IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-03, Issue-12 E-ISSN: 2347-2693

Intrusion Detection System for Black Hole Detection and Prevention in MANET Using Adaptive Neural Fuzzy Inference Systems

K.Santhi[1*] and V.Abinaya[2]

[1*,2] *Computer Science, Bharathiar University, India,*

www.ijcseonline.org

Received: 21/Nov/2015 Revised:03/Dec/2015 Accepted:17/Dec/2015 Published: 31/Dec/21015

***Abstract*— :** Mobile ad hoc network (MANET) is a self-configuring network of mobile nodes formed anytime and anywhere without the help of a fixed infrastructure or centralized management. It has many potential applications in disaster relief operations, military network, and commercial environments. Due to dynamic, infrastructure-less nature, the ad hoc networks are vulnerable to various attacks. AODV is an important on-demand distance vector routing protocol for mobile ad hoc networks. It is more vulnerable to black & gray hole attack. In MANET, black hole is an attack in which a node shows malicious behavior by claiming false RREP (route reply) message to the source node and correspondingly malicious node drops the entire receiving packet. In fuzzy based IDS an intrusion detection system is presented for MANETs against black hole attack detection as well as prevention using fuzzy logic. But it has some issues such as the attack detection accuracy and speed are less, and also it emphasized on very limited features for data collection towards detection of very specific range of attacks. To overcome above issues, the Adaptive Neural Fuzzy Inference Systems (ANFIS) is proposed and detect black hole attack in MANETs. The proposed system will identify the attack over the node as well as provide the solute on to reduce the data loss over the network. Through simulations, the results prove the proficiency of proposed technique which detect the black hole and improves the network performance.

Keywords*— *MANETs, ANFIS, Intrusion detection, Black hole Attack, AODV.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) do not have any preexisting infrastructure or administrative point as like conventional networks. In MANETs, mobile nodes can communicate freely to each other without the need of predefined infrastructure. This effectiveness and flexibility makes these types of networks attractive for many applications such as military operations, rescue operations, neighborhood area networks, education applications and virtual conferences. Mobile nodes play the role of host as well as routers and also support the multi-hop communication between the nodes. By the help of routing protocols, mobile nodes can send the data packets to each other in mobile ad hoc networks. Some characteristics of MANETs are communication via wireless links, resource constraints (bandwidth and battery power), cooperativeness between the nodes and dynamic topology make it more vulnerable to attacks [1] [2].

Due to Manet's characteristics, Prevention based techniques such as authentication and encryption are not good solution for ad hoc networks to eliminate security threats because prevention based techniques cannot protect against mobile nodes which contain the private keys. So that Intrusion detection system is an essential part of security for MANETs. It is very effective for detecting the intrusions and usually used to complement for other security mechanism. That's why Intrusion detection system (IDS) is known as the second wall of defense for any survivable network security [3]. There are some groups which works together to enhance the functioning of mobile ad hoc networks (MANETs). IETF constituted the mobile ad hoc networks working group in 1997 [4].

When any set of actions attempt to compromise with the security attributes such as confidentiality, repudiation, availability and integrity of resources then these actions are said to be the intrusions and detection of such intrusions is known as intrusion detection system (IDS) [5]. The basic functionality of IDS depends only on three main modules such as data collection, detection and response modules. The data collection module is responsible for collecting data from various data sources such as system audit data, network traffic data, etc. Detection module is responsible for analysis of collected data. While detecting intrusions if detection module detects any suspicious activity in the network then it initiates response by the response module. There are three main detection techniques presented in the literature such as misuse based, anomaly based and specification based techniques.

The routing protocols in MANET are mainly categorized into proactive routing protocols, reactive

routing protocols and hybrid routing protocol [6]. In proactive routing protocols, the routing information of nodes is exchanged, sporadically, such as DSDV. In reactive routing protocols, nodes exchange routing information when it is needed such as AODV [7].Some ad-hoc routing protocols are a combination of the above two categories called as hybrid routing protocols. These routing protocols play an important role in determining efficient route between a pair of nodes so that messages can be delivered in a timely manner.

A. Routing

It is the act of moving information from a source to a destination in an inter-network. During this process, at least one intermediate node within the inter-network is encountered. The routing concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the information groups (called packets) through an internetwork. The later concept is called as packet switching which is straight forward, and the path determination could be very complex. Routing protocols use several metrics to calculate the best path for routing the packets to its destination. The process of path determination is that, routing algorithms initialize and maintain routing tables, which contain the total route information for the packet.

B. AODV

It stands for ad-hoc on demand distance vector routing protocol. It is a reactive protocol. It makes the route when it is needed and does not require nodes to maintain the routes to various destinations that are not being used in communication. AODV enables multi- hop routing between participating mobile nodes wishing to establish and maintain an ad- hoc network. AODV is able to provide unicast, multicast and broadcast communication ability. Route tables are used in AODV to store applicable routing information. AODV utilizes both a route table for unicast routes and a multicast route table for multicast routes. The protocol is able to respond to topological changes that affect the active routes in a quick and timely manner.

C. IDS

Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system. The mechanism, by which this is achieved, is called an intrusion detection system (IDS). An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator.

D. Black Hole Attack

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the destination node of the packet that was intercepted. This attack can be easily implemented in AODV during the routing discovery process. Once the forged route has been established the malicious node is able to become a member of the active route and intercept the communication packets. The outcomes of this attack can vary. The malicious node can either stop after inserting the false route information in the network and aim in creating instability and unnecessary network traffic or drop all incoming application packet for the specific destination.

In this paper, the representing an intrusion detection system for MANETs against black hole attack detection as well as prevention using Adaptive Neural Fuzzy Inference Systems (ANFIS)and providing the technique against black hole attack and gray hole which is based on ANFIS rule. The proposed system will identify the attack over the node as well as provide the solution to reduce the data loss over the network. Through simulations, the results prove the proficiency of proposed technique which detects the black hole and improves the network performance.

The rest of this paper is organized as follows: Section 2 presents the literature review of Intrusion detection system. Section 3 describes the ANFIS based IDS on MANETs and Section 4 discusses the results of proposed IDS and finally conclusion and direction for future research is outlined in section 5.

II. RELATED WORK

MonitaWahengbam, NingrinlaMarchang [8] performed a work on “Intrusion Detection in MANET using the Fuzzy Logic”. Fuzzy rule[9] is implementing during the analysis phase to detect the misbehavior over the network. The work will analyze the traffic over a node and take a fuzzy decision regarding the node reliability. The parameters in paper are number of successful data transmitted over the node, number of packets lost. ElmarGerhards-Padilla, Marko

Jahnke et.al[10]performed a work,” Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs”. In this work Author present TOGBAD a new centralized approach, using topology graphs to identify nodes attempting to create a black hole. Author use well-established techniques to gain knowledge about the network topology and use this knowledge to perform plausibility checks of the routing information propagated by the nodes in the network.

LathaTamilselvan, Dr. V Sankaranarayanan [11] “Prevention of Co-operative Black Hole Attack in MANET” gave an approach to combat the Black hole

attack. In MANET, the absence of a fixed infrastructure, thus nodes have to cooperate in order to provide the necessary network functionality. One of the principal routing protocols used in Ad hoc networks is AODV (Ad hoc on demand Distance Vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack .In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. Their approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated. The percentage of packets received through our system is better than that in AODV in presence of cooperative black hole attack. The solution is simulated using the Global Sensor Simulator and is found to achieve the required security with minimal delay & overhead.

Rajib Das, Dr. BipulSyam Purkayasth [12] performed a work," Security Measures for Black Hole Attack in MANET: An Approach". In this paper, Author give an algorithmic approach to focus on analyzing and improving the security of AODV, which is one of the popular routing protocols for MANET. Presented aim is on ensuring the security against Black hole attack. The proposed solution is capable of detecting & removing Black hole node in the MANET at the beginning.

Jathe S.R, Dakhane D.M. [13] performed a work," A Review Paper on Black Hole Attack and Comparison of Different Black Hole Attack Techniques". Communicating without a network infrastructure. Due to security vulnerabilities of the routing protocols, however, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. In this paper Author studied the details about black hole attack, and comparison of different black hole attack techniques.

Rashid Sheikhl, Mahakal Singh Chande et.al [14] gave a paper on "Security Issues in MANET: A Review" In the paper author described security issues like No predefined Boundary, Adversary inside the Network, Changing scale etc. and security criteria .Also explained the intrusion detection systems and Privacy- preservation in MANET using Secure Multiparty Computation solution .

Ochola EO, Eloff MM [15] performed a work, "A Review of Black Hole Attack on AODV Routing in MANET". Black Hole attacks are launched by participating malicious nodes that agree to forward data packets to destination but eavesdrop or drop the packets intentionally, which not only compromise the network, but also degrade network performance. Routing protocols, which act as the binding force in these networks, are a common target of these nodes. The route updates are shared not on a periodic but on an as requirement basis. The control packets create a potential vulnerability that is frequently exploited by malicious nodes. The paper further analyses the impact of Black Hole attack in AODV performance.

A. Mitra *et al* in 2013[16] proposed an Artificial Neural Network (ANN) based automated Black Hole node detection tactic. Proposed ANN based system is dynamic in nature. Implemented intercommunication methodology for detecting the presence of Black Hole node helps to update routing table more dynamically as it is working at both ends: at CRC side and TTR side.

G. Wahane *et al.* in 2014[17] proposed the modification of Ad Hoc on Demand Distance Vector Routing Protocol. The proposed work suggests two new concepts, Maintenance of Data Routing Information Table and cross checking of a node. A security protocol has been proposed that can be utilized to identify multiple black hole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the black hole nodes.

III. PROPOSED METHODOLGY

In this section, the proposed Adaptive Neural Fuzzy Inference Systems black hole attack detection and prevention is explained.

A. System overview

Fig.1 represent system overview of proposed the ANFIS technique to detect the black hole and gray hole attacks. The proposed system will identify the attack over the node as well as provide the solution to reduce the data loss over the network. If ANFIS detects the malicious node means it will apply intrusion prevention system, otherwise the node is selected the route path and transmit the data to intermediate node. Then the intermediate node is sending the data to destination node.

The intrusion prevention system (IPS) mechanism mentioned is differentiates between normal flow and malicious flow in the Network. The IPS system takes the input parameter from the ANFIS matrix which categorizes the range of intrusion in a network. As soon as the malicious behavior of node is detected the IPS mechanism is activated. The IPS system then acts by blocking the malicious nodes by considering node index and modify its path as soon as malicious node is reached, the AODV routing protocol is modified such that it checks the node type and as soon as it matches the type of Black hole or Gray hole node type, the node of that type is blocked and an alternating path is chosen by AODV routing protocol.

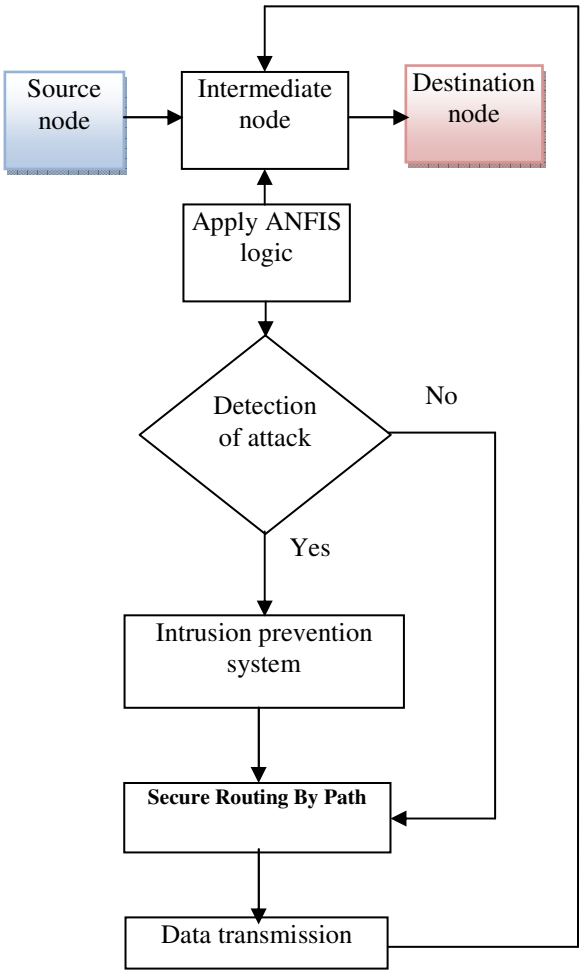

Figure 1. Overall architecture of proposed system

B. ANFIS model for black hole detection

The proposed improved ANFIS model is to detect black hole attack from source to destination nodes. Generally Adaptive Neuro-Fuzzy Inference System (ANFIS) consists of five layers such as input layer, fuzzy layer, and product layer; defuzzifys layer and output layer it was used for detection tasks. The training and testing of the parameters for black hole detection becomes one of the major important issues in detection task.

In this work utilizes use Takagi-Sugeno-Kang type fuzzy model for black hole detection. As transmissions begin from source node to destination node apply ANFIS on each intermediate node and it will check the threshold value for the intermediate node. It consists of two major parts such as antecedent and consequent parts and the structure of ANFIS model is shown in Figure 2.

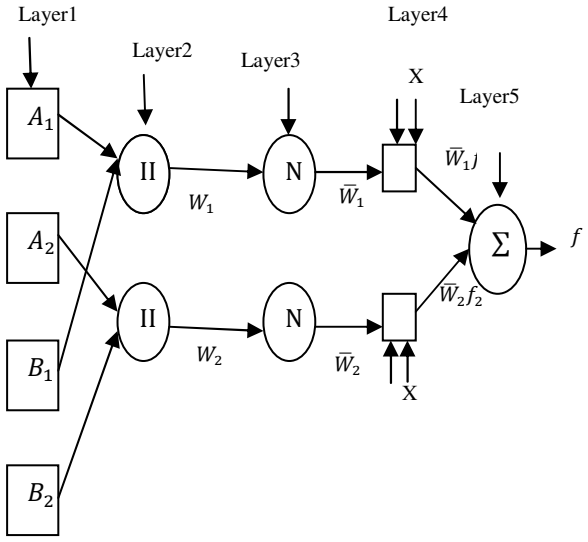

Figure 2. Adaptive Neuro-fuzzy inference systems

Representation of ANFIS model is carried out using fuzzy if-then rules and it is characterize in the following way:

R_i if x_1 is A_{i1} and x_2 is A_{i2} then x_1 is y_i is $f_i(x)$ (1)

where and are the intermediate nodes of transmission area. be the fuzzy membership set function to each rule and y_i is the black hole detection results for i^{th} rule. Fuzzy set A_{ij} at layer for each nodes result has the form,

$$A_{ij}(x) = exp\left\{-\left(\frac{x_j - m_{ij}}{\sigma_{ij}}\right)^2\right\} \quad (2)$$

where m_{ij} denotes centre and σ_{ij} be the measurement of A_{ij}correspondingly to detect the results of black hole. Similarly antecedent parts such as m_{ij}&σ_{ij}in ANFIS model for black hole detection is optimized through RLS.

$$\bar{w}_1 f_1 + \bar{w}_2 f_2 + \cdots + \bar{w}_n f_n = \hat{y}_1 + \hat{y}_2 + \cdots + \hat{y}_n \quad (3)$$

$$\begin{bmatrix} \bar{w}_1 x_1 & \bar{w}_1 x_2 & \bar{w}_1 \\ \bar{w}_2 x_1 & \bar{w}_2 x_2 & \bar{w}_2 \\ . & . & . \\ . & . & . \\ . & . & . \\ \bar{w}_n x_1 & \bar{w}_n x_2 & \bar{w}_n \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} \hat{y}_1 \\ \hat{y}_2 \\ . \\ . \\ . \\ \hat{y}_n \end{bmatrix}$$

$$P(t) = P(t-1) - p(t-1)\varphi(t)(I + \varphi^T(t)P(t-1)\varphi(t))^{-1}\varphi^T(t)P(t-1) \quad (4)$$

$$\theta(t) = \theta(t-1) + P(t)\varphi(t)(y(t) - \varphi^T(t)\theta(t-1))$$

These parameters are known as antecedent nodes. Black hole detection results of ANFIS is obtained by weighting the parameters values of subsequent parts of n rules through the equivalent membership evaluation,

$$\hat{y} = \sum_{i=1}^{n} \bar{w}_i f_i = \frac{w_i}{\sum_{i=1}^{n} w_i} \quad (5)$$

Where

$$w_i = \prod_{j=1}^{n} A_{ij}(x_i) \quad (6)$$

$$y_i = f_i(x) = (a_i x_1 + b_i x_2 + c_i) \quad (7)$$

Where is the node set of ANFIS objective function and it is named as consequent nodes. The weight values of layer 2 and layer 3 are decreased linearly starting during black hole detection process. Since the appropriate choice of the weight value only provides a best detection results among black hole to optimize consequent parts of ANFIS is mathematically specified as,

$$x_{id\,new} = x_{id} + v_{id\,new} \quad (8)$$

$$v_{id\,new} = (w * v_{id}) + c_1\big(rand_1(p_{id} - x - id)\big) + c_2\big(rand_2\big(p_{gd} - x_{id}\big)\big) \quad (9)$$

where ,

$$w = \exp\left(-iter/(spread\_factor \times \max\ \_iteration)\right) \quad (10)$$

$$spread_{factor} = 0.5(spread + deviation)$$

$$c_1 = 2(1 - iter/\max\ \_iteration)\ \&c_2 = 2$$

Where x_{id} and v_{id} represent the source and destination for every nodes of ANFIS model through d -dimensional investigate space correspondingly. In equation represents the velocity of each node in ANFIS models which present adequate information to optimize ANFIS nodes through the examination in solution search space. There are two major parts presented in equation (10), there are first and second parts. The initial part of the equation is used for approximation of the result of current velocity for black hole detection, the second parts move towards to achieve best optimized ANFIS nodes for entire transmission results. From this optimized nodes black hole detection is enhanced in terms of measurements like packet delivery ratio, packet delay and Throughput.$f_i(x)$.

IV. RESULT AND DISCUSSION

A. Simulation Model and Parameters

NS-2 is used to simulate the ANFIS algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. For the MAC layer protocol the distributed coordination function (DCF) of IEEE 802.11 (for wireless LANs) is used. It has the functionality to notify the network layer about link breakage. In the simulation, mobile nodes move in a 500meter x 500 meter region for 50 seconds simulation time. The number of mobile nodes is varied from20 to 100. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250meters. In our simulation, the speed is set as 2m/s. The simulated traffic is Constant Bit Rate (CBR).The pause time of the mobile node is kept as 10sec.

B. Performance Metrics

The proposed Adaptive Neural Fuzzy Inference Systems (ANFIS) is compared with the existing Fuzzy logic [18]. The evaluation is mainly based on performance according to the following metrics:

Table 1 Simulation Parameter

Parameter	Value
No of Nodes	10 to 50
Area size	500 x 500
Mac	802.11
Radio range	250m
Simulation on time	50 sec
Traffic source	CBR
Packet size	512
Mobility model	Random way point
Speed	2 m/s
Pause time	10 sec
Channel data rate	2 mbps

C. Throughput

It is defined as the total number of packets delivered over the total simulation time. It is represented in packets per second or bits per second.

Throughput (bits per second) = (No. of delivered packets * Packet Size * 8) /Simulation Time.

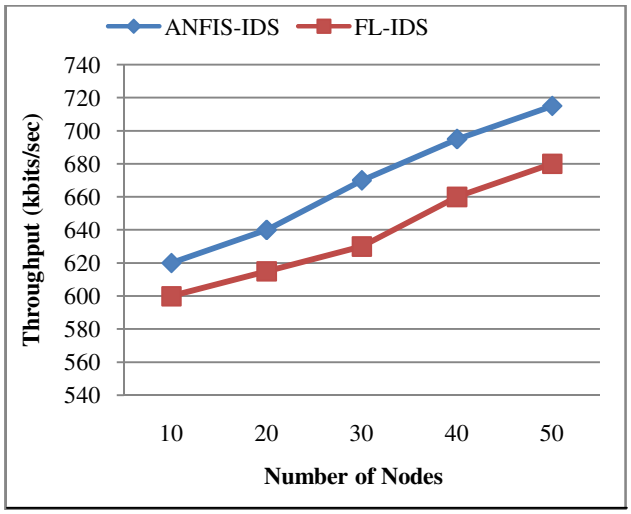

Figure 3. Throughput ratio vs. Number of Nodes

D. 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.

Packet delivery ratio= Number of packets received/ Number of packets sent

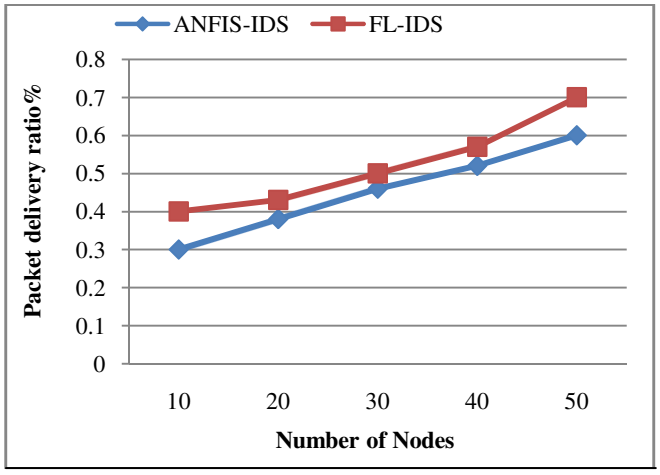

Figure 4. Packet delivery ratio vs. Number of Nodes

E. End-to-End Delay

The average time taken by the packets to pass through the network is called end-to-end delay. Figure 5 shows that average delay vs. number of nodes.

End-to-End delay [packet_ id] = received time [packet_ id]– sent time [packet_ id]

Average Delay = Where, = average end to end delay of node of ith application and n= number of application.

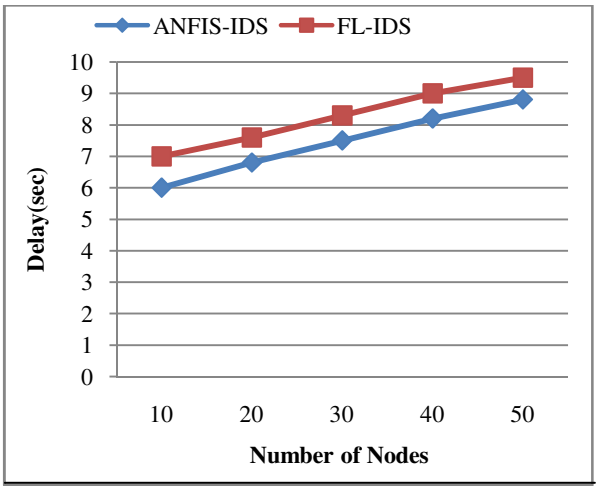

Figure 5. Average delay vs. Number of Nodes

V. CONCLUSION

In this paper, performance analysis of wormhole attacks under different scenarios taking threshold based Algorithms are simulated under NS2. Different performance metrics like Packet Delivery Ratio, Routing Overhead and Delay are used for analysis. Simulation results are based on AODV and DSR routing protocol by varying the number of nodes simultaneously. It can be concluded that AODV performs well than that of DSR. RTT calculation shows best results in packet delivery ratio, routing overhead and end-to-end delay than path tracing approach.

REFERENCES

[1] Y. Li and J. Wei., "Guidelines on selecting intrusion detection methods in MANET", In Proceedings of the Information Systems Educators Conference, **2004**.

[2] A. Hasti, "Study of Impact of Mobile Ad – Hoc Networking and its Future Applications", BIJIT – **2012; January - June, 2012; Vol. 4 No. 1; ISSN 0973 – 5658.**

[3] Y. Zhang and W. Lee., " Intrusion detection in wireless ad hoc networks" , In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), pages **275-283, 2000.**

[4] IETF Mobile Ad-Hoc Networks Working Group (MANET),IETFwebsite**www.ietf.org**/dyn/wg/charter/manet-charter.html.

[5] R. Heady, G. Luger, A. Maccabe, and M. Servilla, "The architecture of a network level intrusion detection system" Technical report, Computer Science Department, University of New Mexico, **August 1990**.

[6] Dokurer,Seimih "Simulation of Black hole Attack in wireless ad-hoc etworks" Master's Thesis AtihmUniversity,Septeber **2006**.

[7] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks," Communications Magazine, **IEEE, vol.40, no.10, pp. 70- 75, October 2002.**

[8] MonitaWahengbam," Intrusion Detection in MANET using Fuzzy Logic", 978-1-4577-0748-3/12/$26.00 © **2012 IEEE.**

[9] G.Kalpana, Dr..M.Punithavalli," fuzzy logic technique for gossip based reliable broadcasting in mobile ad hoc networks", Journal of Theoretical and Applied Information Technology **31st May 2013. Vol. 51 No.3.**

[10] ElmarGerhards-Padilla," Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", 32nd IEEE Conference on Local Computer Networks 0742- 1303/07© **2007 IEEE**.

[11] LathaTamilselvan "Prevention of Co-operative Black Hole Attack in MANET" JOURNAL OF NETWORKS, **VOL. 3, NO. 5, MAY 2008**

[12] K.Selvavinayaki, K.K.Shyam Shankar" "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANET"International Journal of Computer Applications **(0975-8887).volume7-volume11, October 2010.**

[13] Jathe S.R, Dakhane D.M ," A Review Paper on Black Hole Attack and Comparison of Different Black Hole Attack Techniques "International Journal of Cryptography and Security **ISSN: 2249-7013 & EISSN: 2249-7021**

[14] Rashid Sheikhl, Mahakal Singh Chande et.al "Security Issues in MANET: Review" 978-1- 4244-7202-4/10/$26.00 ©**2010 IEEE**

[15] Ochola EO," A Review of Black Hole Attack on AODV Routing in MANET. Information Security South Africa Conference, Proceedings **ISSA 2011**.

[16] A. Mitra, R. Ghosh, A. Chakraborty, D. Srivastva, "An Alternative Approach to Detect Presence of Black HoleNodes in Mobile Ad-Hoc Network Using Artificial Neural Network" in IJARCSSE, **2013.**

[17] G. Wahane, A. Kanthe, s"Techniques for detection of cooperative Black hole Attack in MANET" in IOSR-JCE, **2014**.

[18] AvinashSavaliya, Hardik Patel, BhavikPandya,"Fuzzy Based IDS for Black Hole Detection and Prevention in MANET", **www.academia.edu.**

AUTHORS PROFILE

Dr.K.Santhi received her MCA and M.Phil degree in computer science from Bharathiar University, India in 2001 and 2004 respectively. She received her doctorate in Computer Science from Anna University, India in the year 2014. Currently, she is working as an Associate Professor in the Department of Computer Science, Sri Ramakrishna College of Arts and Science for women. Her research area is networking , MANET.

Abinaya.V received the M.C.A degree from Bharathiar University, India in 2014 . She is pursuing her Master of Philosophy (M.Phil.) in Computer Science (Full Time) at Sri Ramakrishna College of Arts and Science for Women, Bharathiar University , India. Her research area of Networking, MANET.