An Efficient And Secure Intrusion Detection Method In Mobile Adhoc Network Using Intuitionistic Fuzzy

Anusha K[#1] , Jayaleshwari N[#2] , Arun Kumar S[#3] , Rajyalakshmi G V[#4]
[#]School Of Information Technology And Engineering
VIT University, Vellore
Tamilnadu – 632014, India
[1]anusha.k@vit.ac.in
[2]jayaleshwari@gmail.com
[3]aarunkumar889@gmail.com
[4]raji.desire@gmail.com

ABSTRACT

Mobile ad-hoc Network is a self organized wireless network which has a dynamic topology where nodes can be join or leave the network at anytime with large number of nodes. Due to its infrastructure less, dynamic topology and lack of centralization it is vulnerable to many security attacks. In this paper, we propose to detect the attack by using an Intrusion detection system that uses intuitionistic fuzzy logic which aims to detect distrust behavior of node and identify the attacks if it seems to be an attack based on given rules.

Keywords: *Routing protocols, Mobile ad-hoc network, Fuzzy, Intuitionistic fuzzy, Intrusion detection system*

1. INTRODUCTION

1.1 Mobile ad-hoc network

Mobile ad-hoc network [1] is a combination of mobile nodes which forms a network which is temporary, without any requirement of fixed network infrastructure, where other commercial wireless technologies are based on towers and base stations. It is characterized by fast installation, low bandwidth, limited processing capability. Mobile ad-hoc network communication is done by intermediate node in the network. In the nonexistence of proper security mechanism, mobile ad-hoc network is susceptible to many security attacks [2]. An attacker node may act as an intermediate node which may threat to the data which is being transmitted.

1.2 Ad-hoc on-demand distance Vector

The protocol, such as ad-hoc routing protocol is used to set routes between nodes and maintain the routes. The Ad-hoc on demand distance vector (AODV) [3] routing protocol is on-demand routing protocol i.e. whenever route for a particular node is needed, routes are created.

Each and every node in the network has a routing table which is maintained by AODV. It has one entry per destination and depending upon the sequence number routing information is updated that prevent routing loops. Main feature of AODV is to maintain the time based states in each and every node.

1.3 Intrusion Detection System

In networks, intrusion detection monitors activities of the network [4]. First it the collects the activity information and analyzes whether there are any activities which violates the security rules.

Since the mobile ad-hoc network exhibits many successful social applications such as Novel security (military Operations), Civil Sector, Medical diagnosis, Sensor Networks and ubiquitous computing the data need to be secured.

1.4 Fuzzy and Intuitionistic Fuzzy

Fuzzy sets [5-6] theory proposed by Zadeh in 1945 has shown successful applications in various fields. In this hypothesis, the membership of an element to a fuzzy set is single value between zero and one. Fuzzy logic is a computational paradigm that provides a mathematical tool for dealing with the uncertainty and the imprecision that is involved in human reasoning, which is also known as approximate reasoning. The interpretability characteristic of fuzzy logic, which is the capability to express knowledge in a linguistic way, makes fuzzy logic-based systems attractive for application such as medical diagnosis [7]. But in reality non-membership function of an element to a fuzzy set is just equal to 1 minus the degree of membership that is there may be some hesitation degree. So, as the generalization of fuzzy sets, the concepts of intuitionistic fuzzy [8] were introduced by Atanassov in 1986. To describe an intuitionistic fuzzy set completely we need two or more functions such as membership function, non-membership function, hesitation margin. Our fuzzy and Intuitionistic fuzzy based intrusion detection systems are based on the systems respectively [9].

We design an Intrusion Detection System that detects intrusion in a MANET caused by malicious node launching different types of attacks with the help of threshold values, fuzzy logic and intuitionistic fuzzy, we tackle three types of routing attacks exhibits packet forwarding misbehavior known as black hole attack, Gray hole attack towards source and Gray hole attack towards destination. We deal with different aspects such as the relative significance of symptoms, the varied symptom patterns of different attack stages. Here, the symptoms-attack relationship constitutes one source of imprecision and uncertainty in the detecting process.

2. LITERATURE SURVEY

There are many works that are presented in the literature that discuss about techniques for intrusion detection. An intrusion detection system (IDS) was introduced to detect Black hole attack on AODV in MANET using fuzzy logic. This IDS uses two factors forward packets ratio and destination sequence number. These factors were implemented using fuzzy logic in which fidelity level was checked and compared against threshold value and detected presence of black hole attack [10].

A detection schemes uses the Sequential Probability Ratio Test (SPRT). The SPRT had been proven to be an optional detection test when the probability distributions of both normal and abnormal behaviors are given. Furthermore, they introduce non-parametric methods, which do not require training and are more adaptive to mobile scenarios. The proposed detection schemes were implemented and evaluated using 48 nodes and tested on a mobile ad-hoc network emulator at the Army Research lab. The concept and detection accurateness of various schemes were compared, especially in the presence of congestion. They provide trade off analyses among detection latency and probabilities of false alarms and missed detection.[11]

A new intelligent agent-based intrusion detection model for mobile ad-hoc networks uses a combination of outlier detection, attributes selection, and enhanced multiclass SVM classification methods. For this purpose, an effective preprocessing system was proposed that improves the detection accuracy and reduces the processing time. Likewise two new algorithms, namely an Intelligent Agent weighted Distance outlier detection Algorithm and an Intelligent Agent-Based Enhanced Multiclass Support Vector Machine algorithm were proposed for detecting the intruders in a distributed database environment that uses intelligent agents for trust management and co-ordination in transaction processing. The trial result of the proposed model shows that this system detects anomalies with low false alarm rate and high-detection rate when test with KDD cup 99 data sets [12].

A new accurate energy utilization based approach had been proposed using fuzzy logic in evaluating trust for misbehavior detection of a selfish node in MANET [13]. The packet loss is acceptable up to some threshold value; excess packet loss must be avoided. They have presented a fuzzy based decision to check a node is infected by Black hole attack. This system not only identifies the attack over the node but also reduces the data loss over the network [14].

3. METHODOLOGIES AND IMPLEMENTATION

3.1 Threshold value based approach

In this approach we collect the number of dropped packets for each node from the statistic file which is the output file of simulation. The data will be stored in the list called packet list which contains following fields-node number, packets sent as source, packets forwarded, packets received, packets dropped for no route, packets dropped for overflow, packets dropped for maximum hop count, total hop count, no of route selected, number of link broken. From this list we can identify the source, destination and active route through which data has been sent and also number of packets dropped for particular node. Then selection of threshold value plays an important role in detecting the attacks in mobile ad-hoc network. If the packets drop is greater than the given threshold value, then the node is said to be malicious. Depending on the drop of the packets we identified three types of attacks. We use two threshold values to detect the intrusion in the network namely- threshold and Dest_Threshold values, where the Threshold value should be greater than Dest_Threshold value. The node which drops all the packets and the total number of packets dropped should be greater than a threshold value. In gray hole attack towards source, number of packets dropped by node which traverses from source and the total number of dropped packets should be greater than threshold value. The total number of dropped packets which traverses from source should be greater than DestThreshold value.

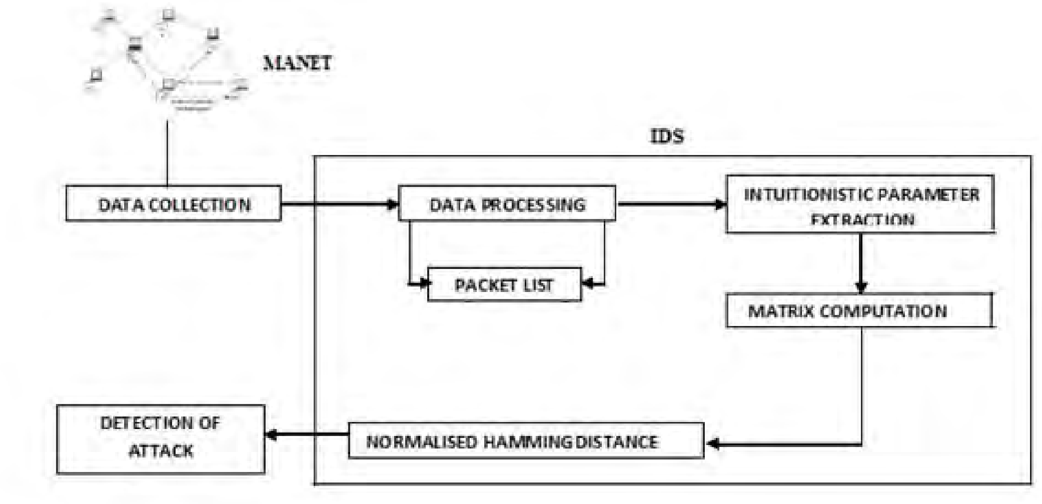

Fig. 1 Proposed System Architecture

In gray hole attack towards destination, number of packets dropped by node which traverses from source and the total number of dropped packets should be greater than threshold value. And the total number of dropped packets which is destined to particular destination should be greater than DestThreshold value.

As an Illustrated example, we take a network 6 nodes and traffic flow is assumed as follows.

1. 4>5>6
2. 6>5>4
3. 1>2>3>6

For a malicious node (node 5) launching a black hole attack. The total number of packets dropped: 65
From the packet list we maintain a list like this for an intermediate node which is the helping node which we defined as black hole attack.

TABLE 1
For node 5 towards Destination

Destination	Npd	Npf
6	43	0
4	22	0

TABLE 2
For node 5 towards Source

Source	Npd	Npf
4	22	0
6	43	0

For node 3 which we assumed to launch a gray hole attack towards source.

TABLE 3
For node 3 towards Source

Source	Npd	Npf
1	0	32

TABLE 4
For node 1 towards Source

Destination	Npd	Npf
2	0	23
3	0	22

For node 1 which we assumed as a node which doesn't have any attack

3.2 Fuzzy based approach

3.2.1 Fuzzy Parameter Extraction:

We applied fuzzy logic approach that is used in medical diagnosis. Here we consider three types of symptoms which may be appearing are i1, i2, and i3.

Indicator i1- when the number of packets dropped is greater than Threshold

Indicator *i2*- when the number of packets dropped is greater than Threshold and the number of packets dropped for the particular destination is greater than Dest_Threshold.

Indicator i*3*- when the number of packets drop is greater than Threshold and the numbers of packets drop for the particular source is greater than Dest_Threshold.

Moreover, we consider three types of attacks a1, a2 and a3.

Attack a1- Black hole attack

Attack a2- Gray hole attack towards destination

Attack a3- Gray hole attack towards source

3.2.2 Fuzzy Computation:

Let S denote the crisp universal set of all indicator I= {i1, i2, i3} and A denote the crisp universal set of all attacks A= {a1, a2, a3}. Let N be the crisp universal set of all nodes N= {1, 2, 3, 4, ...n}, where n= number of nodes. Then we calculate four different types of indication with respect to each node at regular interval of time. These indication are calculated depending on

Ri= N×I, where $\mu_{Rs}(n, i)$ $(n \in N, i \in \mathrm{I})$. This indicates the degree to which the indicator I is present in each node n.

Ro= I×A, where $\mu_{Ro}(i, a)$ $(i \in I, a \in A)$. This indicates the frequency of occurrence of indicator I with attack a.

Rc= I×A, where $\mu_{Rc}(i, a)$ $(i \in I, a \in A)$, corresponds to the degree to which indicator I confirms the presence of attack a.

Ri matrix values are calculated for each node depending on Threshold and Dest_Threshold. Ro and Rc matrices are assigned values based on knowledge about the attacks and their symptoms.

Using relation Ro, Rc, Ri, now we calculate four different indication relations defined on the set N×A nodes and attacks. The indications are as follows:

- The occurrence indication R1= Ri $\circ$ Ro (the operator ‘$\circ$ ‘indicates the max-min composition of Rs and Ro)
- The assurability indication R2= Rs $\circ$ Rc
- Non occurrence indication R3= Rs $\circ$ (1-Ro)
- Non-indicator indication R4= (1-Ri) $\circ$ Ro.

3.3 Intuitionistic fuzzy based approach

3.3.1 Intuitionistic Fuzzy Parameter Extraction:

To make a proper attack for a node with given values of tested indicator I, we propose a new method based on calculating distance between attacks A. Moreover the calculation based on fuzzy intuitionistic method is easy than fuzzy logic.

We applied intuitionistic fuzzy logic approach that is used in medical diagnosis. Here we consider three types of indicator which may appear are i1, i2, and i3.

Indicator i*1*- when the number of packets dropped is greater than Threshold

Indicator *i2*- when the number of packets dropped is greater than Threshold and the number of packets dropped for the destination is greater than Dest_Threshold.

Indicator *i3*- when the number of packets drop is greater than Threshold and the numbers of packets drop for the particular source is greater than Dest_Threshold.

Moreover, we consider three types of attacks a1, a2 and a3.

Attack a1- Black hole attack

Attack a2- Gray hole attack towards destination

Attack a3- Gray hole attack towards source

There will be only two matrixes which decide the attack that would be there in the node or not. Using the normalized hamming distance method the node which gets lowest point, will decided as attacker node with specifying the types of attack it has.

3.3.2 Computation:

We calculate two matrices. Ra and Ri. Ri matrix values are calculated for each node depending on Threshold and Dest_Threshold. Ra matrix is assigned values based on knowledge about the attacks and their indicator. Out task is to make a proper diagnosis of attack in node. To full fill the task we calculate a distance of symptoms from a set of symptoms for each attack. It can be obtained using Normalized Hamming Distance (lowest distance point) or using normalized Euclidean distance.

4. IMPLEMENTATION

4.1Creating Black hole attack

Black hole attack caused by RREQ

An attacker can send fake RREQ messages to form Black hole attack. In RREQ Black hole attack, the attacker pretends to rebroadcast a RREQ message with a non-existent node address. The remaining nodes will revise their route to pass by the non existing node to the destination node. As a result, the normal route will be broken down. The attacker can generate Black hole attack by faked RREQ message as follows:

- Set the target IP address to the destination node's IP address;
- Set the source IP address (in the IP header) to a non-existent IP address (Black hole);
- Give highest sequence number to the attacker node, or decrease the hop count to 1.

Black hole attack caused by RREP

The intruder node may generate a RREP message to form Black hole as follows:

- Set the hop count field to 1;
- Destination IP address as the target node of the route;
- Set the destination sequence number as highest sequence number;
- Set the source IP address (in the IP header) to a non-existent IP address (Black hole).

The attacker unicasts the faked route reply message to the originating node which starts route discovery process. When it receives the faked RREP message, it will consequently update its route to target node through the non-existent node which is a attacker node.

4.2 Creating gray hole attack

The defined attacker node drops the packets selectively. For example, any packet from a node is checked as tcp packet or udp packet , and then dropped.

In this, first part of our work is to collect the network data in the form of statistic file which is the output file of simulation. It gives details about all layers and the application we are using like CBR(Constant Bit Rate), FTP(File Transfer Protocol), TELNET, TRAFFIC GEN. and also gives the details about full routing mechanism which we are using in our scenario. The attacks which we concentrate occurs in the network layer uses aodv or any other protocol.

In the second part of our work is to calculate the different matrics based on the Threshold value and Dest_Threshold value using fuzzy logic. for example Rs matrix is computed : Ri[n_no][1]

In this n_no indicates that node number 1 is indicator 1. Ri[0][1] is set to 1, if the number of packets dropped by node 1 is greater than Threshold value. If the number of packets dropped is between 3 to Threshold value then it is set by trapizoidal membership fuction value which uses

$$\text{Membership function} = \frac{\text{Threshold - No.of packets dropped}}{\text{threshold}}$$

If the number of packet loss is less than 3 packets Ri[0][1] is set to 0. Since 1 or 2 packets loss is acceptable in the knowledge of data transfer in the network. Likewise the matrix will be filled by the data list. In the same way the value for indicator-2 and indicator-3 will be calculated based on Dest_Threshold value. R1, R2, R3, R4 matrics will be calculated with the help of Ro and Rc matrics. The value of those matrics are

$$\text{Ro} = \begin{bmatrix} 1 & .5 & .5 \\ .5 & 1 & .5 \\ .5 & .5 & 1 \end{bmatrix} \qquad \text{Rc} = \begin{bmatrix} 1 & .5 & .5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

In the third part of our work is to calculate the matrix Ri which have three values for a node with a single indicator. Those will be calculated by membership function, non membership function and hesitation degree which follows trapezoidal method. The values for this matrix will use the method which is given in the section 1.4 with the help of Threshold value and Dest_Threshold value. Here the default matrix for indication is assumed based on knowledge of attacks as we defined in fuzzy based approach.

Membership function, non-membership function and hesitation degree values will be calculated based on the following way which all uses trapezoidal method

Let A be the intuitionistic fuzzy set, x is a non empty set,

Membership function and Non-membership function can be defined as

$$A = \{(x, \mu_A(X), v_A(X)) \mid x \text{ belong to } X)\}$$

Where $\mu_A: X \rightarrow [0, 1]$ and $v_A: X \rightarrow [0, 1]$ is the degree of membership and non membership element x belongs to the set A with $0 \leq \mu_A + v_A \leq 1$ for each x belongs to X

Hesitation Degree of x belongs to A is given by,

$\pi_A = 1 - \mu_A - v_A$

The matrix will have the assigned value of following table

TABLE 1: PRIMARY MATRIX

	A1			A2			A3		
I1	1	0	0	0.5	0.5	0	0.5	0.5	0
I2	0	0	0	1	0	0	0	0	0
I3	0	0	0	0	0	0	1	0	0

After calculating the matrix from the intuitionistic fuzzy computation, both the matrix will be given to the normalized hamming distance method which will produce the lowest point for each node. From that the node which have the lowest point among all

Nodes that will be associated symptom for each node. The normalized hamming distance

$$\boldsymbol{l}\,(\boldsymbol{s}(\boldsymbol{n}\mathbf{i}), \boldsymbol{a}\mathbf{k}) = \frac{\mathbf{1}}{\mathbf{10}}\sum_{\boldsymbol{j}=\mathbf{1}}^{\mathbf{3}}(|\boldsymbol{\mu}\mathbf{j}(\mathbf{pi}) - \boldsymbol{\mu}\mathbf{j}(\mathbf{dk})| + |\mathbf{vj}(\mathbf{pi}) - \mathbf{vj}(\mathbf{dk})| + |\boldsymbol{\pi}\mathbf{j}(\mathbf{pi}) - \boldsymbol{\pi}\mathbf{j}(\mathbf{dk})|)$$

Where n_i denotes the number of nodes taken for an experiment, ak denotes that attacks. $\boldsymbol{\mu}\mathbf{j}, \mathbf{vj}, \boldsymbol{\pi}\mathbf{j}$ Are membership, non-membership and hesitation degree value for each node.

5. SIMULATION

We use QualNet 5.0.2 network simulator to simulate the scenario. The scenario which has 1500*1500 canvas area contains network components. The protocol used here is AODV.

TABLE 2: SIMULATION PARAMETER

No. of Nodes	6
Area size	1500 X 1500
Mac	802.11
Packet Size	512 bytes
Mobility Model	Random Way Point
Simulation time	30 Sec
Routing Protocol	AODV

For the second part of work that is fuzzy based approach the above table shows the Ri, R1, R2, R3 and R4 when there is a black hole attack by node 5, gray hole attack towards source1 by node 3

TABLE 3: THRESHOLD=26 AND DEST_THRESHOLD=13, FUZZY

Nodes	Ri	Rl	R2	R3	R4
N1	[000]	[000]	[000]	[000]	[1 1 1]
N2	[000]	[000]	[000]	[000]	[1 1 1]
N3	[00.64]	[.44 .44.64]	[00.64]	[.44.44 0]	[11.56]
N4	[000]	[000]	[000]	[0 0 0]	[1 1 1]
N5	[.8400]	[.84 .48.48]	[.84.48.48]	[0.48.48]	[.52 11]
N6	[000]	[000]	[000]	[000]	[111]

In table, we observe that the occurrence indication (R1) of node 5 shows that there is a indication of black hole attack (0.84), where as the gray hole attack towards destination and gray hole attack towards source are 0.48 each meaning that they are not indicative of these attacks w.r.t node 5. Similarly, the assurability indication (R2) of node 5 shows we can almost confirm (0.84) the black hole attack of node 5, where as the values for other attacks are only 0.48. the non-occurrence indication (R3) of black hole attack for node 5 is 0 compared to 0.48 for gray hole attack towards source and destination.

TABLE 4: SECONDARY MATRIX

	I1			I2			I3		
N1	0	0	1	0	0	1	0	0	1
N2	0	0	1	0	0	1	0	0	1
N3	1	0	0	1	0	0	0	0	1
N4	0	0	1	0	0	1	0	0	1
N5	1	0	0	1	0	0	1	0	0
N6	0	0	1	0	0	1	0	0	1

This will be given to normalized hamming distance formula. Then the table will be having these following values

TABLE 5: THRESHOLD=26 AND DEST_THRESHOLD=13, INTUITIONISTIC FUZZY

	I1	I2	I3
N1	0.4	0.5	0.5
N2	0.4	0.5	0.5
N3	0.3	0.2	0.4
N4	0.4	0.5	0.5
N5	0.2	0.2	0.2
N6	0.4	0.5	0.5

From the above table observe the helping nodes result that is the node which we assumed have been attacker nodes. Result of node 3 and node 5. Node 3 has the lowest value under indicator 2 denotes that node 3 is a gray hole attacker node towards destination. Node 5 ahs the lowest value under all symptoms since shows that it is black hole attacker node.

From the result we can observe that the calculation simplicity is very simple in intuitionistic fuzzy based approach and see the result as easily compared to fuzzy based and threshold based approach.

Wormhole attack

Wormhole is a severe type of attack, where two adversaries are connected to each other through high speed off -channel link. In this, wormhole node receives the packet at one location and sends it to other wormhole node through high speed off - channel link. The most dreadful can happen is that the nodes can be in a dilemma, whether they are close to the destination or not even though they are at far distance. Three types of wormhole attacks are:

- All Pass: In this attack the nodes will pass all the packets irrespective of their size.
- All Drops: In this attack all the packets are dropped by wormhole nodes.
- Threshold: In this it drops all the packets size which are greater than or equal to the threshold value

Performance Metrics

The wormhole attack has been detected based on performance metrics. The Metrics used for detecting the attacks are:

- Packet Delivery Ratio
- Average End-to-End Delay
- Throughput
- Jitter

Packet Delivery Ratio

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by source.

$$\text{Packet delivery ratio} = \frac{\text{Number of packets received}}{\text{Number of packets sent.}}$$

Deviation between normal MANET and Attack MANET

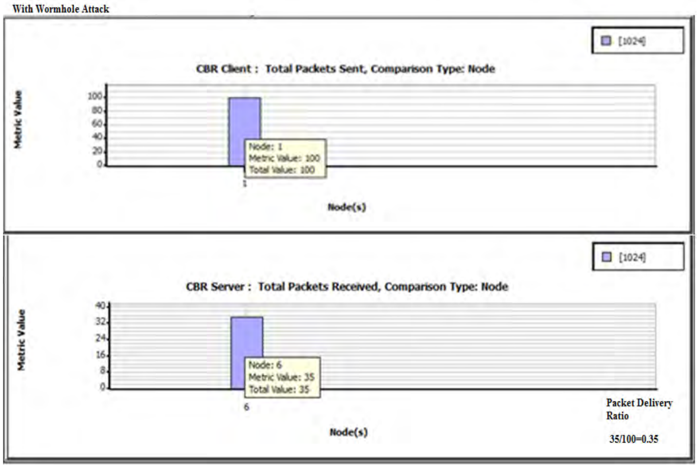

Fig.2 Packet Delivery Ratio

Average End-to-End Delay

Average end-to-end delay is the average time it takes a data packet to reach to destination in seconds. It is calculated by subtracting "time at which first packet was transmitted by source" from "time at which first data packet arrived to destination.

Average End-to-End delay=time at first data packet arrived to des-time at first data packet sent by src.

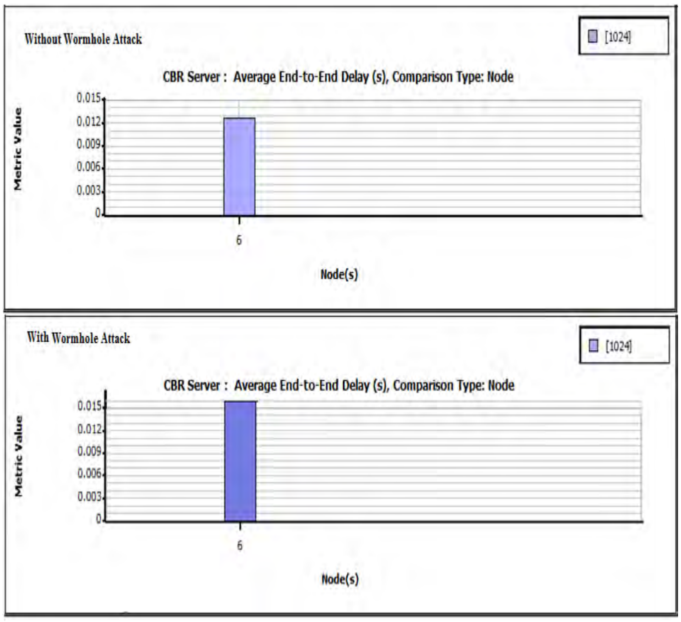

Fig.3 Average End-To-End Delay

Throughput

It is defined as total number of delivered data packets divided by the total duration of simulation time.

$$\text{Throughput}=\frac{\text{Total number of delivered packets}}{\text{total simulation time}}$$

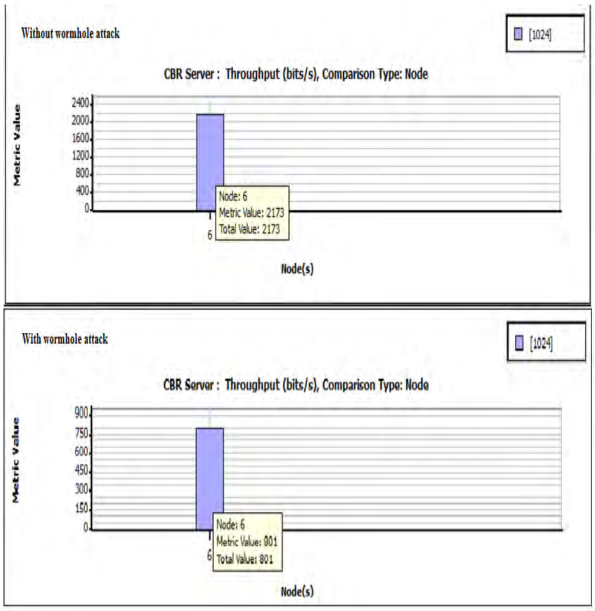

Fig. 4 Throughput

Jitter

Jitter is the variation in the time stuck between packets inward, caused by network congestion, and route changes.

6. CONCLUSION AND FUTURE WORK

We designed an Intrusion detection system that monitors the traffic for detecting black hole, two types of gray hole attacks. Besides we have incorporated intuitionistic fuzzy to handle the imprecise information. In future, the intrusion can be detected not only based on the number of packets dropped, it can be calculated based on hop count, bit rate, packet delivery ratio and more with more attacks for an efficient detection.

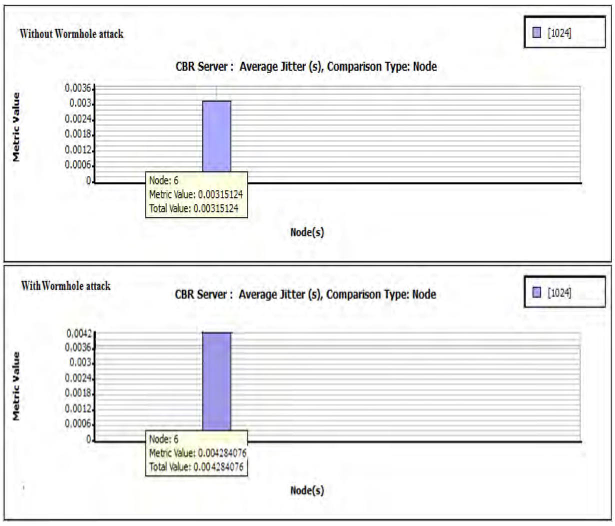

Fig.5 Average Jitter

7. REFERENCES

[1] Aniruddha Chandra: "Ontology for MANET security threats", PROC. NCON, Krishnankoil, Tamil Nadu, Mar. 2005, pp. 171 -17 6.

[2] John A. Clark, John Murdoch, John A. McDermid, Sevil Sen, Howard R. Chivers, Olwen Worthington and Pankaj Rohatgi: "Threat Modelling for Mobile Ad Hoc and Sensor Networks", in Annual Conference of ITA, 2007.

[3] C. E. Perkins and E. M. Royer: "Ad-hoc On-Demand Vector Routing", In Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications; pp. 90-100, New Orleans, LA, February 1999.

[4] D.Sterne, P.Balasubramanyam, D.Carman, B.Wilson, R. Talpade, C. KO, R. Balupari, C-Y Tseng, T.Bowen, K.Levitt and J.Rowe: "A general cooperative Intrusion Detection Architecture for MANETs", Proceedings of the 3'd IEEE International Workshop on Information Assurance, University of Maryland, and March 2005.

[5] S Rajasekaran, G.A. Vijialakshmi Pai: "Neural Networks, Fuzzy Logic, and Genetic Algorithms", PHi Learning Private Limited, P-1 57 - 2 21.

[6] Guan and Klir: "Fuzzy sets & Fuzzy Logic", PHi Learning Private Limited.

[7] R. Radha and S. P. Rajagopalan: "Fuzzy Logic Approach for Diagnosis of Diabetics", Information Technology Journal 6(I); 96-102, 2007.

[8] Atanassov K. (1986): "Intuitionistic fuzzy sets, Fuzzy Sets and Systems", 20 (1986) 87-96.

[9] Eulalia Szmidt and Janusz Kacprzyk: "Intuitionistic fuzzy sets in Some Medical Applications", Fifth International conference on IFSs, Sofia, 22-23 Sept. 2001.

[10] Ekta Kamboj: "Detection of black hole on AODV in MANET using fuzzy" Journal of current computer science and technology, vol.1 Issue 6[2011]316-318.

[11] Shanshan zheng, Tao Jiang and John S: "intrusion detection of in-band wormholes in MANET using advanced statistical methods", IEEE 2008.

[12] S.Ganapathy, P. Yogesh and A.Kannan: "Intelligent agent based intrusion detection system using enhanced multiclass SVM", Hindawi Publishing Corporation, Computational Intelligence and Neuroscience, volume 2012, article ID 850259.

[13] Vijayan R, Mareeswari V and Ramakrishna K: "Energy based trust solution for detecting selfish nodes in MANET using fuzzy logic", International journal of research and review in computer science, vol.2 No.3, June 2011.

[14] Poonam Yadav, Rakesh Kumar Gill and Naveen Kumar, "A fuzzy based approach to detect black hole attack", International Journal of soft computing and Engineering, ISSN: 2231-2307, volume-2, Issue -3, July 2012