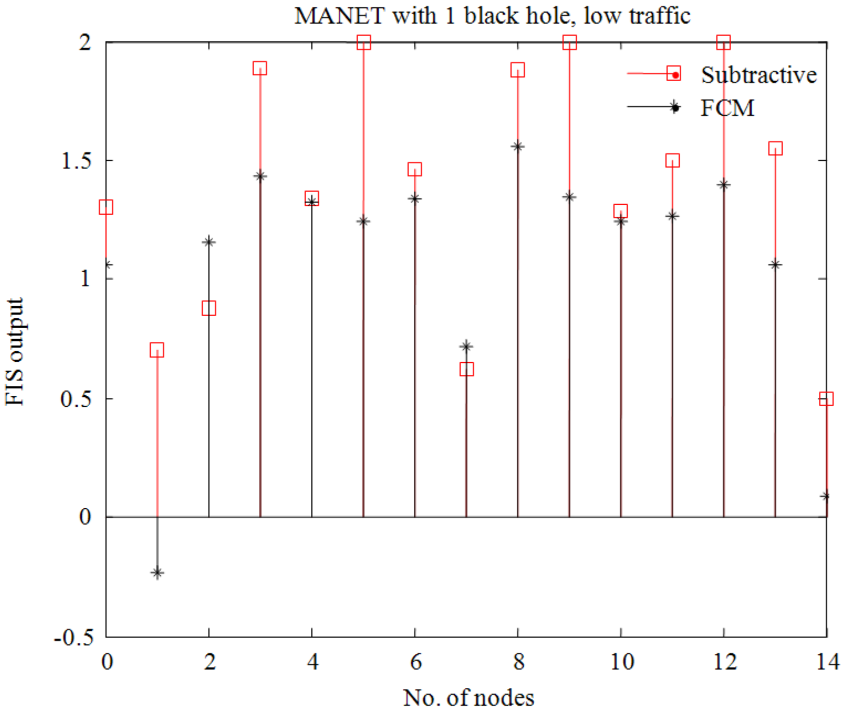

Fig. 2. Output comparison of FIS based hybrid IDS with Subtractive and FCM Clustering for a 15-node network

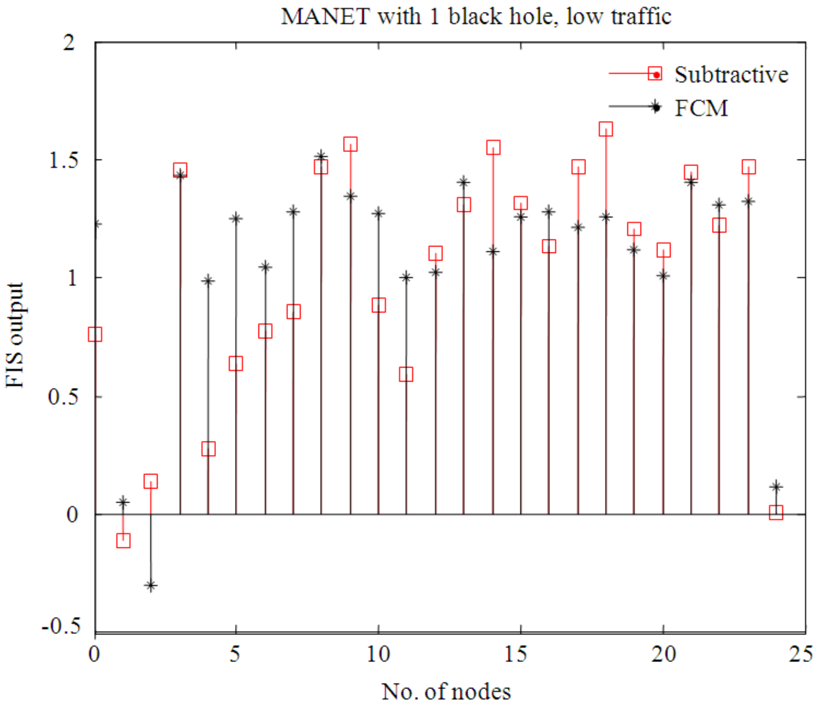

Fig. 3. Output comparison of FIS based hybrid IDS with Subtractive and FCM Clustering for a 25-node network

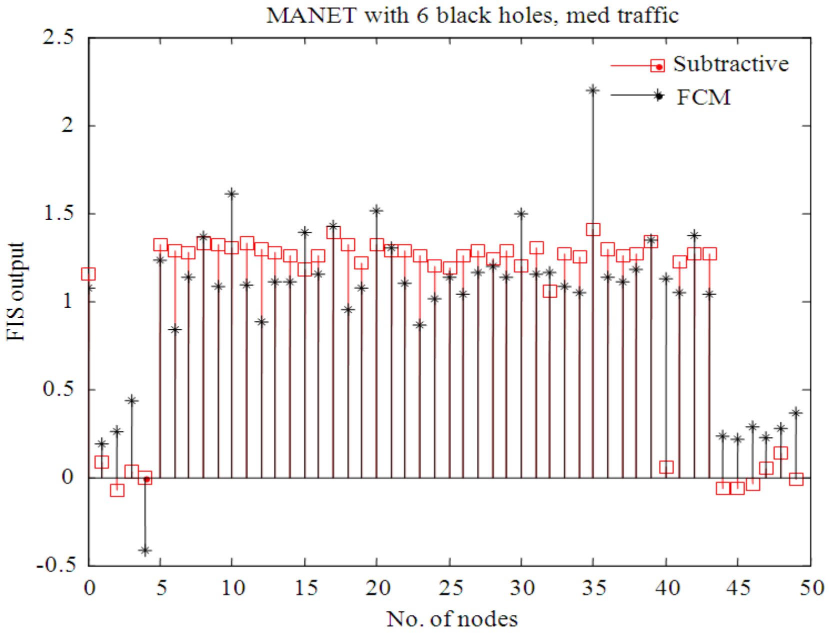

Fig. 4. Output comparison of FIS based hybrid IDS with Subtractive and FCM Clustering for a 50-node network

Table 1. Comparison of FCM and subtractive clustering

Network Size/ clustering	TPR	FNR	FPR
15-nodes/FCM	84.55556	15.444440	7.222222
15-nodes/Subtractive	97.55556	2.444444	9.555556
25-nodes/FCM	98.14815	1.851852	11.222220
25-nodes/Subtractive	100.00000	11.111110	13.555560
50-nodes/FCM	76.03704	23.962960	13.962960
50-nodes/Subtractive	93.81481	21.000000	23.407410

The plots depicted in the previous section illustrates only sample cases for each of the 15, 25 and 50 node networks. Similar experimentation reveals that subtractive clustering improves the performance of the FIS based hybrid IDS than the FCM. **Table 1** gives the comparison between the two systems using FCM and subtractive clustering. It clearly shows that the subtractive clustering results in improved TPR. Except for the 25-node network, subtractive clustering reduces the false negatives, indicated by FNR.

5. CONCLUSION

In this study, a performance analysis is carried out to evaluate the suitability of proper clustering algorithm in the design of hybrid IDS based on fuzzy logic. The two fundamental clustering algorithms are considered for the purpose: FCM and subtractive clustering. The data set required to design the IDS is derived from the simulated network. Upon execution of the fuzzy based IDS using both the algorithms, it is concluded that the subtractive clustering performs better in improving her research may be extended to reduce the FPR by including additional AODV specific parameters.

6. REFERENCES

Anjum, F. and P. Mouchtaris, 2007. Security for Wireless Ad hoc Networks. 1st Edn., John Wiley and Sons, Hoboken, N.J., ISBN-10: 0471756881, pp: 247.

Jang, J.S.R., C.T. Sun and E. Mizutani, 1997. Neuro-Fuzzy and Soft Computing: A Computational Approach to Learning and Machine Intelligence. 1st Edn., Prentice Hall, NJ., ISBN-10: 0132610663, pp: 614.

Murthy, C.S.R. and B.S. Manoj, 2004. Ad Hoc Wireless Networks: Architectures And Protocols. 1st Edn., Pearson Education, ISBN-10: 8131706885, pp: 878.

Perkins, C.E., 2008. Ad Hoc Networking. 1st Edn., Addison-Wesley, Boston, ISBN: 10-0201309769, pp: 384.

Tseng, C.Y., P. Balasubramanyam, C. Ko, R. Limprasittipor and J. Rowe *et al*., 2003. A Specification-based Intrusion detection system for AODV. Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, Oct. 27-30, ACM Press, Washington, DC, USA., pp: 125-134. DOI: 10.1145/986858.986876