Journal of Theoretical and Applied Information Technology
31st May 2014. Vol. 63 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FUZZY BASED DETECTION AND SWARM BASED AUTHENTICATED ROUTING IN MANET

[1]K.SHANTHI, [2]T.JEBARAJAN
[1]Assistant professor, Department of Computer Science and Engineering
Cape Institute of Technology, Tamilnadu, India
[2]Professor, Rajalakshmi Engineering College,
Thandalam,Chennai, Tamilnadu, India
E-mail: [1]shanthik0804@gmail.com

ABSTRACT

In mobile ad hoc networks (MANET), Artificial Intelligence (AI) based distributed intrusion detection (DIDS) techniques are very rarely available. In general, these techniques are used for either detection or authentication process. In this paper, we propose a combined approach named as fuzzy based intrusion detection and swarm based authenticated routing in MANET. This technique involves the detection of attacker level of the nodes in the network layers such as MAC layer, physical layer and routing layer using fuzzy logic technique. Based on the detected attacker level, the trust value of each node is updated. When source node wants to transmit a data packet to the destination, the route with trustworthy nodes is selected using swarm based ant colony optimization (ACO) technique. By simulation results, we show that proposed technique enhances the secured data communication.

Keywords: *MANET, Authentication, Routing, Attack*

1. INTRODUCTION

Mobile Ad hoc networks (MANETs) are the brand new communication standard used for wireless communication. Unlike wired infrastructures, it does not require any expensive base stations [1]. A mobile ad hoc network is defined as collection of autonomous nodes that forms an infra structure less topology [2]. Each node can operate as an end system and also as a router to forward packets. Hence it provides an attractive networking option for connecting mobile devices quickly [3]. Each node acts as a wireless router to route packets to the neighbor nodes to reach the intended destination [1]. Here each node communicates with nodes in its range and also to those outside its range using mulitihop communication [4]. Manets can be used for a wide range of application due to its inherent flexibility. Some of the applications include military, emergency response situations, search and rescue mission, data collection, virtual classes and conferences having laptops, PDA or other devices in wireless communication[5][1].

1.1 Attacks on MANETs

The dynamic nature of MANET's makes it more susceptible to numerous threats like passive eavesdropping, spoofing and modification of information [6]. Unlike wired networks, MANETs are more vulnerable to attacks. More over the flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices introduced new security risks [7]. MANETs are subjected to two types of attack namely active and passive attacks. The passive attack involves only eavesdropping of data. In the case of active attacks involves actions performed by adversaries like replication, modification and deletion of exchanged data. The attacks in MANET can cause congestion, propagation of incorrect routing information. It may also lead to the prevention of services from working properly or to the complete shutdown of the process [2]. Some of the most common malicious activities in MANETs are black hole (grey hole), worm hole attack, node impersonation [4].

1.2 Intrusion Detection System (IDS)

The process of monitoring activities in a system which can be a computer or a network is called intrusion detection. The mechanism that performs this task is called the Intrusion Detection System (IDS) [1]. It plays an important role in detecting the different types of attacks. One of the main functions of intrusion detection is to protect the network, analyze and find out intrusions among normal audit data [8].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The IDS can be classified into three categories which can be adjusted and suited for MANET.

Stand-alone IDS: The IDS runs on each node independently to determine intrusions in this architecture. The IDS's on the network does not have any cooperation or data exchange among itself. It is more suitable for flat network infrastructure than for multilayered network infrastructure.

Distributed and cooperative IDS: In Distributed and cooperative IDS, every node in the MANET participates in the Intrusion Detection. It responds through an IDS agent running on them. The IDS agent detects and collects local events and data in order to identify possible intrusions and also initiates a response independently.

Hierarchical IDS: The architecture is an extended version of the distributed and cooperative IDS architectures. It is proposed for a multilayered network infrastructure. Here the network is divided into clusters. The cluster head controls each cluster. Each IDS agent runs on every member node. It is responsible for its nodes monitoring and deciding on locally detected intrusions. The cluster head is responsible locally for its nodes and for its cluster. It monitors the network packets and initiates the global response when an intrusion is detected [4].

1.3 Issues of current IDS

Some of the unique problems for Intrusion Detection System (IDS) presented by the MANETs are

i) One of the limiting factors in IDS on MANETS is the monitoring of traffic promiscuously within wireless radio range.
ii)The mobility of the nodes.
iii) In ad hoc network, nodes are more vulnerable to compromise.
iv) An IDS may not be able to get enough sample data for accurate intrusion detection due to its dynamic network topology.[2]
v)The existing technique lacks flexibility. Hence cannot guarantee simultaneous satisfaction of diverse performance and cost requirements such as bandwidth consumption, sensing accuracy, continuous availability and detection latency [12].
vi) The current IDS are tuned specifically to detect known service level network attacks. The network administrator is allowed to detect the policy violations from the existing data or the data collected. The data is enormous so that the analysis process is time consuming.

The presence of high number of false positives and also limited resources to proactively analyze the data for policy violations causes the wastage of limited resources.[9]

1.4 Problem Identification

Artificial Intelligence (AI) based distributed intrusion detection (DIDS) techniques for MANETS are very rarely available. Generally these techniques are used for either detection or authentication in MANET. But a joint approach is required for accurate detection and mitigation of attacks in all the layers using AI techniques.

Swarm intelligence can be considered as the study of the collective behavior of multi-component systems that coordinate using decentralized controls and self-organization [14]. It is inspired by the process by which swarms of ants converge to the optimal route to a food source by progressively reinforcing the successful paths using pheromone secretions [15]. It uses mobile software agents for network management. These agents are autonomous entities, both proactive and reactive. It has the capability to adapt, cooperate and move intelligently from one location to the other in the communication network [16].

Fuzzy logic is preferred to solve a problem by using reasonable computational power and time. It uses heuristic method to provide a satisfying solution [17]. It is a widely deployed technology for developing sophisticated control systems. It also provides a simple way to get definite precise conclusion and solutions based on unclear, imprecise, ambiguous or missing input information [18].

In this paper, we propose a Fuzzy and Swarm based distributed intrusion detection system authenticated routing for MANET.

2. RELATED WORK

Sureyya Mutlu and Guray Yilmaz [2] have introduced an intrusion detection framework for MANETs based on trust relationship. In the proposed framework, intrusion detection system relied on local and global determination of attacks within network. It is carried out in a distributed fashion with cooperation among nodes. An intrusion detection alert message is distributed throughout the network to report the anomaly. The reputation of intrusion detection alert messages is used for trust assessment. The proposed framework utilizes a distributed and cooperative trust based intrusion detection system to cope with the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

disadvantages drawn from mobility of nodes and the probability of selfishness, which are unique to MANETs.

James Cannady [5] has presented a new approach for the detection of attacks in MANETs. They also described the latest results of a research program that is designed to enhance the security of wireless mobile ad hoc networks (MANET) by developing a distributed intrusion detection capability. The current approach used learning vector quantization neural networks. It has the ability to identify patterns of network attacks in a distributed manner. This capability enables the proposed approach to demonstrate a distributed analysis functionality which facilitates the detection of complex attacks against MANETs.

Aikaterini Mitrokotsa1 et al [6] have presented an intrusion detection engine that is part of a local IDS agent in every node of a MANET. The collaboration of all the local IDS agents composes an IDS for MANET. The proposed intrusion detection engine is based on emergent SOMs a special and efficient class of neural networks that generates as an output a map. It also provided visual representation of the classification performed. They exploited the advantage of visualizing the network traffic and examined how eSOM performed in classifying normal and attack behavior in MANET based on MAC layer features. They also exploited the advantage of visualizing network traffic

Shengrong Bu et al [10] have presented a distributed scheme of combining authentication and intrusion detection. In the proposed scheme, the most suitable biosensor (for biometric-based authentication) or IDS is dynamically selected based on the current security posture and energy states. The problem was formulated as a stochastic multi-armed bandit problem, and its optimal policy can be chosen using Gittins indices. It also presented astructural results method for computing the Gittins index.

Rainer Bye et al [11] used techniques from design theory to provide multi-path peer-to-peer communication scheme. Here the adversary can not perform better than guessing randomly the originator of an alert message. They investigated related research on CIDS to identify the common building blocks and to understand vulnerabilities of the Collaborative Intrusion Detection Framework (CIDF). They also focused on the problem of anonymity preservation in a decentralized intrusion detection related message exchange scheme.

Kyriakos Manousakis et al [12] have introduced an active maintenance mechanism that is distributed utilizing one hop information. The mechanism focused on the maintenance of optimally formed tree ID structures, utilized for the collection and processing of ID data. The maintenance is called active, as opposed to the existing passive maintenance mechanisms, which are triggered only when the feasibility (e.g. connectivity) of the ID structures is violated, because continuously the participating nodes monitor their neighborhood characteristics that are related to the ID structures design objectives and take restructuring decisions so that the quality (design objectives) of the ID structures is maintained.

Mouhannad Alattar et al [13] proposed a distributed intrusion detection system that analyses activity logs so as to generate the rules which are used to detect intrusion. The proposed system correlates information found in the multiple traces provided by surrounding devices to deal with the distributed nature of an ad hoc network. The performance is further evaluated, in terms of e.g., intruder detection rate and false positive.

3. PROPOSED SOLUTION

3.1 Overview

In this paper, we propose a fuzzy based detection and swarm based authenticated routing technique in MANET. In this technique, the attacker levels of each node in the network layers are estimated using fuzzy logic technique. Based on the attacker level, the trust value of the nodes is updated. When a node wants to transmit a data packet to the destination node, the route with trustworthy nodes is selected using swarm based ant colony optimization (ACO) technique. This ensures the secured data communication.

3.2 Fuzzy Based Intrusion Detection

This technique involves the detection of attacker levels in the network layers using Fuzzy logic technique. The steps that determine the fuzzy rule based interference are as follows.

- **Fuzzification:** This involves obtaining the crisp inputs from the selected input variables and estimating the degree to which the inputs belong to each of the suitable fuzzy set.
- **Rule Evaluation:** The fuzzified inputs are taken and applied to the antecedents of the fuzzy rules. It is then applied to the consequent membership function.

Journal of Theoretical and Applied Information Technology
31st May 2014. Vol. 63 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- **Aggregation of the rule outputs:** This involves merging of the output of all rules.
- **Defuzzification:** The merged output of the aggregate output fuzzy set is the input for the defuzzification process and a single crisp number is obtained as output.

Initially, the fuzzy logic engine analyzes each layer namely the MAC layer, physical layer, routing layer for the detection of abnormal behaviors. Then the information gathered are stored in an attack database whose format is shown in table 1.

Table -1 Attack Database

Layer	Intrusion Frequency (F)	Probability of successful attack (P)	Severity (S)
MAC Layer	F_1	P_1	S_1
Physical Layer	F_2	P_2	S_2
Routing Layer	F_3	P_3	S_3

The parameters in the above table are briefly described below

Intrusion frequency (F): It is defined as the attack intensity against the layer that is subject to monitoring. Its unit is attacks/ unit time.

Probability for successful attack (P): It describes the method by which the attacker tackles to overcome the proactive controls. It value ranges from (0-1).

Severity(S): It describes the impact of an attack on the layer.

The fuzzy inference system is illustrated using fig 1.

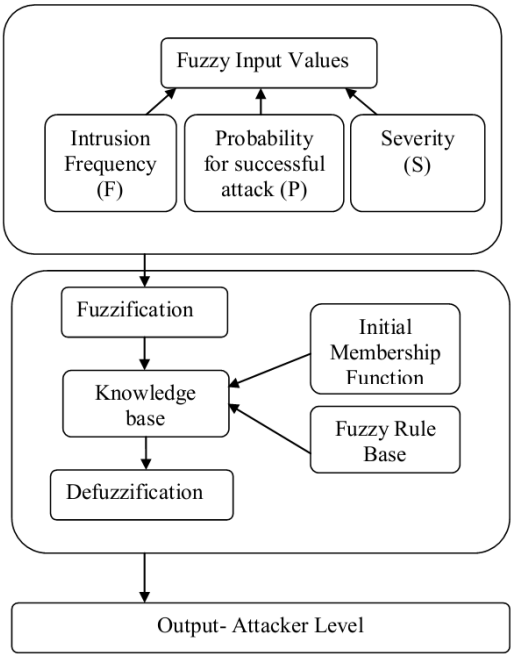

Fig 1 Fuzzy Interference System

Fuzzification

This involves fuzzification of input variables such as intrusion frequency (F), probability of successful attack (P) and severity (S) and these inputs are given a degree to appropriate fuzzy sets. The crisp inputs are combination of F, P and S. We take two possibilities, high and low for F, P and S.

Figures 2, 3, 4, and 5 show the membership function for the input and output variables. Due to the computational efficiency and uncomplicated formulas, the triangulation functions are utilized which are widely utilized in real-time applications. Also a positive impact is offered by this design of membership function.

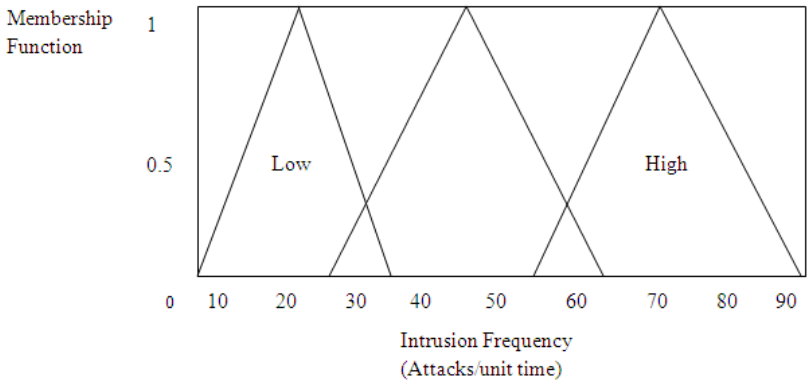

Fig 2 Membership Function Of Intrusion Frequency

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

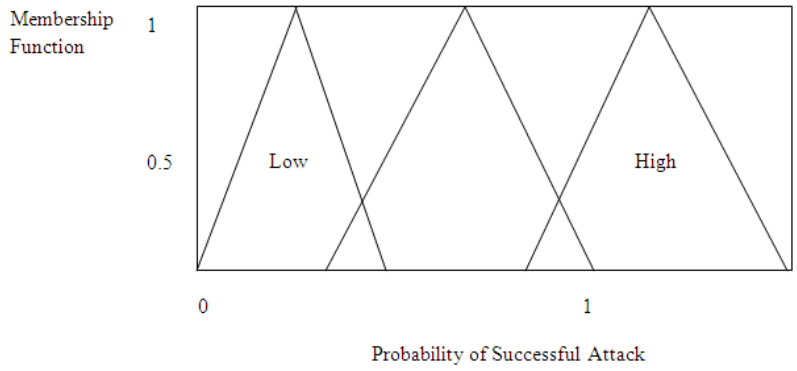

Fig 3 Membership Function Of Successful Attack Probability

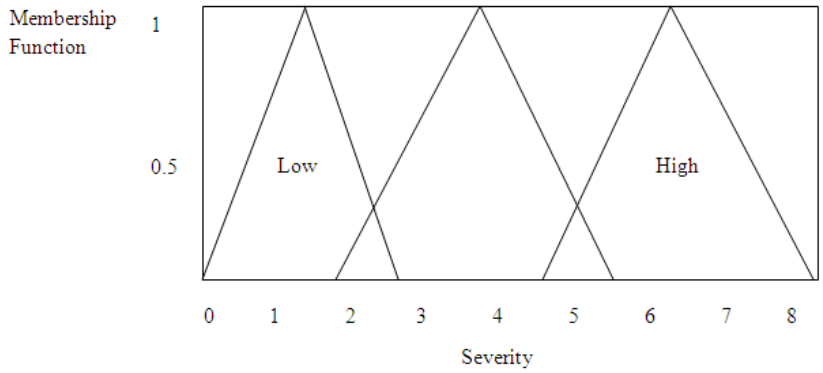

Fig 4 Membership Function Of Severity

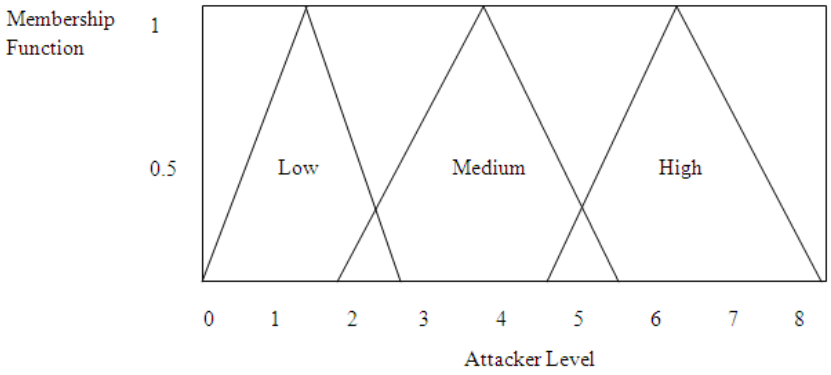

Fig 5 Membership Function Of Attacker Level

In table 2, F, P and S are given as inputs and the output represents the level of attacker (AL) in each node in the respective layer. Based on the attacker level, the trust value of malicious node is reduced (Explained in section 3.3). The eight fuzzy sets are defined with the combinations presented in table 2.

Table 2: Fuzzy Rules For The Determining Output

S.No	F	P	S	AL
1.	Low	Low	Low	Low
2.	Low	Low	High	Medium
3.	Low	High	Low	Medium
4.	Low	High	High	High
5.	High	Low	Low	Medium
6.	High	Low	High	High
7.	High	High	Low	High
8.	High	High	High	High

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2 demonstrates the designed fuzzy inference system. This illustrates the function of the inference engine and method by which the outputs of each rule are combined to generate the fuzzy decision.

If F, P and S are low, then the attack level is low

If F and P are low, S is high, then the attack level is medium

If F and S are low, P is high, then the attack level is medium

If F is low, P and S are high, then the attack level is high

If F is high, P and S are low, then the attack level is medium

If F and S are high, P is low, then the attack level is high

If F and P are high, S is low, then the attack level is high

If F, P and S are high, then the attack level is high

Defuzzification

The technique by which a crisp values is extracted from a fuzzy set as a representation value is referred to as defuzzification. The centroid of area scheme is taken into consideration for defuzzification during fuzzy decision making process. The formula (1) describes the defuzzifier method.

$$\text{Fuzzy\_cost} = [\sum_{allrules} z_i * \lambda(z_i)] / [\sum_{allrules} \lambda(z_i)] \quad (1)$$

Where fuzzy_cost is used to specify the degree of decision making, z_i is the fuzzy all rules, and variable and $\lambda(z_i)$ is its membership function. The output of the fuzzy cost function is modified to crisp value as per this defuzzification method. [11]

3.3 Maintaining Trust Value of the node based on attack detection

We consider that each node maintains an initial trust value (T_i). Based on the attacker level detected, the trust value of respective malicious nodes is decreased by the factor α_i (where i = 1, 2, 3, 4,…., n) which is illustrated in following three cases:

Case 1:
If AL = Low
Then T_i is reduced by the factor, $\alpha_i = \alpha_1 > 0$
End if

Case 2
If AL = Medium
Then
T_i is reduced by the factor, $\alpha_i = \alpha_2 > \alpha_1 > 0$
End if

Case 3
If AL = High
Then
T_i is reduced by the factor, $\alpha_i = \alpha_3 > \alpha_2 > \alpha_1 > 0$
End if

3.4 Swarm Based Authenticated Routing

In this technique, we consider swarm intelligence based on ant colony optimization (ACO) technique for performing authenticated routing. This process involves two ant agent namely forward ant (FA) and backward ant (BA).

The steps involved in this algorithm are as follows.

Step 1
When source (S) wants to transmit the data packet to destination (D), it launches FA with a threshold trust value (T_{th}) attached with it.

Step 2
The mobility of FA visiting each N_i is based on probabilistic decision rule (shown in Eq.1).

$$P_r(N_i,S) = \begin{cases} \frac{[a(N_i,S)]^{\zeta}.[b(N_i,S)]^{\sigma}}{\sum_{N_i \in N_R}[a(N_i,S)]^{\zeta}.[b(N_i,S)]^{\sigma}}, & \text{if r} \notin RT(N_i) \\ 0, otherwise \end{cases} \quad (2)$$

where $a(N_i,S)$ represent pheromone value

b (N_i, S_o) represent the bandwidth related heuristic value.

N_R represents the receiver node.

RT (N_i) represents the routing table for N_i.

ζ and σ are the parameters that control the relative weight of the pheromone and heuristic value respectively.

Step 3
FA moves through N_i utilizing the rule described in step 2, and verifies whether the trust value of the visited node is greater than the trust threshold value.

If $T_i > T_{th}$

Journal of Theoretical and Applied Information Technology
31st May 2014. Vol. 63 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Then

FA continues its path and keeps updating the routing table until it reaches D

Else if $T_i < T_{th}$

Then

The node is omitted from getting updated in the routing table.

End if

Step 4

Each FA deposits a quantity of pheromone ($\Delta\tau^u(r)$) in the visiting N_i as per the following equation

$$\Delta\tau^u(r) = 1/X_s^u(r) \quad (3)$$

where $X_s^u(r)$ represents the total number of N_i visited by FA during its tour at iteration r and u = 1, 2….n

Step 5

When FA reaches D, BA is generated and the entire information collected by FA is transferred to BA.

Step 6

The BA then takes the same path as that of its corresponding forward ant, but in the opposite direction. It updates the pheromone table with the trust value of the respective N_i.

Step 7

Once S receives the BA, it collects the routing information about all N_i along each path from its updated pheromone table.

Step 8

From the collected information, S chooses the route with trustworthy nodes for data communication.

Figure 1 shows the movement pattern of the ant agents and Figure 2 illustrates the discovery of the authenticated route.

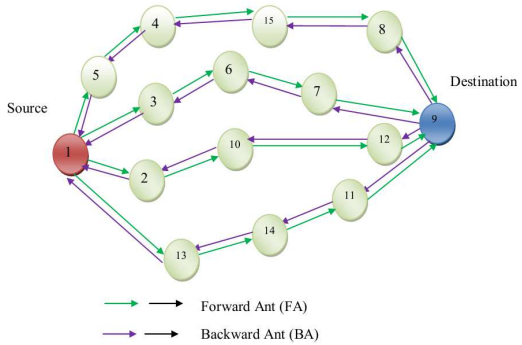

Fig 6 Movement of Forward and Backward Ant

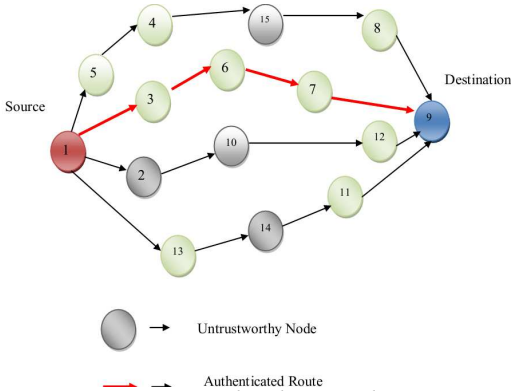

Fig 7 Swarm Based Authenticated Routing

Fig 7 demonstrates the swarm based authenticated routing. Path ($S\text{-}N_3\text{-}N_6\text{-}N_7\text{-}D$) devoid of untrustworthy nodes is selected as authenticated route for data transmission. The path with untrustworthy (malicious) nodes, N_2, N_{10}, N_{14} and N_{15} are rejected since it is not secured.

4. SIMULATION RESULTS

4.1 Simulation Model and Parameters

We use Network Simulator Version-2 (NS2) [19] to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. We have varied the number of nodes as 20, 40, 60, 80 and 100. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In our simulation, the node speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in table 3

Table 3: Simulation Settings

No. of Nodes	20, 40, 60, 80 and 100.
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	10m/s
No. Of Attackers	1,2,3,4 and 5.
Routing Protocol	FDSAR

4.2 Performance Metrics

Journal of Theoretical and Applied Information Technology
31st May 2014. Vol. 63 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

We evaluate mainly the performance according to the following metrics.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Average Packet Drop: It is the average number of packets dropped by the misbehaving nodes.

Throughput: It is the number of packets received by the receiver.

We compare our Fuzzy Based Detection and Swarm Based Authenticated Routing (FDSAR) with the DIstributed Cooperative Trust-based Intrusion Detection System (DICOTIDS) [2].

4.3 Results

A. Based On Attackers

In the first experiment, we vary the number of attackers as 1, 2, 3, 4 and 5.

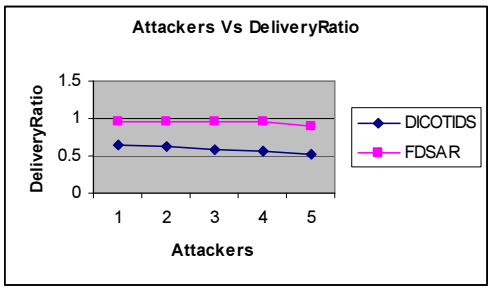

Fig 8 Attackers Vs Delivery Ratio

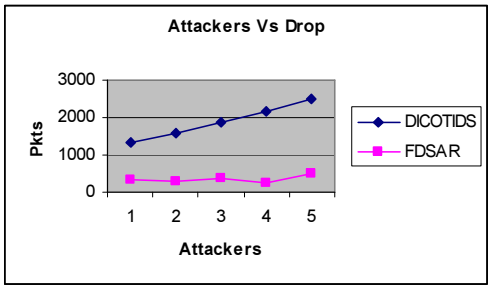

Fig 9 Attackers Vs Drop

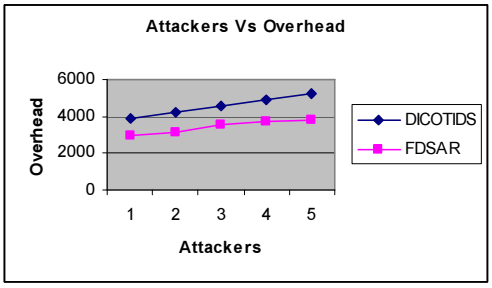

Fig 10 Attackers Vs Overhead

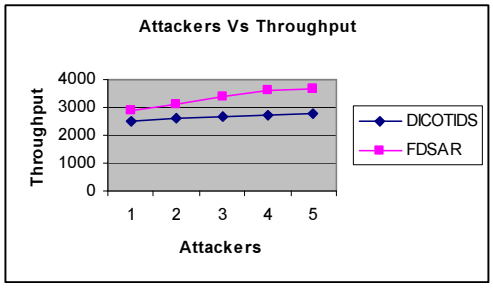

Fig 11 Attackers Vs Throughput

From figure 8, we can see that the delivery ratio of our proposed FDSAR is higher than the existing DICOTIDS protocol.

From figure 9, we can see that the packet drop of our proposed FDSAR is less than the existing DICOTIDS protocol.

From figure 10, we can see that the overhead of our proposed FDSAR is less than the existing DICOTIDS protocol.

From figure 11, we can see that the throughput of our proposed FDSAR is higher than the existing DICOTIDS protocol.

B. Based on Nodes

In our second experiment we vary the number of nodes as 20,40,60,80 and 100.

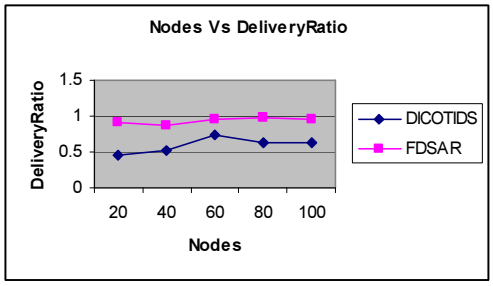

Fig 12 Nodes Vs Delivery Ratio

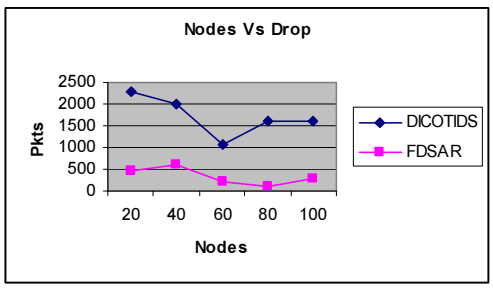

Fig 13 Nodes Vs Drop

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

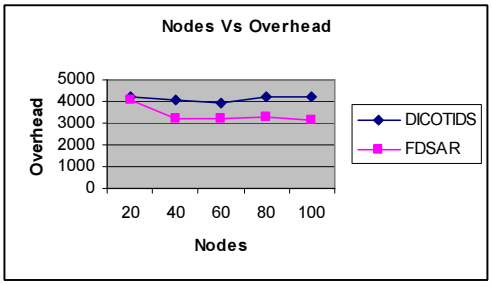

Fig 14: Nodes Vs Overhead

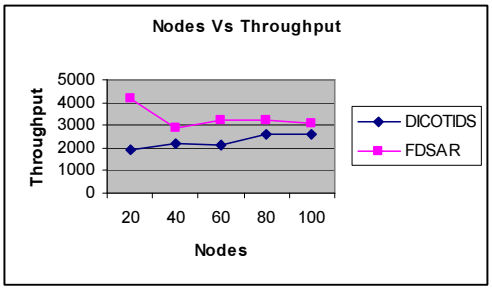

Fig 15: Nodes Vs Throughput

From figure 12, we can see that the delivery ratio of our proposed FDSAR is higher than the existing DICOTIDS protocol.

From figure 13, we can see that the packet drop of our proposed FDSAR is less than the existing DICOTIDS protocol.

From figure 14, we can see that the overhead of our proposed FDSAR is less than the existing DICOTIDS protocol.

From figure 15, we can see that the throughput of our proposed FDSAR is higher than the existing DICOTIDS protocol.

5. CONCLUSION

In this paper, we have proposed a combined approach named as fuzzy based detection and swarm based authenticated routing in MANET. This technique involves the detection of attacker level of the nodes in the network layers such as MAC layer, physical layer and routing layer using fuzzy logic technique. Based on the detected attacker level, the trust value of each node is updated. When source node wants to transmit a data packet to the destination, the route with trustworthy nodes is selected using swarm based ant colony optimization (ACO) technique. By simulation results, we have shown that proposed technique enhances the secured data communication.

REFERENCES:

[1] Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi, "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes", *World Academy of Science, Engineering and Technology*, pp.351-355, 2008.

[2] Sureyya Mutlu and Guray Yilmaz, "A Distributed Cooperative Trust Based Intrusion Detection Framework for MANETs", pp.292-298, 2011.

[3] S.S.Chopade and N.N.Mhala, "A Co-Operative Intrusion Detection System in Mobile Ad-Hoc Network", *International Journal of Computer Applications*, Vol. 18, No.6, pp.34-39, March 2011.

[4] S. Mangai and A.Tamilarasi, "An Improved Location aided Cluster Based Routing Protocol with Intrusion Detection System in Mobile Ad Hoc Networks", *Journal of Computer Science*, Vol.7,Iss no. 4, 505-511, 2011.

[5] James Cannady," DYNAMIC NEURAL NETWORKS IN THE DETECTION OF DISTRIBUTED ATTACKS IN MOBILE AD-HOC NETWORKS", *International Journal of Network Security & Its Application (IJNSA),* Vol.2, No.1, Jan.2010.

[6] Aikaterini Mitrokotsa1, Nikos Komninos2, and Christos Douligeris, " Protection of an Intrusion Detection Engine with Watermarking in Ad Hoc Networks", *International Journal of Network Security*, Vol.10, No.2, PP.93–106, Mar. 2010.

[7] Sevil Sen and John A. Clark, "A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad Hoc Networks", 2009.

[8] Farhan Abdel-Fattah, Zulkhairi Md. Dahalin, Shaidah Jusoh, "Distributed and Cooperative Hierarchical Intrusion Detection on MANETs", *International Journal of Computer Applications*, Vol. 12, No.5,pp. 32-40, Dec2010.

[9] Madjid Khalilian, Norwati Mustapha, Md Nasir Sulaiman, Ali Mamat, "Intrusion Detection System with Data Mining Approach: A Review", *Global Journal of Computer Science and Technology*, Volume 11 Issue 5 Version 1.0 April 2011

[10] Shengrong Bu, F. Richard Yu, Peter X. Liu and Helen Tang, "A Computationally Efficient Method for Joint Authentication and Intrusion Detection in Mobile Ad-hoc Networks",2011.

[11] Rainer Bye and Seyit Ahmet Camtepe, Sahin Albayrak "Collaborative Intrusion Detection

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Framework:Characteristics, Adversarial Opportunities and Countermeasures", *International conference on Collaborative methods for security and privacy*, 2010

[12] Kyriakos Manousakis, Dan Sterne, Geoff Lawler, Natalie Ivanic, "Distributed Active Maintenance for Intrusion Detection Structures", *Military Communication conference,* pp 1038 – 1043, 2010.

[13] Mouhannad Alattar, Francoise Sailhan, Julien Bourgeois, "Modeling and Detecting Intrusions in ad hoc Network Routing Protocols", *3SL Workshop, RENPAR, SYMPA, CFSE conferences,* 2011.

[14] Muhammad Saleem, Gianni A. Di Caro, Muddassar Farooq, "Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions", pp.1-28, 2010.

[15] ShabanaMehfuz and M. N. Doja, "Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs", *Journal of Artificial Evolution and Applications*,pp. 1-16,2008.

[16] I. Kassabalidis, M.A. El-Sharkawi, R.J.Marks II, P. Arabshahi, A.A. Gray, "Swarm Intelligence for Routing in Communication Networks", *IEEE Global Telecommunications Conference (GLOBECOM)*, 2001.

[17] Kjetil Haslum, Ajith Abraham and Svein Knapskog, "Fuzzy Online Risk Assessment for Distributed Intrusion Prediction and Prevention Systems", *Proceeding of the Tenth International Conference on Computer Modeling and Simulation (UKSIM)*, pp 216-223, 2008.

[18] Wassim El-Hajj, Fadi Aloul, Zouheir Trabelsi, "On Detecting Port Scanning using Fuzzy Based Intrusion Detection System", *International wireless Communications and Mobile Computing Conference* (IWCMC), 2008.

[19] Network Simulator: http:///www.isi.edu/nsnam/ns