Cluster Head Based Intrusion Detection System for Black Hole Attacks in Wireless Ad Hoc Networks using 2 Level Fuzzy Logic System

Christeena Joseph[1], P.C.Kishoreraja[2], Radhika Baskar[3]
{christeena003@gmail.com[1], pckishoreraja@gmail.com[2], radhikabaskr@gmail.com[3]}

Department of Electronics & Communication Engineering,SRM Institute of Science and Technology, Ramapuram Campus,Chennai[1],Department of Electronics Communication Engineering,SRM University, Delhi-NCR, Sonepat, Haryana[2],Department of Electronics & Communication Engineering,Saveetha School of Engineering, Saveetha Institute of Medical & Technical Sciences[3]

Abstract. Ad hoc networks are autonomous and infrastructure-less wireless systems where nodes act as routers and hosts. Security is the primary issue for the functionality of these networks. Security for ad hoc networks can be incorporated by prevention and detection mechanisms. This research work focuses on a two-level fuzzy-based intrusion detection system for identifying black hole attacks in ad hoc networks. This method can reduce the complexity of the rule base of the fuzzy inference system. To reduce the complexity of detection, communication overhead and to make the detection scheme energy efficient, further, a cluster-head-based intrusion detection system is designed and implemented. The impact on network performance with no attack, with black hole attack, and with intrusion detection scheme deployed in all nodes and cluster heads are analyzed. The proposed cluster-based 2 level fuzzy logic intrusion detection mechanism was able to achieve the detection rate and accuracy to a maximum of 100%,false alarm rate to 0% and detection delay to in varying attacker scenario.

Keywords: Adhoc Networks, Blackhole attacks, Cluster head, IDS, Fuzzy Logic.

1 Introduction

In ad hoc wireless networks nodes cooperate among themselves to carry out all the functions in the network. Adhoc networks are prone to safety hazards due to the open medium,from malicious nodes inside the network, lack of infrastructure, restricted power supply, dynamic topology, and cooperative algorithms. These attacks range from passive eavesdropping to active Denial of service attacks[12][13].The security solutions for ad hoc networks involve proactive solutions which incorporate measures to prevent host or network-based attacks. Reactive solutions like intrusion detection system is an effective method to monitor identify and isolate these attacks. This paper analyses the impact of the black hole intrusion in the network and the effectiveness of the intrusion detection system in identifying, isolating the black hole attack, and improving the performance of the network[14]. The proposed work focuses on a two-level fuzzy-based intrusion detection system for identifying black hole attacks in ad hoc networks. This method can reduce the complexity of the rule base in the fuzzy inference system. To reduce the complexity in detection, communication overhead, and to make the detection scheme energy efficient, further, a cluster head-based IDS

I3CAC 2021, June 07-08, Chennai, India

DOI 10.4108/eai.7-6-2021.2308789

is implemented. The impact on network performance with no attack, with black hole attack, and with IDS Scheme deployed in all nodes and cluster heads are analyzed for varying number of attacks.

2.Literature Survey

Debdutta and Nabendu Chaki [2] proposed a 2 layered cluster network in which the node with the lowest node id is selected as cluster head. The function of the cluster head at layer 1 is to collect the route information of the nodes. It monitors the false routes generated by a node, detects the intrusion, and alerts the corresponding layer 2 cluster head.The cluster head of the outer layer informs the nodes in the outer cluster about the intruder. This method was able to reduce the processing and communication overhead between the cluster heads at layers 1 and 2.This IDS considered only a single network parameter to detect black holes, though the PDR rate is improved. Barman Roy and Rituparna Chaki [1] present a cluster-based intrusion detection algorithm that detects blackhole attacks in a MANET based on the trustworthiness of the nodes. The network is layered and the cluster head of each layer is responsible for the members of its cluster and communicates with the cluster head of layer 2. The selection of cluster head is based on three parameters battery power, mobility, and trust value of a node in the cluster. The IDS deployed in the cluster heads detects black hole attacks with a destination sequence number. This work analyzed the network performance but failed to analyze detection performance. Monita Wahengbam and Ningrinla Marchang [3] proposed a method for black hole and gray hole attacks using a fuzzy logic system based on 2 threshold values threshold and dest threshold Though the attacks are detected the maximum detection rate is 80%.Deepa Krishnan [6] proposed an IDS scheme with a lightweight, low overhead mounted on programmable mobile agents. The behavior-based approach is modeled with efficient fuzzy logic to significantly reduce the false positives and increase detection rates. Though the method claims to have improved detection rate no experimental results are given in the paper. Ajanta Konar and R.C. Joshi [5] proposed a Self-Organizing Map to isolate unknown patterns and predict their malicious nature from neighboring map units. A small fuzzy model is implemented in every map unit to achieve improved classification. The small fuzzy rule-base corresponding to the selected map unit will be updated if a new attack occurs, thereby reducing the processing overhead. It gives a high detection rate in KDD 99 cup dataset with a very low false-positive rate but failed to show improvement in network performance and classify attack types. Balan et al [4] proposed a robust fuzzy logic technique to detect black hole and gray hole attacks based on packet drop.Though the network performance is analyzed, the method failed to analyze detection performance. Kulbushan et al in [7] discuss IDS based on fuzzy logic to detect black hole attacks on AODV protocol. The fuzzy-based IDS implemented on each node consists of four modules. The fuzzy parameter extraction module extracts the parameters like forwarding packed ratio and average sequence number from the network traffic. This is given to a fuzzy computation module that works on fuzzy rules to compute the fidelity level. The fidelity level is then compared with a threshold value in the fuzzy verification module to check the behavior of the node. If in case a malicious activity is noted alarm module broadcast an alarm packet with the IP address of the black hole node and the system isolates it. The results show improved performance for the parameters false positive alarm, detection rate, packet delivery ratio, average end to end delay, routing overhead as compared to AODV with the black hole. Abhijit Deodhar and Ritesh Gujarathi

[9] in their paper highlight the clustered approach as the single point of failure. This scheme protects from a situation where the cluster head is compromised. A backup cluster which is a replica of the cluster head monitors the cluster head and provides additional security by operating a backup intrusion detection algorithm. Though the load balancing is done, the paper fails to discuss the IDS deployed in cluster heads and the performance improvement. Alka Chaudhary et al [10] developed an anomaly intrusion detection system based on a Sugeno-type fuzzy inference system to detect the packet dropping attack in mobile ad hoc networks with minimal resources. The proposed system was capable to detect the packet dropping attack with a high detection rate and low false alarms at different mobility levels.

3.Blackhole attack & its impact on network performance

3.1 Blackhole attack

A black hole attacks the network layer by claiming that it has a fresh route to the destination and eventually absorbs the packets forwarded to the destination [3]. Figure 1 illustrates the operation of a black hole attack. When source node 1 wants to send the packets to the destination node 3,it initiates the route discovery process by broadcasting the route request RREQ. Nodes 2, 4, and B receive it. The node B which is a black hole intruder immediately forges and sends a Route Reply RREP packet to 1 with the highest destination sequence number and minimum hop counts to the destination. Hence claiming it has the shortest and fresh path to node 3. Node 1 receives the RREP packet from B, assuming it to be the shortest route, starts sending the packets to 3 through B. Malicious node B being a black hole absorbs all the data packets without forwarding them to the destination[10]

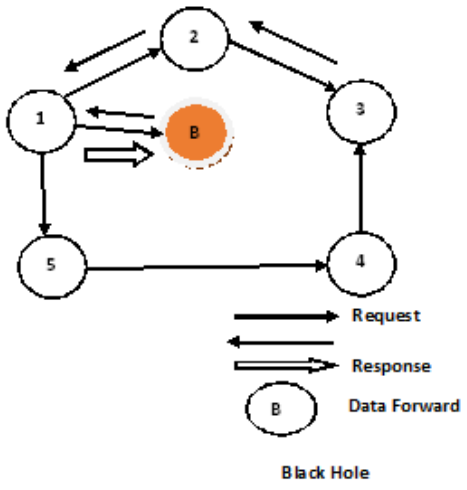

Figure 1 Black Hole Attack

3.2 Simulation of network with no attack & black hole attacks

An analysis is carried out to understand the performance degradation in the network under blackhole attacks. Simulations are done in NS 2 by varying the size of black hole attackers to analyze the effect of the black hole attack on the network parameters. The simulation profile is

given in Table1.All nodes including the black hole nodes are randomly placed. The network performance metrics like Packet Delivery Ratio(PDR), delay, throughput, control overhead, Normalized Routing Head (NORH),and energy are analyzed.

Table 1. Simulation Parameters

Simulation Parameter	Value
Simulation Area	1000*1000 m
Routing Protocol	AODV
Traffic Source	CBR
Number of nodes	150
Size of the data packet	512
Node Placement	Random
Simulation time	200s
Connection time	25s
Speed	0 m/s
Number of flows	3
Number of black hole nodes	1-5

3.3 Performance analysis of the network with varying black hole attacks

The simulated output of black hole attacks in the network is shown in Figure 2.Table 2. shows the performance of the network with no attack and an increasing number of black hole attacks.The performance degradation w.r.t PDR under blackhole attacks is shown in Figure 3.

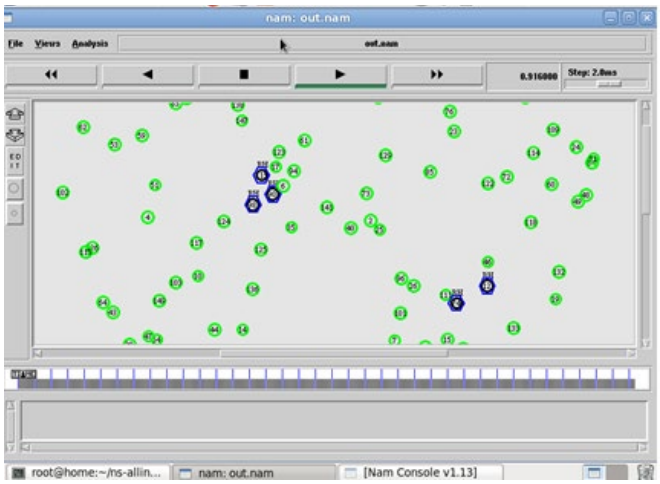

Figure 2. Network with Black Holes

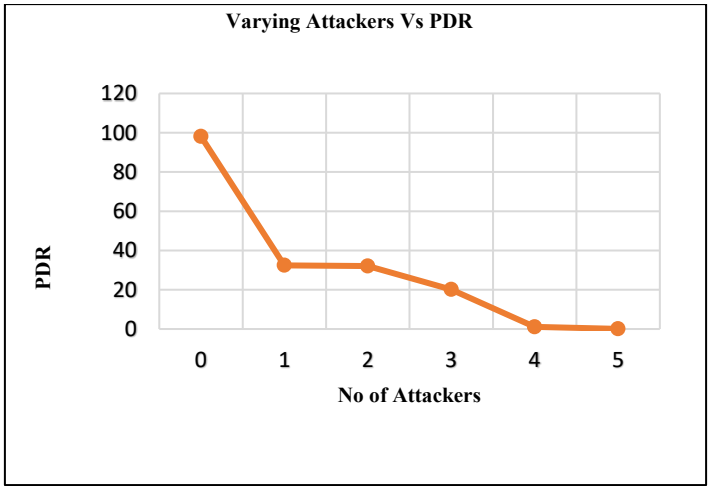

Figure 3.packet delivery ratio withvarying attackers

It is evident from the graphs that with black hole attacks, the Packet Delivery Ratio (PDR) and throughput decreases. With an increasing number of attacks, the PDR and throughput reduce and is almost close to zero with 5 attacks. The black hole attracts and consumes most of the packets routed to the destination and only a few packets manage to reach the destination. Energy consumption reduces with an attack than with no attack, as the black hole does not any perform route discovery and sends the RREP to the source. The black hole attack drops the packets which also results in a decrease of end-to-end delay. The overall delay also varies based on the attacker's position, the time it takes to attack the network and divert the traffic towards itself. Control overhead decreases with an attack than compared to no attack. In case of no attack, more packets are sent to find the route to the destination.With a black-hole attack, fewer control packets are sent in the network as the black hole fakes the RREP and sends it to the source. The NROH also increases with black holes as fewer packets reach the destination.

Table 2. Performance of the network with varying black hole attacks

Network parameter	**No of Black Hole Attacks**					
	0	**1**	**2**	**3**	**4**	**5**
PDR	**98.06**	**32.44**	**32.04**	**20.12**	**1.07**	**0.07**
TpT	**120482**	**32809**	**32000**	**19884**	**1065**	**71.01**
COH	**4149**	**3863**	**3853**	**3897**	**3928**	**3787**
NROH	**3.70**	**8.36**	**8.33**	**15.70**	**261**	**3787**
Delay	**0.37**	**0.018**	**0.045**	**0.0839**	**0.089**	**0.09**
Energy	**6.38**	**3.79**	**4.50**	**4.57**	**3.72**	**3.59**

4.Proposed method

4.1Overview of the proposed intrusion detection system

Fuzzy logic is a computational model that deals with uncertainty and the imprecision of human reasoning with mathematical tools [3].The unique feature to showcase knowledge linguistically makes fuzzy systems the better choice for applications including intrusion detection. This research work focuses on a cluster head-based fuzzy logic intrusion detection system for detecting black hole attacks using the fuzzy logic method[31][32]. As observed from the related work, most of the IDS schemes have taken few parameters in detecting the black hole attacks. In this work, the fuzzy logic system is modified as a two-level fuzzy inference system. Mamdani fuzzy inference model is used in this work. This work incorporates a feature set from the network layer to profile the normal pattern of the ad hoc network. More the features extracted from the network layer to profile the normal pattern, the higher will be the accuracy in detecting the intrusion. The proposed two-level fuzzy inference system reduces the number of rules written into the rule base and the level of computations involved. In this work, the IDS is employed in cluster heads which monitors and collects the network parameters from its members thereby reducing the processing and communication overhead incurred than when all the nodes are deployed with IDS. The nodes in the network monitor the neighbourhood nodes by an overhearing mechanism and store the network parameters in the monitor table maintained in the node with the node id. In the case of cluster-based IDS, the cluster head monitors the behavior of the member nodes in promiscuous mode and stores the parameters in the monitor table. When the IDS is deployed, the feature set is extracted from the monitor table in both cases. The Two-level Fuzzy logic checks for the intrusions. When the Black Hole attacks are detected the current node or the cluster head updates the node id of the black hole in the Blackhole table. The node or the cluster head broadcasts an alarm packet with a black hole id to the members of the cluster or the one-hop neighborhood in case of nodes deployed with IDS. The nodes which receive the alarm messages remove the black hole node entry from the routing table. Figure 4. shows the cluster-based IDS method for black hole detection using fuzzy logic

Algorithm for cluster based IDS using fuzzy logic

Step 1: Network is partitioned into clusters

Step 2: Cluster head is selected by the mechanism of connectivity

Step 3: The cluster head is selected as IDS agent

Step 4: The fuzzy module is incorporated into IDS agent for detection with the following components

- *Fuzzy parameter extraction*
- *Fuzzy computation using if-then rules*
- *Fuzzy output module*

Step 5: Alarm packet generation in case black hole is detected

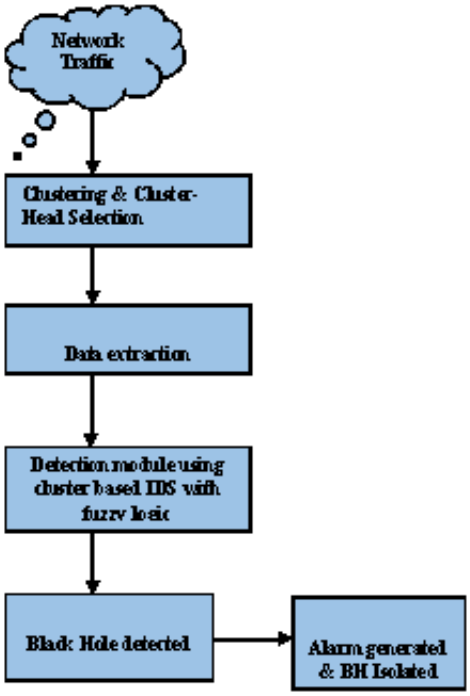

Figure 4. Cluster-based IDS method for black hole detection using fuzzy logic

4.2 Algorithm for clustering and cluster head selection

Cluster-head-based IDS employ cluster heads to monitor and collect the network parameters from its cluster members thereby reducing the processing and communication overhead incurred when the nodes are deployed with IDS.

All Nodes are assigned with the unique Node ID
Network Area Partitioned into N Grid with X_Region, Y_Region
Each Grid is identified by Grid_ID
All the nodes in the Grid send hello message to neighbours
Node_id, Residual_Energy, Nb_count , Grid_ID,Cluster_Head_ID_X_pos, and Y_position
Node Receives Hello Message Update their Neighbour Table
If Nb_count > Highest Nb_Count in Neighbour Table
    Node Selected as Cluster Head
    Set CH=1
    Send CH_Announcement to neighbour in their grid
Node receives CH_Announcement
    If node Grid_ID == CH Grid_ID
        Set CM=1
        Set CH_ID=Sender Node ID
        Send Cluster_Join Message to CH_ID
Node receives Cluster_Join Message
    Update CM in Member Table

4.3Two level fuzzy inference system for black hole detection

In this work, a total of 8 features is extracted from the network. The proposed two-level fuzzy inference system reduces the number of rules written into the rule base and the level of computations involved. Each feature is given five linguistic values such as low, moderate, normal, high, and very high. The membership function of each linguistic variable is given by dividing each attribute into triangular fuzzy sets.

Many *"if-then rules"* to be created in the rule base is $N=x^n$ where x is the number of linguistic variables and n is the number of attributes selected. Belarbiet al.[11][18]. The total number of fuzzy if-then rules to be written into the fuzzy rule base with 8 network parameters and 5 linguistic variables are 58. It is impossible to create a single fuzzy if-then rule base when the attributes or the network parameters are large i.e. n=8 which is more than 300000 rules in the rule base. Such a rule base would result in high computational complexity; more run time and may fail to predict the required output. In the two-level fuzzy inference system for black hole detection, the feature set which consists of 8 parameters from the network layer is partitioned into two sets of 4 parameters. The rule base required for each fuzzy inference in level 1 is then 54 =625 and the number of rules in the level 2 rule base is 52 = 25.With the two-level fuzzy logic method, the total number of rules to be written in to rule base can be reduced to 1275. Figure 5.shows the 2 level fuzzy inference IDS for black hole detection.

4.3.1Feature set description

Forwarded Data packet Ratio (FPR): Ratio of the packets forwarded to the packets received by the node.

Delay: ∑(packet received time-packet sent time)/ number of packets received

Sequence number(Seq_Num): sequence number of the packet sent.

Average Sequence number (Avg_Seq_Num): average of the sequence number of the packet received by the node.

Packets Sent (PS): number of the packets sent by the node.

Packets Received (PR): number of the packets received by the node.

Throughput (Tpt): number of bits received by the node in a given amount of time. It is measured in kbps.Tpt =(Number of packets received*packetsize*8)/connection duration

Data Packet Drop Ratio (DPR): Ratio of number of packets dropped to the number of packets received

4.3.2Algorithm for two level fuzzy inference system

IDS Agent monitor and collect features periodically
All features are stored in the monitor table
Forward Packet ratio (FPR), Delay, Destination SeqNo (Seq_Num),
Average Sequence No(Avg_Seq_Num) Number of Packet Sent(PS),
Number of Packet Received(PR), Data Packet Drop Ratio(DR), Throughput(Tpt)
If (Detection ==Start)
for each node in the parameter table
Perform Level-1 fuzzy logic computation
Select features FPR,Delay, Seq_Num, Avg_Seq_Num
Do Fuzzification
Apply Fuzzy Rule
Collect the output1 from the fuzzy engine
Select features PS,PR,DR,Tpt
Do Fuzzification

Apply Fuzzy Rule
Collect the output2 from the fuzzy engine
Perform Level-2 fuzzy logic computation
Select output1 and output2 as Input
Apply Fuzzy Rule
Collect the output3 from the fuzzy engine
If (output3 ==LOW)
Node declared as an attacker
Node Id added into the block list
Alarm Packet Sent to all neighbours

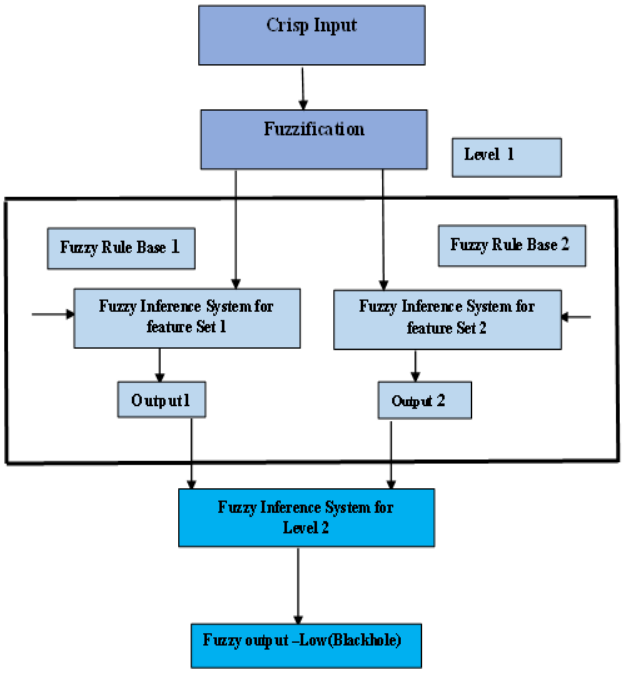

Figure 5. 2 level fuzzy inference IDS for black hole detection.

5. Experimental results

The simulation of two level fuzzy based intrusion detection system for detecting theblack hole attacks is carried out in Network Simulator (NS2) for the following cases with varying black hole nodes.

1..Detection with Fuzzy Logic-based IDS deployed in all nodes (without cluster head) in the network (DWOCH).

2..Detection with Fuzzy Logic-based IDS deployed in the cluster Heads (DWCH).

The performance and comparative analysis are carried out for the IDS Schemes. The efficiency of the proposed method with the existing methods is also analyzed.

Detection performance parameters:The standard performance evaluation parameters are used to investigate the results of Fuzzy logic-based IDS.In the proposed method, the abnormal behavior is shown as positive and normal events as negative.

True Positive (TP): intrusions correctly identified as intrusions

False Positive (FP): normal events being identified as intrusions

True Negative (TN): normal events correctly identified as normal

False Negative (FN): intrusions incorrectly identified as normal [33]

Detection Rate (DR) $DR = \frac{TP}{(FN+TP)}$ (1)

False Alarm Rate (FAR) $FAR = \frac{FP}{(FP+TP)}$ (2)

$\text{Accuracy} = \frac{(TP+TN)}{(TP+FP+TN+FN)}$ (3)

Average Detection Delay(DD) $DD = \frac{\sum(\text{Detection start time} - \text{Attacker Detect time})}{\text{Total number of attackers}}$ (4)

5.1 Simulation

The simulation is done using NS-2 to create the network and hence to cluster and select the cluster head for the clusters. The simulation of a wireless ad hoc network with 2 level fuzzy logic IDS deployed in all the nodes, random nodes, and cluster heads is done for the varying black hole attackers. The simulation profile of Table 1 is followed. Figure 6. and Figure 7. show the formation of cluster and cluster heads.

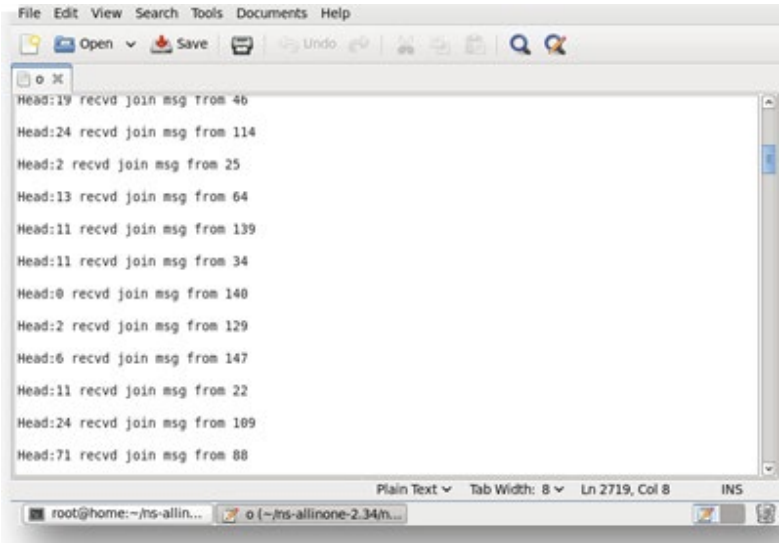

Figure 6. Formation of cluster

5.2 Performance analysis of 2 level fuzzy IDS with varying attackers

The simulations are done for the scenarios with i) Fuzzy logic IDS deployed in cluster head ii) Fuzzy logic IDS deployed in all nodes.The performance of the network concerning PDR, delay, throughput, control overhead, Normalized control overhead, and energy are analyzed. The detection parameters are also analyzed to study the efficiency of the DWOCH and DWCH IDS deployment methods.Table 3. shows the network performances forDWOCH and DWCH IDS schemes.Figure 8. Shows the improvement in the PDR after implementing IDS.Figure 9. shows the variations in the parameters of both the detection schemes compared

to black hole attackers. The parameters PDR and throughput are improved to 81% then blackhole attacks. This is because after the detection and isolation of black hole attacks the packets are routed in an optimum path to the destination. The delay is increased compared to the black hole attack as the drop ratio is decreased considerably and maximum packets reach the destination and also it is less than no attack condition.It is increased by 31.4% with DWOCH and 8.7% higher with DWCH. In detection schemes, the control overhead is increased compared to black hole attacks as it involves more exchange of control packets for detection and isolation

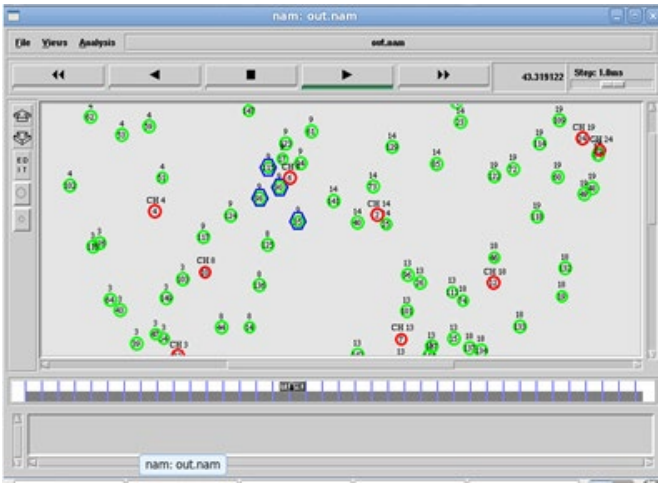

Figure 7. Cluster Heads and Attackers

The total average energy consumption is also increased to 41% and 30.8% in DWCH and DWOCH as more packets are recovered and sent to the destination. The Normalized routing Overhead is reduced to 99% compared to a black hole attack as more packets are delivered at the destination. The average variation in the network parameter results shows that DWCH is better than DWOCH in improving the performance of the network after detecting and isolating the black hole attack.

Figure 10. shows the improvement in network parameters with DWCH IDS than DWOCH IDS for varying attackers. The delay, control overhead, and energy consumed is less in the DWCH method than DWOCH as only cluster heads are involved in the detection. The control packets for detection, alarm generation are less in this case. Similarly, the energy consumed and delayare higher in DWOCH as all the nodes in the network are involved in the detection. The PDR, Throughput is improved as more packets are delivered at the destination in the shortest path, and also the detection is accurate with cluster head as it covers all the regions. For the same reason, the NROH is reduced in DWCH compared to DWOCH. In the Network parameters,the maximum improvement is in the end-to-end delay which is 34%.This is because the cluster head-based fuzzy IDS covers the area and detects the blackhole attacks in its cluster and blocks it less time than the all node-based fuzzy IDS and hence reducing end-to-end delay.Table 4.shows the detection performance of the 2 level fuzzy logic IDS schemeemployed in cluster heads and all nodes. The detection parameters accuracy is higher with less number of attacks and reduces with an increasing number of attackers. Detection delay increases with more attacks. The average detection performance of DWCH is better than

DWOCH. The false alarm rate varies between 0 and 0.5.All the detection parameters show improved performance in DWCH compared to DWOCH.

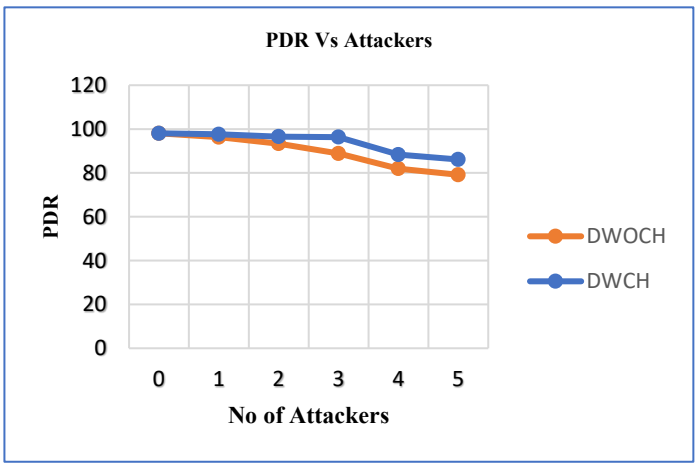

Figure 8. Packet Delivery Ratio with DWOCH and DWCH for varying attackers

From the literature survey, the results of the existing methods for detecting black hole attacks are analyzed. AikateriniMitrokotsa et al (2008)[20] IDS using Classifiers: MLP, Linear classifier, Bayesian Classifier, SVM got DR of 0.85-0.38 and PDR of 0.47. Huike Li Dagum et al (2009) Novel IDS using SVM & fuzzy network achieved DR of 0.98-0.93[21]. Farhan Abdul Fattah et al(2010)[22] Conformal Prediction K Nearest Neighbour& Distance-based Outlier Detection(black hole attacks) were able to get TPR of 0.99-0.96, FPR of 0.01-.001, and Accuracy of 0.99-0.97. Kulbhushan et al (2011) IDS with Fuzzy level with Thresholding (black hole attacks) achieved DR of 0.91-.87, FPR of 0.06-.08, and PDR of 0.9-1[24]. Ming Yang Su (2011) IDS with Anti Black Hole Mechanism using a threshold for suspicious value(black hole attacks) achieved TPR 1, FPR of 0.06-.08, and PDR of 0.65-0.9[25].MonitaWahenngham et al (2012)[3] IDS with Fuzzy level with Thresholding(black hole attacks) could achieve DR of 0.8-0.2. Chundong Se et al(2013)[26] IDS using Path-based and Collision based using dynamic thresholding (black hole attacks) got DR of 1-0.85. Nadeem et al (2014)[27] Intrusion detection & adaptive response mechanism (black hole attacks got DR of 0.92-0.8. AnujRana et al (2015)[28] Enhanced AODV modified method achieved DR of 0.95-0.9. BasanthSubbu et al (2016)[29] IDS using Bayesian Game Formulation was able to get DR of 0.995 FPR of 0.654-.0165 and PDR of 0.97. Heerendra et al (2018)[30] Agent-based detection mechanism achieved a PDR of 94% and Moudnia et al (2019)[31] using fuzzy-based IDS was able to get DR of 0.998.

Table 3. Network performance with DWOCH and DWCH IDS schemes for varying Attackers

Network parameters	No of Attackers 1		2		3		4		5	
	DWOCH	DWCH	DWOCH	DWCH	DWOCH	DWCH	DWOCH	DWCH	DWOCH	DWCH
PDR	96.27	97.61	93.32	96.56	88.85	96.33	81.96	88.35	79.15	86.12
Tpt	97363	98712	94380	97647	87776	95161	81087	87278	78188	85077
COH	4079	3731	5240	4209	4779	4127	5485	4592	5465	4583
NROH	2.975	2.684	3.942	3.061	3.381	3.079	5.479	3.736	5.263	3.825
Delay	0.040	0.023	0.068	0.036	0.123	0.089	0.122	0.098	0.135	0.119
Energy	7.001	5.763	8.395	6.455	6.502	5.873	6.250	5.827	6.012	5.267

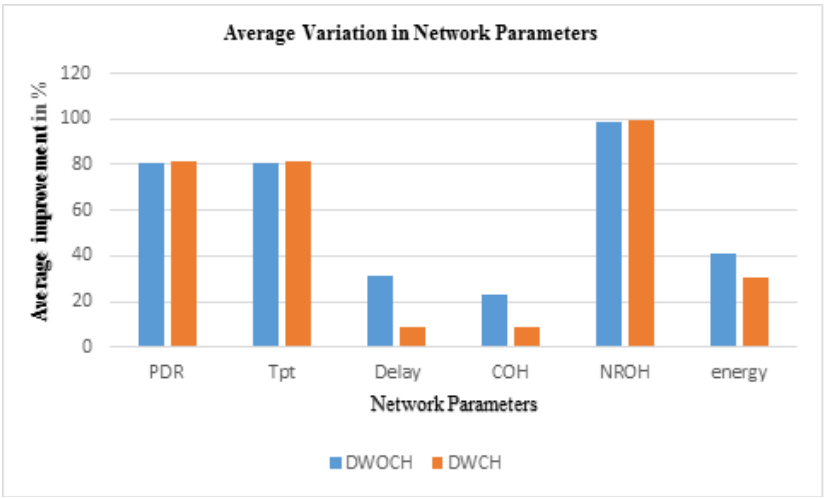

Figure 9 Variations in the parameters of both the detection schemes compared to black hole attackers.

The 2 level fuzzy logic-based IDS implemented in detecting black holes were able to reduce the no of rules in the rule base to 99.6% for the extracted network feature set. It is evident from the experimental results that the proposed method was able to improve the detection rate and accuracy to a maximum of 100%. The false alarm rate was reduced to 0%. The results show that the 2 level fuzzy IDS for detecting black hole attacks is reliable and scalable.

Table 4. Detection parameters with 2 level fuzzy logic-based IDS deployed in all nodes(DWOCH) and Cluster heads(DWCH)

Detection parameter	No of Attackers									
	1		2		3		4		5	
	DWOCH	DWCH	DWOCH	DWCH	DWOCH	DWCH	DWOCH	DWCH	DWOCH	DWCH
DR	1	1	1	1	0.666	1	0.75	0.75	0.8	0.8
Accuracy	0.993	1	0.993	0.993	0.98	0.993	0.980	0.986	0.973	0.98
FAR	0.5	0	0.333	0.333	0.5	0.25	0.4	0.25	0.428	0.33
DD	0.1	0.1	2.6	1.3	2.667	1.67	3.34	3	3.8	3

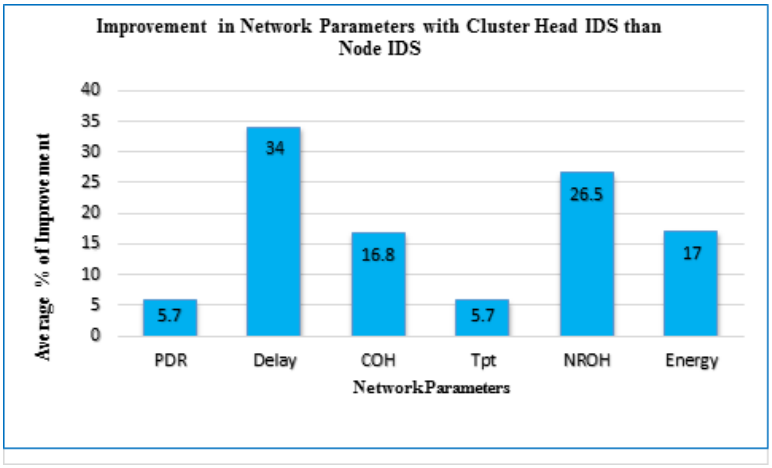

Figure 10. Improvement in network parameters with DWCH IDS than DWOCH IDS for varying attackers

6 Conclusion & Future Work

An intrusion detection system is a security system that monitors the nodes and network traffic and there is a great scope for designing an IDS system. This work addressed the impact of a black hole attack in a wireless ad hoc network and a 2 level fuzzy-based IDS to identify and isolate the attacks. Simulations are carried for 2 level Fuzzy based IDS for varying numbers of attackers. A comparative study of the network performance and detection parameters of 2 level fuzzy-based IDS deployed on cluster-based and all nodes are also carried out in this work. With the 2 level fuzzy logic IDS, the IDS performance parameters are

improved. The cluster head based fuzzy logic IDS shows improved performance than the node-based fuzzy logic IDS. The main goal of the proposed IDS is to minimize the false alarm rate, improve the detection rate, accuracy, and detection delay and increase the network performance which is achieved through this research work and is evident in the results. In the future, adaptive Techniques can be developed to change the rule base based on network dynamics and multi-level fuzzy logic can be designed to detect multiple network attacks.

References

[1] Debdutta Barman Roy,NingrinlaMarchang. MCBHIDS Modified layered cluster based algorithm for black hole IDS India Conference (INDICON), Annual IEEE India Conference (INDICON); 2013.1 – 6

[2] Debdutta Barman Roy,NabenduChaki and RituparnaChaki, BHIDS: A New Cluster Based Algorithm For Black Hole IDS, Security And Communication Networks,Security Comm. Networks.2010; 3:278–288

[3] MonitaWahengbam&NingrinlaMarchang (2012) Intrusion Detection in MANET using Fuzzy Logic.3rd National Conference on Emerging Trends and Applications in Computer Science.2012; 978-1-4577-0748

[4] Vishnu Balan. E, Gokulnath C, Priyan M K, Prof. Usha Devi G. Fuzzy Based Intrusion Detection Systems in MANET. ELSEVIER Procedia Computer Science. 2015; 50: 109 – 114

[5] Ajanta Konar and Ramesh Joshi C. An Efficient Intrusion Detection System Using Clustering Combined with Fuzzy Logic.Contemporary Computing, of the series Communications in Computer and Information Science.2010; 94: 218-228.

[6] Deepa Krishnan. A Distributed Self-Adaptive Intrusion Detection System for Mobile Ad-hoc Networks using Tamper Evident Mobile Agents. International Conference on Information and Communication Technologies ELSEVIER, Procedia Computer Science, 2015;46 :1203 – 1208

[7] Kulbhushan and Jagpreet SinghFuzzy Logic Based Intrusion Detection System AgainstBlackhole Attack on AODV in MANET. IJCA Special Issue on Network Security and Cryptography NSC.2011;28-35

[8] AlkaChaudhary, Vivekananda Tiwari and Anil Kumar. A Novel Intrusion Detection System for Ad Hoc Flooding Attack Using Fuzzy Logic in Mobile AdHoc Networks, IEEE International Conference on Recent Advances and Innovations in Engineering. 2014; 1-4

[9] Christeena Joseph, P. C. Kishoreraja, RadhikaBaskar ,M. Reji.Performance Evaluation of MANETS under Black Hole Attack for Different Network Scenarios. Indian Journal of Science and Technology. 2015;Vol 8(29).1-10

[10] AbhijitDeodhar ,RiteshGujarathi.A Cluster Based Intrusion Detection System for Mobile Ad Hoc Networks.citeseer ,1-15

[11] K. Belarbi, F. Titel, W. Bourebia, K. Benmahammed. Design of Mamdani fuzzy logic controllers with rule baseminimisation using genetic algorithm. Engineering Applications of Artificial Intelligence 2005; 18 875–880

[12] Praveen Joshi.Security issues in routing protocols in MANETs at network layer.Elsevier Procedia Computer Science 2011,3:954–960

[13] Satyabrata Chakrabarti and Amitabh Mishra.QoS Issues in Adhoc Wireless Networks. IEEE Communication Magazine. 2001;142-148

[14] Raman Singha, Harish Kumar.B and Singla.R.KAn intrusion detection system using network traffic profiling and online sequential extreme learning machine, Expert Systems with Applications,2015; 42:8609-8624

[15] Tayde K.S and Sahu.A.M.Challenges and Future Directions in Ad Hoc Networking-Review, International Journal of Advanced Research in Computer Science.2013;4:180-186.

[16] Sanjay Dhurandher.K, Isaac Woungang, RaveenaMathur, and PrashantKurana, GAODV: A

Modified AODV Against Single and Collaborative Blackhole Attacks in MANETS. 27th International Conference on Advanced Information Networking and Application workshops.2013;357-362
[17] Sergio Pastrana, Aikaterini Mitrokotsa, Agustin Orfila and Pedro PerisLopez,. Evaluation of classification algorithms for intrusion detection in MANETS Elseiver Knowledge-Based Systems 36:2012;217–225
[18] Vydeki, D, Bhuvaneswaran.R.S Effect of Clustering in Designing A Fuzzy Based Hybrid Intrusion Detection System For Mobile AdHocNetworks.Journal of Computer Science 9 2013;(4): 521-525.
[19] Maryam Fathi Ahmadsaraei and Abolfazl Toroghi Haghighat.A New Intrusion Detection System to deal with Black Hole Attacks in Mobile Ad Hoc Networks. Journal of Computer & Robotics 2013;6:7-14
[20] Aikaterini Mitrokotsa, Manolis Tsagkaris and Christos Douligeris 8. Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms. IFIP International Federation f'or Information Processing,Advances in Ad Hoc Networking.2008;265:133-144.
[21] Huike Li, Daquan Gu. A Novel Intrusion Detection Scheme Using Support Vector Machine Fuzzy Network for Mobile Adhoc Networks.IEEE Second Pacific Asia Conference on Web Mining and Web based Application.2009
[22] Farhan Abdel-Fattah, Zulkhairi Md.Dahalin and Shaidah Jusoh .Dynamic Intrusion Detection Method for Mobile Adhoc network Using CPDOD Algorithm.IJCA Mobile Adhoc Networks2010;.22-29.
[23] Kulbhushan and Jagpreet Singh.Fuzzy Logic Based Intrusion Detection System Against Blackhole Attack on AODV in MANET. IJCA Special Issue on Network Security and Cryptography.2011; NSC. 28-35
[24] Ming Yang S.U. Prevention of Selective Black hole Attacks on Mobile Adhoc Networks Through Intrusion detection systems. Elsevier computer Communications.2011;34:107-117
[25] Chundong She , Ping Yi , Junfeng Wang, Hongshen Yang.(2013)Intrusion Detection for Black Hole and Gray Hole in MANETs. KSII Transactions on Internet And Information Systems 2013;.7:1721-1736
[26] Adnan Nadeem and Michael Howarth. An Intrusion Detection & Adaptive Response Mechanism for MANETS. Elsevier Adhoc Networks.2014;13:368-380
[27] Anuj Ranaa, Vinay Ranab and Sandeep Gupta EMAODV: Technique To Prevent Collaborative Attacks in MANETS 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS2015, ELSEIVER Procedia Computer Science 2015;70: 137 –142
[28] Basant Subba, Santosh Biswas and Sushanta Karmakar. Intrusion detection in Mobile Ad-hoc Networks: Bayesian Game Formulation. Elsevier Engineering Science and Technology, an International Journal 2016;19:782–799
[29] Heerendra Mahore, Ratish Agrawal, Roopam Gupta. Agent Based Black Hole Detection Technique in AODV Routing Protocol.2018 International Conference on Advanced Computation and Telecommunication (ICACAT),Bhopal, India
[30] HoudaMoudnia, Mohamed Er-rouidib, HichamMouncifc, Benachir El Hadadi .Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET. Procedia Computer Science 2019;151 1176–1181
[31] Ansam Khraisat, Iqbal Gondal, Peter Vamplew and Joarder Kamruzzaman. Survey of intrusion detection systems:techniques, datasets and challenges. Cybersecurity.2019; 2:20
[32] Hongyu Liu and Bo Lang. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey.Applied Sciences.2019; 9, 4396.1-28
[33] Husain Shahnawaz And Gupta S.C. Black Hole Attack In AODV & Friend Features1 Unique Extraction To Design Detection Engine For Intrusion Detection System In Mobile Adhoc Network. Journal of Engineering Science and Technology.2012;7: 623 – 634.