IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Detection of Sink Hole Attack Using Decision Tree in Manet

Rohit.Wandra[1*], Parveen Kumar[2], Anita Suman[3]

[1,2,3]Dept. of Electronics and Communication Engineering, B.C.E.T, Gurdaspur, India

[*]*Corresponding Author: acp.rohit@gmail.com, Tel.: 7009929280*

DOI: https://doi.org/10.26438/ijcse/v7i3.297302 | Available online at: www.ijcseonline.org

Accepted: 17/Mar/2019, Published: 31/Mar/2019

***Abstract*—** Mobile Ad-hoc network (MANET) is an ad-hoc wireless network with a routing network background typically located at the top of a link layer of the network. For the transmission of data routing protocols plays an essential role. Since the topology in MANET is not stable (nodes are moving) therefore routing as well as maintenance of the network is a challenging task. The difficulty that most of the researchers have analyzed is the energy consumed by the sensor nodes. The first problem of this research is to find a trust-based route so that the network can be protected against any additional cost used during the searching of an appropriate node. For this purpose, the Zone Routing Protocol (ZRP) routing mechanism with the concept of Artificial Bee Colony (ABC) algorithm has been used. Another problem that has been considered in this research is to protect the network from external attacks named as sinkhole attack. These attacks are also known as smart attack, as, when these attacks came into the network the sensor nodes do not know that whether the data is transmitted to the genuine node or to the malicious node. Therefore to resolve this problem, machine learning approach named as decision tree is used. The performance parameters are evaluated to measure the efficiency of the network. It has been determine that the Packet Delivery Ratio (PDR) of the proposed system has been increased by 1.19% compared to the existing work.

***Keywords*—** MANET, OLSR, ABC, Decision tree, sinkhole attack.

I. INTRODUCTION

During previous years, Mobile Ad Hoc Network (MANET) has gained immense attention of researchers. The theory of MANET is dependent on the available devices that are linked to each other to form the network [1]. It is different from other existing or traditional networks. MANET is not dependent on any pre-existing network or infrastructure to carry out their actions. The dynamic nature of MANET reduces its cost and implementation time. The fundamental structure of Mobile Ad Hoc Networks is illustrated in Figure 1. The routing protocols that enable multi-hop data transfer in these networks form the backbone of MANET. The attacks on these networks change with the change in the topology of these dynamic networks [2]. To deal with such malicious attacks the routing protocols must be powerful. The routing protocols easily deal with varying topologies but the malicious attacks remain the concern to be fixed. By evaluating the performance of MANET, the application that it supports can be identified. Network layer parameters can be defined as the network performance metrics that are analyzed and evaluated in this research [3].

The architecture of MANET is depicted in figure 1, which comprises of four clusters each consisting of a gateway cluster head represented by a red circle. The cluster head is responsible for communicating with different nodes within the network. The ordinary that is placed randomly in the network is represented by the white circle, whereas source and destination nodes are represented by orange and green colour respectively.

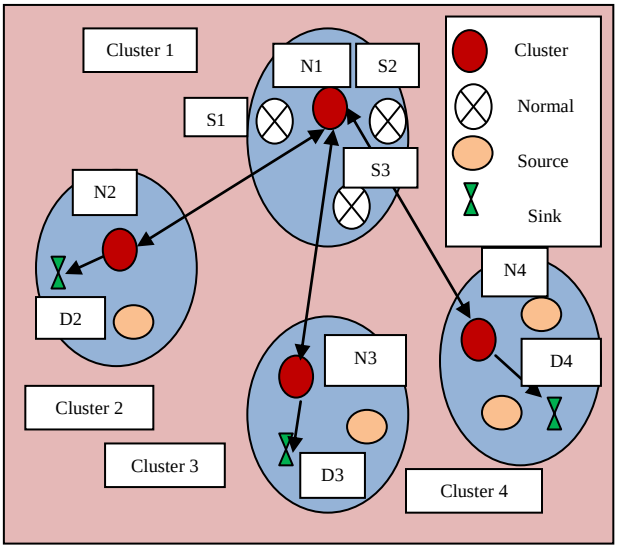

Figure 1. The architecture of MANET [4]

Therefore, whenever the node wants to transmit data, a request id sends to the cluster head, if the destination node

present in the same cluster then the data is transmitted directly. In case of destination node present in the different cluster, then the data is transmitted from one cluster head to another cluster head and then to the destination node [5].

A. Routing protocols in MANET

In MANET, the route is creating by using routing protocols, mostly, three types of routing protocols are available in MANET named as a proactive, reactive and hybrid routing protocol. Proactive routing protocols employ a link-state routing mechanism that often floods information towards their neighbours. The proactive routing protocol maintains routing information and keeps the data up-to-date by swapping the data packet with its neighbours. The overhead occurs in proactive routing protocols are minimized by using reactive protocol. The distance-vector routing algorithm is used to sets the route to the destination node only when the node wants to transmit data. Hybrid is the combination of both reactive as well as a proactive routing mechanism. An example of hybrid routing is ZRP. In this research work, ZRP is used to find a route between the source and the destination node. The concept of ZRP is shown in figure 2.

The nodes in the network cover zone radius as presented in figure 2. In case, if the destination node lies within the source zone region then the routing is formed similar to the proactive routing algorithm. In case, if the destination node lies away from the source node zone then the route is created by using a reactive routing algorithm [6]. The properties of both proactive and reactive routing algorithms are combining and better explained in figure 2.

In figure 2, there are three zones created by the source node, node 10 and node 13 respectively. The source node (S) wants to send data to the destination node (N14). It broadcast a message to the border nodes depicted by black colour. The nodes on the border of zone region check the destination node in its routing table. Since node 14 is not in its zone region; therefore it repeats the border casting process. Node 2 finds the destination node address and hence, it sends a reply message to the source node in this way the process is repeated and the route is formed between the source node and a destination node. As there is no centralized security management system, these types of networks are vulnerable to sinkhole attack. This paper will discuss the ongoing communication problems with the sinkhole attack. Sinkhole attack is a major security problem in MANET, which occurs mostly on the network layer. The data is drawn from the adjacent junctions to the offshore edge, and then falsifies routing information that generates a node that knows the path to a particular node of the local network. So, the sinkhole tries to attract the entire network traffic. Therefore, it warns the data packet or the package is completely down. To overcome this problem an optimization algorithm (ABC) along with a classification algorithm (Decision Tree) has been used [7].

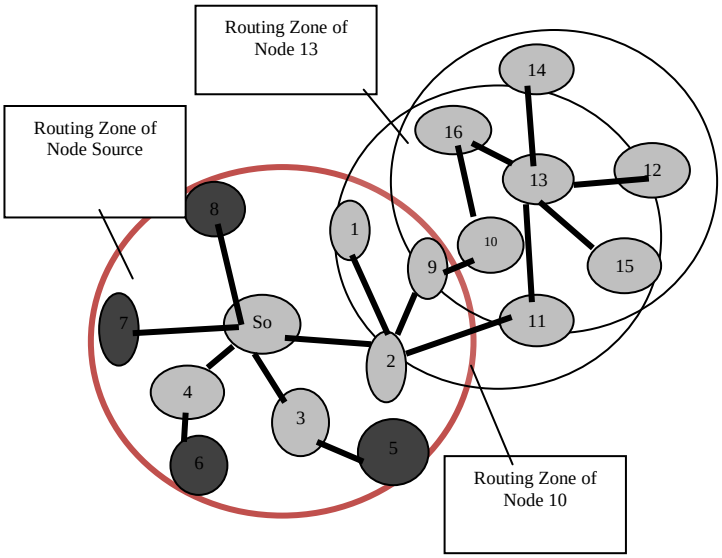

Figure 2: ZRP routing protocol [8]

Rest of the paper is organized as follows, Section I contains the introduction of MANET along with ZRP as a routing mechanism; Section II contains the related work of MANET. In Section III, the methods and technique used in the present work are discussed. Section IV contains the experimental results followed by conclusion and references.

II. RELATED WORK

A number of researchers have contributed to defending the network from different types of attack by utilizing different techniques. A state-of-art is provided in the table below:

Table 1. Existing work in MANET

Sr. no.	Authors & Year	Methods	findings
1	Patel et al., [2018]	Trust Value based Algorithm has been used in which the nodes form a group on the basis of energy consumption	The parameters such as throughput, packet delivery, routing performance and packet loss have been measured.
2	Zhang et al., [2015]	Proposed a cross-layer distributed algorithm for the minimization of delay.	From the experiment, it has been examined that the delay up to 34.8 % has been reduced while comparing

			the delay value measured with an individual AODV routing protocol.
3	Chatterjee et al., [2015]	Dynamic Source Routing (DSR) along with ant colony optimization (ACO) scheme has been used.	The PDR and delay up to 0.75 and 150ms have been achieved
4.	Jain et al., [2015]	AODV routing mechanism has been used	The black hole node has been detected and the performance of the network has been enhanced by 30 %.
5.	Chouhan et al., [2017]	Presented a modified AODV to prevent the network from wormhole attack	The parameters such as PDR, throughput, delay up to 80%, 60 % and 5msec have been measured with respect to the number of malicious nodes.
6.	Brar et al., [2017]	Particle swarm optimization (PSO) as an optimization mechanism to protect the network from the black hole attack.	System performance works well in the presence of a single black hole node and degraded as the number of malicious nodes appears in the network
7.	Gupta and J [2017]	Prevention of network from grey hole attack using PSO algorithm	The performance in terms of computed metrics such as throughput, delay and drop packet have been measured.
8	Jebadurai et al. [2018]	Node collision mechanism has been employed for the prevention of network from sinkhole attack	The PDR up to 0.85 has been obtained.

III. METHODS AND MATERIALS

In this section, the methods of proposed work used for preventing the network from sink hole attack by using ABC and Decision tree are presented.

A. Artificial Bee colony algorithm

It is a swarm inspired algorithm used to optimize the route on the basis of nodes properties such as energy consumption, collision rate and co-ordinate of the nodes. IF the energy consumed by the node is higher than the pre-defined value then the optimization algorithm with defined fitness function is applied in the network. This algorithm helps to create an optimized route [17]. The bees are mainly worked into three ways, initially, scout bees are used to discover route along with ZRP routing protocol. Secondly, the bees check the quality of the route and the last one is to integrate food from the sources [18].

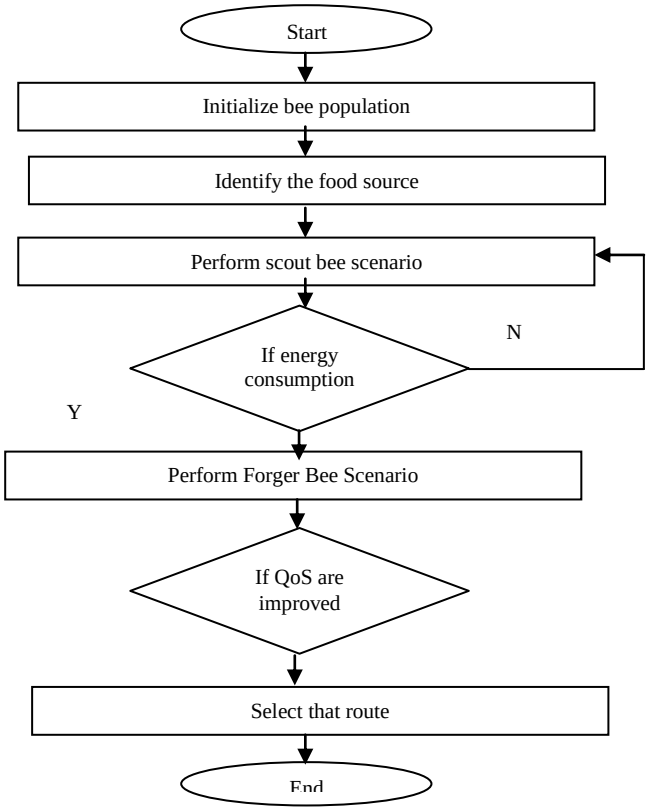

Figure 3. ABC algorithm

B. Decision Tree

Decision tree is used for differentiating the normal node from the sinkhole node. It is tree-like structure that utilizes possible results such as random results, resource costs, and utilities. If the route is discovered between the source and destination node then the attacker or intruder in the set route using the Decision Tree is checked and if attacker is

discovered then their identification in the cache routing table is stored. On the behalf of the attackers' activities, the types of attacker are checked and the presentations from the attacker are analyzed so that best results can be achieved. To check the accuracy and efficiency of the proposed simulation work, QoS parameters like Throughput, Delay, and Packet Delivery Ratio etc are computed [19].

IV. EXPERIMENTAL RESULTS

The experiment has been performed in the MATLAB tool by utilizing a communication tool along with an optimization and classification tool.

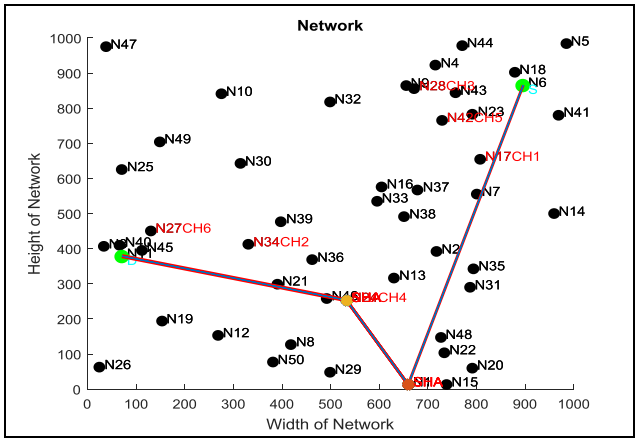

Figure 4. Network

Figure 4, shows the network designed with 1000 * 1000 areas. The network comprises of 50 numbers of nodes along with source node and the destination node. The route is determined by using the ZRP routing protocol as indicated by the blue line.

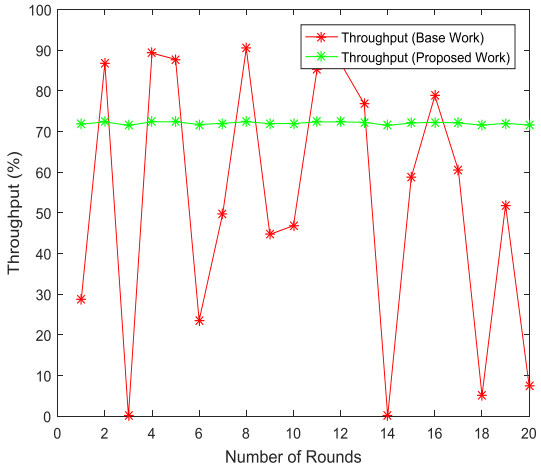

Figure 5. Throughput

The capacity of the network is determined via throughput. Here, throughput measured for the base work in which DSR has been used as a routing algorithm is represented by the red line. The throughput measured for the proposed work that utilized ZRP as a routing algorithm along with optimization and classification algorithm. There is an increment of 36.11% in the throughput while comparing with the existing work.

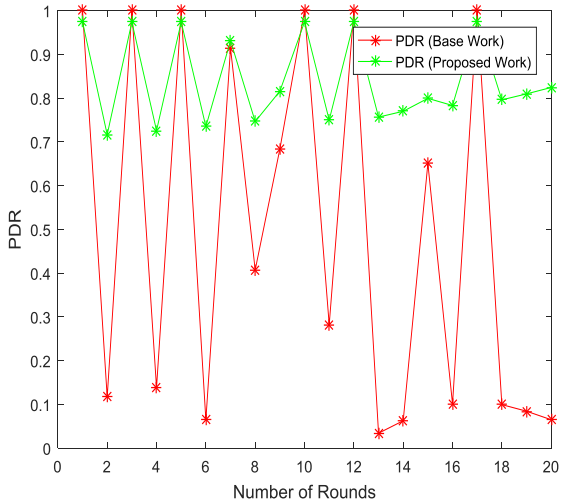

Figure 6.PDR

The PDR metric represents the rate of a number of packets delivered to the destination node with respect to the total data transmitted for the source node. From the graph, the PDR of the proposed work has been increased by 35.48 % compared to the existing work.

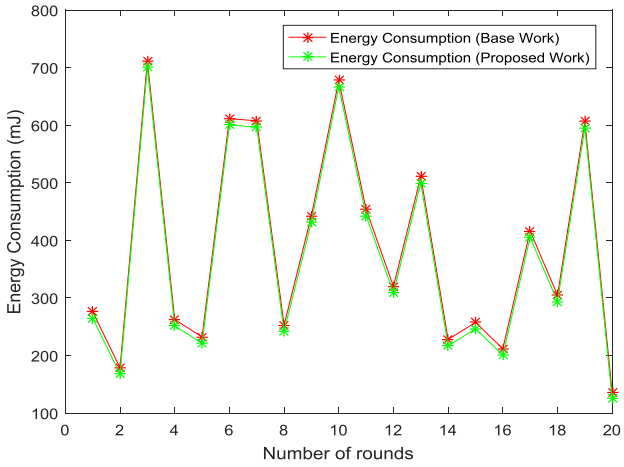

Figure 7. Energy consumption

Figure 7, represents the energy consumed by the sensor nodes while transmitting data from the source node to the destination node. From the figure, it is clear that the energy consumed by the nodes while using optimization along with classification algorithm is very small compared to the existing work. The energy consumption ratio of the proposed work has been reduced by 2.85 % compared to the existing work.

Delay is essential parameters because when it exists in the network, the sensor nodes relay messages and the network are populated.

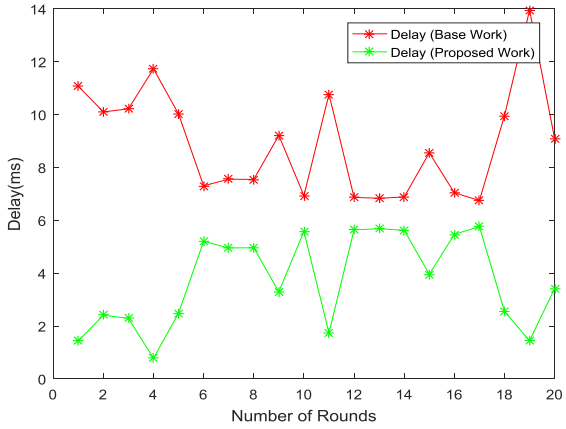

Figure 8. Delay

The delay has been reduced by 58 % of the existing work.
To determine the efficiency of the proposed work, the comparison between proposed work and existing work performed by **Jebadurai et al. [16]** has been illustrated in figure 9.

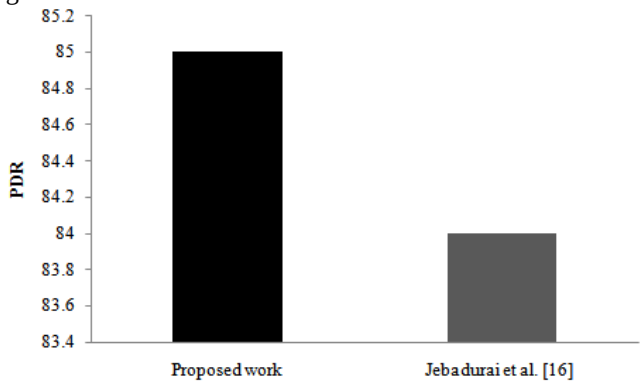

Figure 9 Comparison of PDR

It has been observed that the average values of PDR measured for the proposed and existing work are 85 % and 84 % respectively. Thus there is an enhancement of 1.19% respectively.

V. CONCLUSION

In this research, we are observing the effect of sinkhole attack in the network, which is deployed with 50 number of nodes. The routing has been performed by ZRP routing protocol. ZRP is a hybrid routing protocol that combines the advantages of both proactive and reactive routing mechanism. The effect of sinkhole attack has been analyzed without using the artificial intelligence algorithm and with artificial intelligence algorithm. From the experiment, it has been observed that When there is no machine learning approach applied, the average of throughput, PDR, energy consumption and delay values measured for 5 number of iterations are 42%, 0.51, 460 mJ and 3 msec and 58.13 % respectively have been measured.

In the case of machine learning and optimization approach, the sinkhole attack is detected and the path of data transmission has been changed from the fake route to the genuine route. In this process, the performance of the network has been increased and the increased values of throughput and PDR are 35.48 % and 48.72 % respectively. The energy consumption and delay values have been reduced by 2.85 % and 58 % respectively. Also, in comparison to existing work PDR value is increased by 1.19%.

REFERENCES

[1] K. Agarwal, LK. Awasthi, "Enhanced AODV routing protocol for ad hoc networks," InNetworks, ICON, 16th IEEE International Conference, pp. 1-5, 2008.

[2] A. Hinds, M. Ngulube, S. Zhu, H. Al-Aqrabi, "*A review of routing protocols for mobile ad-hoc networks (manet)*," International journal of information and education technology. Vol. 3, No.1, 2013.

[3] A. Al-Maashri, M. Ould-Khaoua, " Performance analysis of MANET routing protocols in the presence of self-similar traffic," InLocal Computer Networks, Proceedings 2006 31st IEEE Conference, pp. 801-807, 2006.

[4] A. Bagwari, & R. Jee, "*The Criteria Require for Cluster Head Gateway Selection in Integrated Mobile Ad hoc Network*," International Journal of Engineering Science and Technology (IJEST), 2011.

[5] A. Khandakar, " *Step by Step Procedural Comparison of DSR, AODV and DSDV Routing protocol*," In International Proceedings of Computer Science & Information Tech , Vol. 40, No. 12, 2012.

[6] P. K. Sahu, B. Acharya, & N. Panda, "QoS Based Performance Analysis of AODV and DSR Routing Protocols in MANET," In 2018 2nd International Conference on Data Science and Business Analytics (ICDSBA), pp. 221-225, 2018.

[7] Y. Jahir, M. Atiquzzaman, H. Refai, A. Paranjothi, & P. G. LoPresti, "*Routing protocols and architecture for Disaster Area Network: A survey*," Ad Hoc Networks, Vol. 82, pp.1-14, 2019.

[8] Z. J. Haas, & M. R. Pearlman, "*The performance of query control schemes for the zone routing protocol*," IEEE/ACM Transactions on networking, Vol.9, no. 4, pp.427-438, 2001.

[9] N. J. K. Patel, & K. Tripathi, "*Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method*, International Journal of Scientific Research in Science, Engineering and Technology, Vol.4, Issue 4, pp. 281-287, 2018.

[10] X. M. Zhang, Y. Zhang, F. Yan, & A. V. Vasilakos, "*Interference-based topology control algorithm for delay-constrained mobile ad hoc networks*," IEEE Transactions on Mobile Computing, Vol. 14, No.4, pp.742-754, 2015.

[11] S. Chatterjee, & S. Das, "*Ant colony optimization based enhanced dynamic source routing algorithm for mobile Ad-hoc network*,". Information Sciences,Vol.295,pp. 67-90, 2015.

[12] A. K. Jain, & V. Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks," In Pervasive computing (ICPC), 2015 international conference, pp. 1-6, 2015.

[13] A. S. Chouhan, V. Sharma, U. Singh, & R. Sharma, "A modified AODV protocol to detect and prevent the wormhole usingh using hybrid technique," In Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference , Vol. 2, pp. 621-625, 2017.

[14] S. Brar, & M. Angurala, "*Cooperative Black Hole Attack Prevention by Particle Swarm Optimization with Multiple Swarms*," International Journal of Advanced Research in Computer and Communication Engineering, Vol.5, issue10, pp.424-429, 2017.

[15] J. Gupta, "Improved approach of co-operative gray hole attack prevention monitored by meta heuristic on MANET," In Signal Processing, Computing and Control (ISPCC), 2017 4th International Conference, pp. 356-361, 2017.

[16] I. J. Jebadurai, E. B. Rajsingh, & G. J. L. Paulraj, "*A Novel Node Collusion Method for Isolating Sinkhole Nodes in Mobile Ad Hoc Cloud*," In Advances in Big Data and Cloud Computing Springer, Singapore, pp. 319-329, 2018.

[17] R. Kalucha, & D. Goyal, "*A review on artificial bee colony in MANET*," International Journal Computer Science Mobile Comput.,Vol. 3, no.7, pp.34-40, 2014.

[18] P. Visu, J. Janet, E. Kannan, & S. Koteeswaran,, "*Optimal energy management in wireless adhoc network using Artificial Bee Colony based routing protocol*," European Journal of Scientific Research, Vol. 74, No. 2, pp.301-307, 2012.

[19] Y. Freund, & L. Mason, "*The alternating decision tree learning algorithm,*" In icml , Vol. 99, pp. 124-133, 1999.

