ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

Secure Collaborative Contact Based Watchdog for Detecting Selfish Nodes in MANET using Hash Chain Technique

Sonal Jitendra Patil

Student, Department of Computer Science, SSVPS BS Deore College of Engineering, Dhule, India.

Abstract: Mobile Ad hoc Network (MANET) is composed of mobile nodes which are connected by wireless links using without any pre-existing infrastructure. In network some nodes cooperate in order to work properly but some nodes not cooperate unwilling to forward packets to other nodes behave like selfish, leading to selfish node behavior. This leads to overall performance degradation. Watchdog detects selfish nodes it leads to wrong detection of false positive and false negative. More advanced technique is collaborative contact based watchdog technique based on diffusion of selfish node information when contact occurs but this approach doesn't provide security like node authentication. This paper proposed secure collaborative contact based watchdog using hash chain it provide security in network to giving node authentication and reduces the effect of malicious nodes.

Keywords: MANETs, Hash chain, Selfish nodes, watchdog, Authentication.

I. INTRODUCTION

Two of the basic technologies that are considered as the core for these types of networks are mobile ad-hoc networks (MANETs) and opportunistic and Delay Tolerant Networks (DTNs). The cooperation on these networks is usually contact based. Mobile nodes can directly communicate with each other if a contact occurs. Mobile Adhoc Network (MANET) has no centralized infrastructure like the base station to forward the packets to the destination and so the intermediate nodes forward the packet to the destination, the sender trusts the intermediate nodes for their packet delivery. MANETs and DTNs nodes must forward traffic unrelated to their own use. That is, these networks rely on network cooperation schemes to work properly. Nevertheless, in the real world, most nodes have a selfish behavior and are unwilling to forward packets for others. Additionally, some nodes can exhibit malicious behavior trying to disturb the normal network behavior, and others can be faulty nodes. In all the cases these misbehaving nodes will not cooperate in the transmission of packets. Therefore, detecting such nodes is essential for the overall network performance. Watchdogs are appropriate mechanisms to detect misbehaving and selfish nodes in computer networks. Essentially, watchdog systems overhear wireless traffic and analyses it to decide if the neighbors nodes are behaving in a selfish manner. Such selfish nodes do not consume any energy such as CPU power, battery and also bandwidth for retransmitting the data of other nodes and they reserve them only for themselves. There are two main strategies to deal with selfish nodes; first strategy tries to motivate nodes to actively participate in the forwarding activities. The second strategy detection and exclusion is a straight-forward way to cope with selfish nodes and several solutions have been presented. The impact of node selfishness on MANETs is shown that when no selfishness prevention mechanism is present, the packet delivery rates become seriously degraded. A more detailed study [3] shows that a moderate concentration of node selfishness has a huge impact on the overall performance of MANETs, such as the average hop count, the number of packets dropped, the offered throughput, and the probability of reachability. Detecting such nodes quickly and accurately is essential for the overall performance of the network. There are several techniques to deal with such selfish nodes a first study of misbehaving nodes and the proposal to use watchdogs to detect them was introduced in. This work proposed a Watchdog and Pathrater over the DSR protocol to detect non-forwarding nodes, maintaining a rating for every node. Watchdog systems overhear wireless traffic and analyses it to decide whether neighbor nodes are behaving in a selfish manner [4]. When the watchdog detects a selfish node it is marked as a positive detection (or a negative detection, if it is detected as a non-selfish node). Nevertheless, watchdogs can fail on this detection, generating false positives and false negatives that seriously degrade the behavior of the system. One harmful malicious node can be lying about the status of other nodes, producing a fast diffusion of false negatives or false positives. Malicious nodes are hard to detect using watchdogs, as they can intentionally participate in network communication with the only goal to hide their behavior from the network. Collaborative Contact-Based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. The diffusion of information about positive or negative detections of selfish nodes introduces several issues about the Reputation of the neighbor nodes. The first issue is the consolidation of information, that is, the trust about

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

neighbor's positive and negative detections, especially when it does not match with the local watchdog detection. Another issue is the case of malicious nodes. Regarding the diffusion of information on the network; our approach does not assume any security measures, such as message cyphering or node authentication. Nevertheless, if these measures exist, the effect of malicious nodes in CoCoWo will be very reduced or even non-existent. This paper introduce Secure collaborative contact based watchdog using hash chain can overcome the problem occur with CoCoWa. Hash chain provide security by node authentication also this paper include Dijkstra's algorithm it find shortest path between source to destination because of this time required is less. This approach reduces the time and increase precision also provides security while detecting selfish nodes. In this paper use one-way Hash function to update the key for each session after the communication has been established. Also, by changing the number of times the hash function executes, we can change the symmetric key for each session.

II. RELATED WORK

CoCoWa is combination of watchdog and dissemination of information. To reduce the detection time of selfish nodes based on contact dissemination. If one node has previously detected a selfish node using its watchdog it can spread this information to other nodes when a contact occurs. This way, nodes have second hand information about the selfish nodes in the network. The goal of our approach is to reduce the detection time and to improve the precision by reducing the effect of both false negatives and false positives.

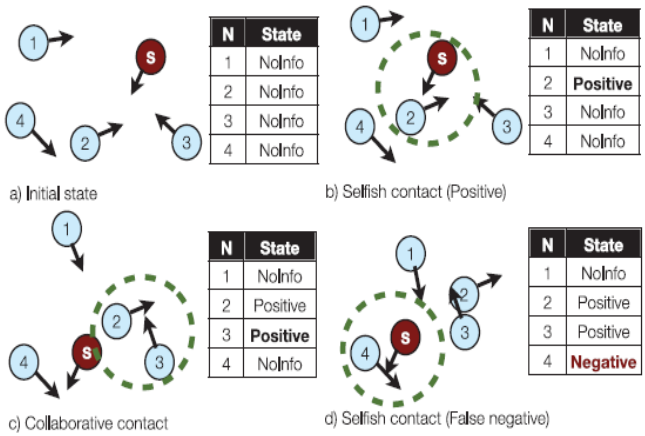

Fig.1. Example of CoCoWa

An example of how CoCoWa works is outlined in Fig. 1. It is based on the combination of a local watchdog and the diffusion of information when contact between pairs of nodes occurs. A contact is defined as an opportunity of transmission between a pair of nodes (that is, two nodes have enough time to communicate between them). Assuming that there is only one selfish node, the figure shows how initially no node has information about the selfish node. When a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non-selfish node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this information to it; so, from that moment on, both nodes store information about these positive (or negative) detections. Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly, through the collaborative transmission of information that is provided by other nodes. Under this scheme, the uncontrolled diffusion of positive and negative detections can produce the fast diffusion of wrong information, and therefore, a poor network performance. For example, in Fig.1, on the last state d), node two and three have a positive detection and node four has a negative detection (a false negative). Now, node one, which has no information about the selfish node, has several possibilities: if it contacts the selfish node it may be able to detect it; if it contacts node two or three it can get a positive detection; but if it contacts node four, it can get a false negative.

III. SYSTEM ARCHITECTURE

The Local Watchdog has two functions: the detection of selfish nodes and the detection of new contacts. The local watchdog can generate the following events about neighbor nodes: PosEvt (positive event) when the watchdog detects a selfish node, NegEvt (negative event) when the watchdog detects that a node is not selfish, and NoDetEvt (no detection event) when the watchdog does not have enough information about a node (for example if the contact time is very low or it does not overhear enough messages). The detection of new contacts is based on neighborhood packet overhearing; thus, when the watchdog overhears packets from a new node it is assumed to be a new contact, and so it generates an event to the network information module. The Diffusion module has two functions: the transmission as well as the reception of positive (and negative) detections. A key issue of our approach is the diffusion of information. As the number of selfish nodes is low compared to the total number of nodes, positive detections can always be transmitted

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

with a low overhead. However, transmitting only positive detections has a serious drawback: false positives can be spread over the network very fast. Thus, the transmission of negative detections is necessary to neutralise the effect of these false positives, but sending all known negative detections can be troublesome, producing excessive messaging or the fast diffusion of false negatives. Consequently, we introduce a negative diffusion factor γ , that is the ratio of negative detections that are actually transmitted.

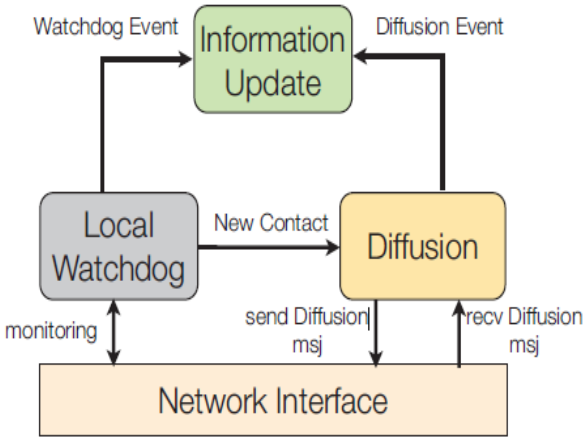

Fig.2. CoCoWa Architecture

Updating or consolidating the information is another key issue. This is the function of the Information Update module. A node can have the following internal information about other nodes: NoInfo state, Positive state and Negative state. A NoInfo state means that it has no information about a node; a Positive state means it believes that a node is selfish, and a Negative state means it believes that a node is not selfish. A node can have direct information (from the local watchdog) and indirect information (from neighbor nodes). CoCoWa is event driven, so the state of a node is updated when the PosEvt or NegEvt events are received from the local watchdog and diffusion modules.

IV. SYSTEM MODEL AND DATAFLOW DIAGRAM

The network is modeled as a set of N wireless mobile nodes, with C collaborative nodes, M malicious nodes and S selfish nodes (N = C + M + S). Our goal is to obtain the time and overhead that a set of D ≤ C nodes need to detect the selfish nodes in the network. The overhead is the number of information messages transmitted up to the detection time. Note that the following models evaluate the detection of a single selfish node. The effect of having several selfish nodes in a network is easy to evaluate, and it does not require a specific model. If we assume that selfish nodes are not cooperative, we can analyze the impact of each selfish node on the network independently. In the case of several selfish nodes (S > 1) on a network with N nodes, we can assume that there are C = N − S cooperative nodes. MANETs assumes that mobile nodes voluntary cooperate to work properly. This cooperation is a cost intensive activity and some nodes can refuse to cooperate, leading to the Selfish node behavior where sometimes watchdogs lack of enough time or information to detect the Selfish nodes. Thus, this paper propose a Secure collaborative contact-based watchdog (SCoCoWa) using hash chain provide security at the time packet transfer and it well detect the selfish node properly that is the effect of false positive and false negative. As shown in the paper, a collaborative approach reduces the time and increases the precision when detecting the Selfish nodes. The local watchdog is modeled using mainly and importantly with the three parameters which give detection mechanism three parameters: the probability of detection pd, the ratio of a false positives pfp and the ratio of a false negatives pfn. The first parameter, the probability of detection (pd), reflects the probability that, when a node contacts another node, the watchdog has enough information to generate a PosEvt or NegEvt event. This value depends on the effectiveness of the watchdog, the traffic load and the mobility pattern of nodes. In this Secure collaborative contact based watchdog system, provides keys to each and every node in the network. ID and Mac address will be assign to each and every node in network i.e. assign key to each node. The monitoring mechanism used here is hash chain mechanism which monitors all such nodes in the network and reports to the sender of misbehavior through acknowledgement as soon as the sender receives the ACK(acknowledgement) from the hash chain. It has to reroute to the different path which increases the precision when detecting the Selfish nodes. This paper propose a Secure collaborative contact-based watchdog (SCoCoWa) using hash chain technique, so that information about selfish is quickly propagated. Node authentication security is provide in network when contacts occurs in between nodes. As shown in the paper a secure collaborative approach reduces the effect of malicious nodes and increases the precision while detecting selfish nodes. Accurate detection of the Selfish nodes is avoiding both a false positive and false negatives. Precision and security is the main advantage if the secure Collaborative Contact Based Watchdog technique. This has been a serious disadvantage earlier which is overcome by this efficient technique SCOCOWA.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

Selfish Node detection

When sender will check the ID and Mac adresss at it find that hash value is different then it will be detected as attacker. Ack about this different in hash value is send to sender. Then again new shortest path will be search by dijkstra's algorithm and same packet will be send to the new alternate shortest path. The attacker list is stored in the database and when other contacts it, it sends the stored information to contact nodes that is Diffusion of information. Alternate path may or may not contain selfish node. If it does not contain any selfish node in the path, it forwards the packet to the correct destination. If it is the selfish node the alternate path is selected for sending the packet to the destination. Sender is sending the packet to the destination i.e. at receiver through alternate path which is shortest path when path contains any selfish node. The selfish node is detected through SCoCoWa mechanism which efficiently detects the selfishness by comparing Id and mac address of node in network after checking it generate hash value is check by sender if it is not in that range then mechanism decides that this is misbehaving node since the mechanism changes the node and transmit the packet through the new path. In every node, the watchdog mechanism works in the background and stores the positive and negative detection of the selfishness in the routing path. The already store information about another node behavior is transmitted when the node contact with sender node. This mechanism plays an important role in the correct delivery of information to the receiver without changing the content of packet. This gives security and confidentially of the information transmission in mobile Adhoc network where cooperation plays an important role in packet forwarding.

V. RESULT ANALYSIS

This Section is devoted to evaluate the performance of SCoCoWa. This paper is focus on the impact of False Positive and False Negative. The number of nodes should be consider during the evaluation are 40 (N= 40) and the number of selfish nodes are 5 (S= 5). Parameter used for this evaluation is shown in table.

Table I: The Parameter Setup

Simulation Parameter	Value
Simulator	Glomosim
Number of nodes	40
Number of Selfish Nodes	05
Topology	Random
Network Area	2000 X 2000
Queue type	Priority Queue
Routing protocol	AODV
Application agent	CBR
Transmission range	250m
Simulation time	100sec

a. Effect of False positive and false negative is more in CoCoWa. In Secure CoCoWa, as node authentication is provided, every time the information database table of node is updated after collaboration therefore the impact of false positive and False negative is less in SCoCoWa.

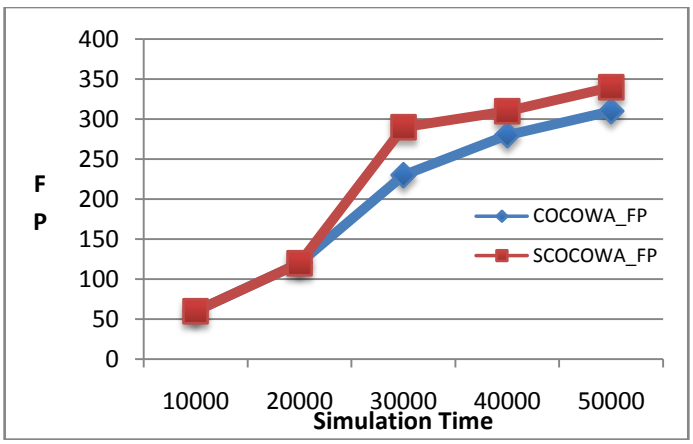

Fig.3. Comparsion graph for False positive of CoCoWa and SCoCoWa.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

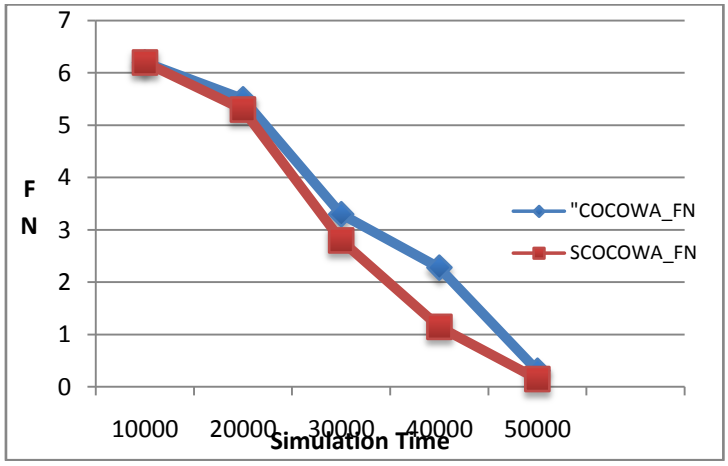

Fig.4 Comparison graph for False Negative of CoCoWa and SCoCoWa.

b. Throughput: Amount of data transfer successfully from source to destination in a given time period. No of messages transfer unit time are more in secure CoCoWa.as node authentication is provided by this technique risk of to forward packet to attacker node is decrease therefore no of packets send in per unit time are more.

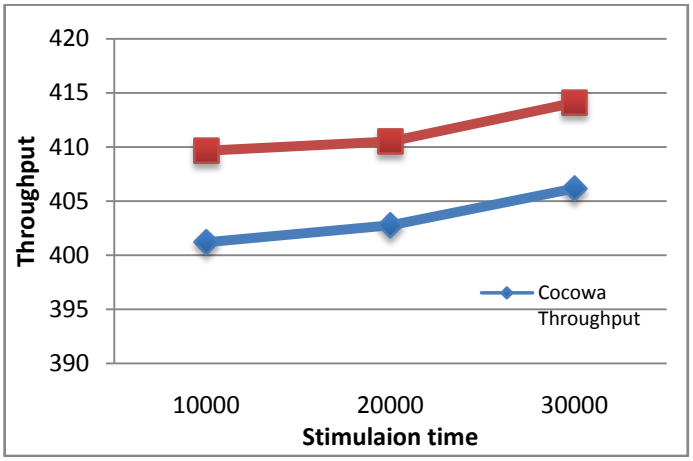

Fig.5. Comparison graph for Throughput of CoCoWa and SCoCoWa.

c. Packet Delivery Ratio: Ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by sender. The packet delivery ratio is increase when maximum no of nodes reach to its destination. In Secure CoCoWa as authentication provides so its reach at destination. PDR is increase in SCoCoWa.

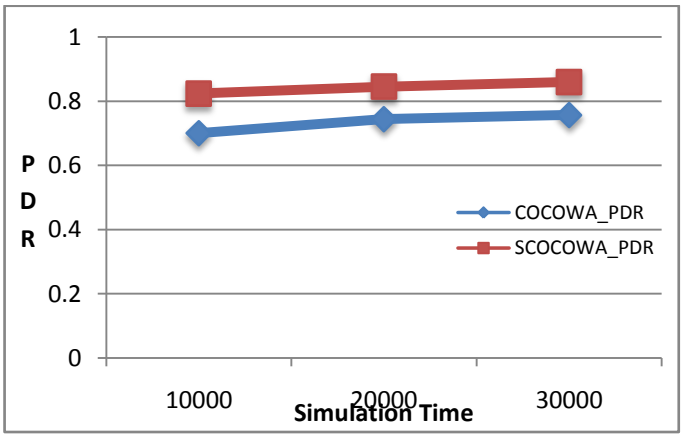

Fig.6. Comparison graph for PDR of CoCoWa and SCoCoWa

d. Delay: The delay of a network is specified that how long it takes for bit of data to travel across the network from source node to destination node. In CoCoWa Delay is more because sometime information about selfish node is

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

not properly disseminate in network. As well as there is no security scheme for malicious node. This all problems will overcome in SCoCoWa so delay is less as compare to CoCoWa.

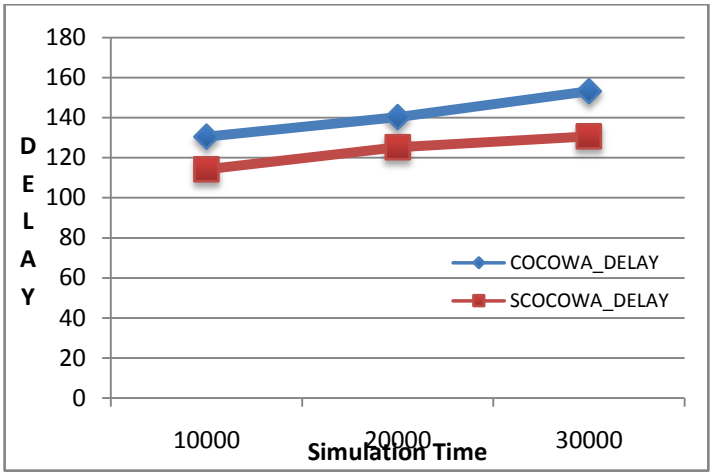

Fig.7. Comparison graph for Delay of CoCoWa and SCoCoWa

e. Routing Overhead: Overhead is any combination of excess or indirect compution time, memory, bandwidth or other resources that are required to perform a specific task. In SCoCoWa slightly decreases as compare to CoCoWa.

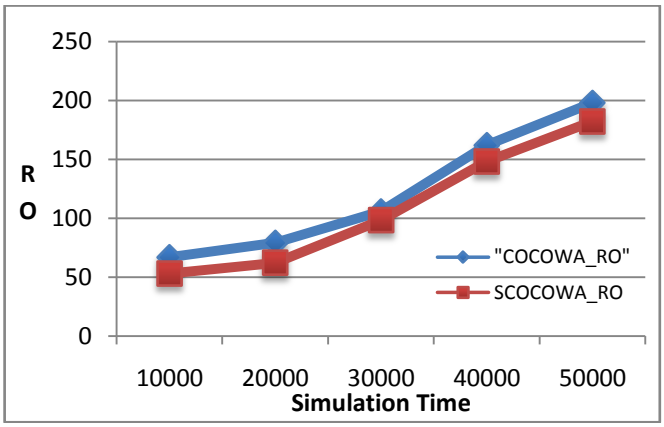

Fig.8. Comparison graph for RO of CoCoWa and SCoCoWa

VI. CONCLUSION

This paper proposes the secure collaborative contact based watchdog technique to detect selfish node accurately and decrease the effect of malicious nodes. Also provide authentication while sending the packets. Thus it increase precision and effect of malicious nodes and increase the accuracy. Secure collaborative Contact based watchdog using hash chain reduces the harmful effect of false negative and malicious nodes. SCoCoWa is provide authentication when contact occurs between the two collaborative nodes and also find shortest path to reach at destination. It isolates the selfish nodes in network as well as provide security during transmission this improves the performance.

REFERENCES

[1]"CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes," IEEE TRANSACTIONS ON MOBILE COMPUTING, vol. 14, no. 06, pp. 1162-1175, June 2015.
[2]Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni Enrique Hern´andez-Orallo, "Improving Selfish Node Detection in MANETs Using a Collaborative Watchdog," IEEE COMMUNICATIONS LETTERS, vol. 16, no. 5, pp. 642-646, MAY 2012.
[3]C. K. N. Shailender Gupta and C. Singla, "“Impact of selfish node concentration in MANETs," Int. J. Wireless Mobile Netw, vol. 3, no. 2, pp. 29-37, apr 2011.
[4]Laurence T. Yang Sajid Hussain and Md Shafayat Rahman, "Key Predistribution Scheme using Keyed-Hash Chain and Multipath Key Reinforcement for Wireless Sensor Networks,".

BIOGRAPHY

Sonal J.Patil Pursuing Bachelor of engineering in computer science from SSVPSBS Deore college of Engg, Dhule (North Maharashtra University).