A Novel Framework for Prevent The Denial Of Service Attacks in MANET

Prof. M. Anandhi
Department of Computer Science
Cauvery College for Women
Trichy, Tamilnadu, India
manandhi.cs@gmail.com

Prof. Dr. T. N. Ravi
Department of Computer Science
Periyar E.V.R College (Autonomous)
Trichy, Tamilnadu, India

Abstract— In the field of networks, the Mobile ad hoc networks (MANETs) are one of the best and lively mobile networks which are capable of shaping when the infrastructure of pre-existing communication is not present. And in further to mobility, the restricted resources like storage space, bandwidth and battery power are used to categorize a MANET. The primary theory in MANETs is that the transitional nodes assist in forwarding the packets. Mobile Ad hoc Networks are very weak in terms of Denial of Service (DoS) because of their prominent characteristics. A MANET is a self-diagnostic model that includes multiple mobile wireless nodes. The node misbehaviour is due to egocentric reasons where it can considerably reduce the performance of MANET. A self-centred node endeavours to exploit the resources simply for its own intention and it hesitates to distribute the resources with their neighbours. As a result, it plays a vital role to detect the self-centred nodes to progress the concert of MANET. Initially, our proposed structural design of a MANET is constructed and the message linking in the mobile is originated. The packet drop is to ensue in MANET because of the egocentric node or network traffic. In this proposed paper, triangular vision modelling framework exploits the detection of the misbehaving nodes and the egocentric node in the MANET. The triangular vision view depicts a clear picture in identifying the ideal route by using the behaviour of nodes where it helps to detect the egocentric nodes and misbehaving nodes in the MANET. The two methods called Report Based Method (RBM) Detection and Trace and Hope based Method (THBM) detection are used to detect the egocentric nodes and misbehaving nodes in the proposed framework for the Mobile Ad hoc network.

Keywords*-component; DoS,MANET,Prevent,Attack,Report Based Method, Trace and Hope based Method*

*****

I. INTRODUCTION

Mobile ad hoc network (MANET) [1] is a one of the fast growing wireless network among the mobile devices. This kind of system is self-diagnosing system of mobile nodes which is associated by wireless links. In comparatively the network has latest communication concept, which holds a collection of mobile phone devices corresponding through a wireless medium. The major setback in MANETs is the numerous amount of network distributions, because of the boundless association of the mobile nodes in the system. As a result of that in some of the data gets inaccessible to some of the nodes. Accordingly, the access of data needs to be measured cautiously in MANET. All mobile nodes in MANET necessitate the remaining nodes to self-assured the sachets. The nodes are hanged around for a pre-explained occasion among the following communications. A mobile node could behave badly owing to network traffic and egocentrisms [2]. On account of egocentric or cruel reasons or faulty nodes the node might behave badly and as a result, it can significantly shrink the performance of MANETs.

In MANETs, nodes perform efficiently in both routers and ordinary nodes. As a result of dynamic network topology and necessity of inner communications, network security has transported a great challenge for networking communities. In contrast to traditional networks, MANETs are more vulnerable towards the DoS attacks [3] because of limited resources where it forces the nodes to be unquenchable in resource utilization. If there is no cooperation, even the regular activities of small number of nodes may drastically diminish the proceedings of the system. For example, a misbehaving node rejects any packets passing through the network where it results in repeated retransmissions, and also in turn causes network congestions [4]. Moreover, a wireless link does not afford the same protection for data transmissions as it does in wired link counterpart. Therefore, some of the users or receivers surrounded by the series of the interaction and it can detect or obstruct with data packets for routing information [5]. In addition to that, battery power is another crucial resource for mobile nodes. If the power of the battery has been utilized up, where it causes the cruel attacks in variously as the major deficiency attack, the casualty determines not to offer network services. In view of the fact that, all nodes can be mobile and the major transformations in connectivity of the network and resource availability also interprets a network to dissimilar attacks. This identifies the finding to solve the obstacles of attacks in the network.

The misbehaviour node [6] reveals the deviation from the original routing and forwarding. Through that a source node can transmit the packets to the destination node with other nodes in MANET. The egocentric nodes act and involve in the routing process, which purposely drop the packet and delay [7]. These irregularities of the egocentric nodes will impact the effectiveness, consistency, and the fairness. An egocentric node does not execute the steps related to packet forwarding method for data packets discrete to it. The egocentric node utilizes its limited resources merely for its individual purpose, because of the storage and energy constraints for each node in the MANET. The major objective is to save its resources to the maximum, consequently this type of misbehaving node junk all received packets except those which are intended to it. The egocentric nodes ignore to distribute their resources. This action is take place in the data link layer, which is more significant, and in specifically when the mobile nodes acquire small enduring power. The prominent features [8] of the egocentric nodes are as follows:

- Non-participation in routing
- No transmission or reply to HELLO messages
- Intentional postponement of route request (RREQ) packets
- Data packet dropping

This paper considers both the MANET's and DoS attack rooted by an egocentric node. Through our proposed framework, the reputation-based system for encouraging nodes to assist both in resource deployment and preventing DoS attacks [9] and to detect the wormhole attack caused by a malicious node. In this proposed research explores the sense of the egocentric node in MANET using the Trace and Hope based Method (THBM) method. The process consists of both packet dropping recognition scheme [10] and an egocentric node mitigation scheme [11]. The egocentric node is essential to produce a trust report during each neighbour, which reports its earlier communication reports to the neighbouring node. Based on that report, the neighbouring node perceives whether the egocentric node has dropped packets. The neighbouring node gathers the confident report to notice misreporting and then it detects which node has dropped packets. An egocentric node can report false information to hide the packet dropping from being detected.

II. MOBILE AD HOC NETWORK CLASSIFICATION AND DOS ATTACK SCENARIOS

Based on the composition of different nodes where it helps to structure a network. In further to the examination, the unprepared networks are divided into two major categories. the one is cooperative and second one is non-cooperative [12]. In the first category, the cooperative nodes structured the networks supported on universal targets to attain the firm objectives. For example the networks can be created in emergency relief operations, military applications, combined data processing and conference sessions. During this period, every members of the group have common goals, and therefore they cooperate the things efficiently. In the second category, a network is produced to establish message in civilian environments. And there is no reason for common cooperation. simultaneously as the nodes in a network system used by the armed forces in the battlefield or in a disaster management area can be assumed to cooperate, whereas there is no good reason to presume that networks generated by civilians with change goals and interests will assist. Such network can be created by a group of people who wants to communicate by performing a temporary network setting. The major objective of each user is usually to maximize his/her own benefit, and for this reason the network may suffer from misbehaving nodes which may cause to hoard their self resources while using early nodes for packet forwarding [13]. As if it gives the impression that it is apt to employ a method that persuades the collaboration in non-cooperating networks to progress the performance of the network.

On the other hand the non-cooperation in MANETs takes place in misbehaving nodes and be in short of resources in non-misbehaving nodes. The noncooperation takes place due to misbehaving nodes scenario [14], when nodes fail to cooperate in a situation is due to either to malicious behaviour or egocentricness to capitalize on their own benefits. In other scenarios such as non-cooperating, a node possibly will make safe to forward a packet but run out to do so, otherwise mayn't ready to forward the packets to hoard its resources. But in both scenarios, network services can be corrupted because of lack of cooperation between the nodes. In this study we consider and solve the noncooperation. The non-cooperation happens due to short of resources scenario, whereas nodes fail to cooperate because of insufficient resources. This resource (limited memory, bandwidth, or energy) deficiency may crop up the result in describing the wireless network or environmental conditions like unreliable connectivity or network load [15]. This kind of non-cooperative behaviour is called reasonable non-cooperation. The primary issue is that it requires attention in pondering the load, which is required to apportion the network load equally among the nodes.

The DoS attacks intend the resources where it can be divided into three different scenarios. The principle attack scenario marks the Storage and Processing Resources [16]. It is an attack that generally boards the storage space, memory or process of the service provider. In this case, where a node constantly sends an applicable flooding packet to its neighbourhoods and to excess the storage space and exhaust the memory of the particular node. This averts the node from sending packets or receiving packets from other valid nodes. While neighbourhood watch monitoring is capable to thwart the episodes of such events gradually through the malevolent nodes.

The secondary attack scenario targets the energy resources, particularly the battery power of the service provider. As mobile devices are activated by battery power, energy is an essential resource in MANETs. A malevolent node may endlessly send a false packet to a node with the objective of overriding the victim's energy of battery and thwarting the other nodes from passing with the node [17]. The primary objective of concentration is more efficient in observing whereas, it can assist the detecting such nodes and protecting their consequences.

The final attack scenario targets the bandwidth. In such cases, where an attacker located between the multiple communicating nodes and disrupt connectivity desires to dissipate the network bandwidth [18]. The malevolent node is constantly capable of sending packets with bogus source IP addresses of the other nodes, thereby overloading the network. This devours the resources of all neighbours that communicate, excess the network and results in performance degradations. Here the proposed algorithm is to restrict both the nodes (egocentric and malevolent node) from corrupting network performance by allowing incentives to persuade support and punishing nodes [19] that do not work together.

III. DESCRIPTION OF THE PROPOSED FRAMEWORK

A. *Triangular Vision View Framework*

The triangular vision view of the framework for the streaming access pinnacles to deal with the insecurity of node movement and the requirement of seamless service head-off. For each mobile node, the position like of the triangular vision view, a shape of the virtual fan communication zone is conserved on the direction of the movement. On a particular cell or node, the degree and the volume of communication are to be built by the streaming access point of the cell or node which is decided by the hoarded virtual illuminance of the triangular vision view and its overlapping area.

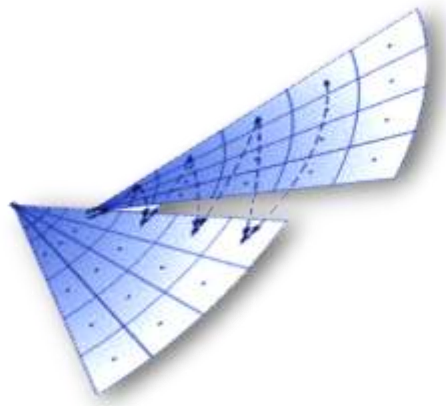

Figure 1: Triangular Vision View Framework

The major concerns in identifying the access points for streaming which are accountable for transmit the timing and the amount of the data to communicate in unraveling the effective and undemanding by means of the single framework called the Triangular Vision View Framework. This framework generates the new mapping structure for the mobile nodes in MANET.

B. *Egocentric Node Detection in Proposed Framework*

The proposed framework of MANET has been created and the nodes in the network are installed according to the architectural model. The Numerous nodes take part in the MANET for brazening and changing the statistical packets between the source and the destination. Each and every node in MANET executes the routing function as mandatory [20] and they should forward traffic. Along with all the nodes, a few of the nodes will act egocentrically; this kind of nodes is called egocentric nodes [21]. A few nodes in MANET could be activated egocentrically, which elucidates the using through limited resources only for its own profit, while every node in the network has the source boundaries such as battery and storage limitations. These kind of nodes are intended to be beneficiary nodes. But it should not make the own resource accessible to others. These nodes are intended to get the highest profits from the network while trying to protect their own resources [22]. The behaviours of the egocentric nodes are shown below:

- Egocentric nodes *don't forward data messages.* This type of nodes will forward the messages, but it won't send data messages and drop them.
- Egocentric nodes *don't forward RREQ messages*: In this type of nodes do not forward the RREQ messages. It drops these packets on the way to avert making up the route member for such others nodes.
- Delayed forwarding RREQ messages: This kind of egocentric nodes forwards the messages with a delay.

Egocentric nodes *don't* forward RREP messages: in this kind of egocentric node exists in MANET, when it will drop all RREP messages.

Algorithm 1: (Trace and Hope Based Method for Egocentric Node detection)

Step 1: RREQ (Resource Request) send to the destination (des) by the source (src).

Step 2: RREQ is received by the Destination (des) from the Source (src) and the RRES (Resource Response) is send back to the source (src).

Step 3: The information of neighbour is sensed and gathered

i. Queue Size
ii. Energy
iii. Packet Count

Step 4: The report rules are validated and the report is generated.

Step 5: Using the below equation the trust value is calculated,

$$V_d^{ab} = \frac{v_p + s/2}{v+s} \qquad v_d, v \geq 0,\ s>0$$

where calculation of trust is V_d , the node *a* to *b* is represented by *ab***,** direct trust is represented by des. The time success is illustrated by v_p, the time transaction is represented by v and the node packet size is represented by s and it is positive real number .

Step 6: Cur_TV is retrieved (Cur_TV is Current trust value)

$$\text{Threshold value} = \frac{Transmission\ range\ of\ the\ network}{Number\ of\ the\ nodes\ in\ the\ network}$$

```
    if (Cur_TV > threshold value)
{
    if (the detection of the egocentric node)
            the egocentric node is added to block list ($B_l$)

            else

            the data is transferred to the destination node;
    }
```

Step 7: At last, the performance evaluation takes place.

The network jamming [23] leads to reduction through the high load. The egocentric node is established for the drop in the data packet. Subsequently, the egocentric node is authenticated for fake reporting, when the reporting node misreports the data. And it should be block listed. These processes reiterate all the mobile nodes in MANET, in accordingly the obtaining the set of egocentric nodes from the other nodes of the network. The block list and packet transmission fixed on whether the packet is available or not. (i.e., the above algorithm will be repeated for all the mobile nodes available in the MANET to detect the presence of egocentric nodes from the other nodes in the network)

C. *Report Based Method (RBM)in our Proposed Framework*

In the proposed framework, the proposed report based method has concentrated on dipping the effects of Denial of Service (DoS) attack [24]. This method contains Cyclic Redundancy Check (CRC), Hop Count, Route ID, Source Address, Sequence Number and Destination address. When the malicious node is perceived, it will be mechanically entered in the table list. In comparison to the existing results, the proposed framework with report based method accomplishes high performance in terms of recognition, efficiency, latency and packet delivery ratio [25].

Algorithm 2:

In our proposed Triangular Vision View in the detection system consists of the following steps:

Step 1: Using intermediate nodes, the packets are sent to the destination node from the source node.

Step 2: When the packet is received at the intermediate node, the sequence number, route id and source id are checked. The packets are dropped when there is no valid route id.

Step 3: The misbehaviour list table is used to store the dropped packets, and the packet dropping ratio is verified by the intermediate node. The calculation is packet dropping ratio is done by the ratio between the number of packets sent by number of packets dropped and it is multiplied by the total number of nodes in the network

$$\frac{Number\ of\ dropped\ packets}{Number\ of\ sent\ packets} \times Total\ Number\ of\ nodes\ in\ the\ network$$

The threshold dropping ratio is set as s_{rpd}. The whole route is not valid when the ratio of packet dropping is greater than the s_{rpd} otherwise it is valid.

The malicious behaviour is identified by the nodes recommendation. By collecting the recommendation to node R from the node S by the recommendation evaluation is given by

$$T_R^S = \frac{\sum_{U \in \gamma} U\ |S \rightarrow D| * U\ |D \rightarrow R|}{U\ |S \rightarrow D|}$$

The group of recommenders is γ.
$U\ |S \rightarrow D|$ is trust vector of node S to D.
$U\ |D \rightarrow R|$ is the trust vector of node D to R.

The presence of malicious node is indicated by dropping of more packets, invalid route id neighbourhood node false recommendation. By means of the misbehaviour detection table, it automatically isolates the node when it is identified as the misbehaving node. DoS attack injects such kind of nodes.

Step 4: The RERR(Route Error) packets are sent back to the source when there is problem occurs and the RREP(Route Reply) packets are sent to the source when all the fields are verified.

Step 5: At last, the numbers of packets received are checked by the destination node. By means of the proposed RBM method, the DoS attack behaviour can be successfully detected.

IV. EXPERIMENTAL SETUP AND METRICS

A. *Simulation Model and Parameters*

The projected triangular vision view framework is employed with the network simulator. In our simulation, for 50 seconds of simulation time in the 1000 meter x 1000 meter square region the 100 mobile nodes will move. The transmission of the nodes will be 250 meters for all nodes in the network. The constant variable bit rate is used as the replicated traffic. The simulation parameters and setting are organised in the Table 1.

TABLE 1: SIMULATION SETUP PARAMETERS

Parameters	**Value/Ranges**
Simulator	NS2
Simulation Area	1000m x 1000m
Speed (m/s)	1 m/s to 20 m/s
Packet rate	5 packets /s
Traffic source	CBR
Number of nodes (max)	100
Transmission range	250m
Packet Size	80 bytes
Simulation Time	50 Seconds

B. *Performance Metrics*

Through this proposed investigation we appraise the performance of the framework largely according to the following metrics:

Packet Delivery Ratio: The ratio between the total number of packets sent by the source and total number of data packets received by the destinations.

Egocentric Node Detection: The ratio between the number of egocentric nodes in the network and total number of egocentric nodes detected is called as egocentric node detection.

Misbehaving Node Detection: The ratio between the sum of misbehaving nodes and sum of misbehaving nodes detected is called misbehaving node detection.

Latency: From the source to destination, the overall surviving data packets are called as latency.

C. *Simulation Environment*

The present study facilitates us to accomplish a performance evaluation by using NS2 [26]. The packet delivery ratio, egocentric node detection rate, misbehaving node detection rate and latency are examined as the performance metrics. The egocentric node and malicious node can be identified by the techniques called Report based Method (RBM) and Trace and Hope based method. The Simulation parameters are shown in Table 1.

V. DISCUSSION OF THE RESULT

A. *Triangular Vision View Framework*

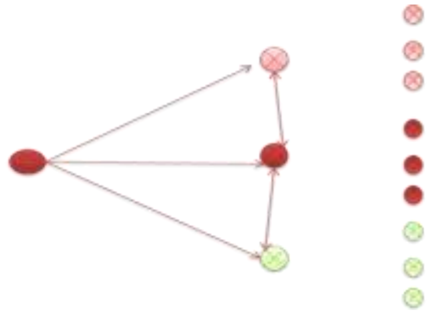

FIGURE 2: PROPOSED DYNAMIC TRIANGULAR VISION VIEW FRAMEWORK

The Figure 2 depicts the outcome of the dynamic triangular vision view model. In the primary level, there are three possible nodes that envelop the throughput, energy and node behavior from the sink in the MANET (at earlier stage itself throughput, energy and bandwidth of the node and node logs is to be considered for the further process then only the nodes can be used for the process). Similarly, each three nodes selects the another three nodes and vice versa for future predictions.

B. *Packet Delivery Ratio*

The ratio between the number of packets received by a traffic sink and number of packets extended by a traffic source is called PDR (Packet Delivery Ratio). Figure 3 shows the comparison detection result of the THBM and RBM in the proposed framework of Triangular Vision View. The number of nodes are represented in x-axis and in terms of percentage the packet delivery ratio is represented in y-axis of the graph.

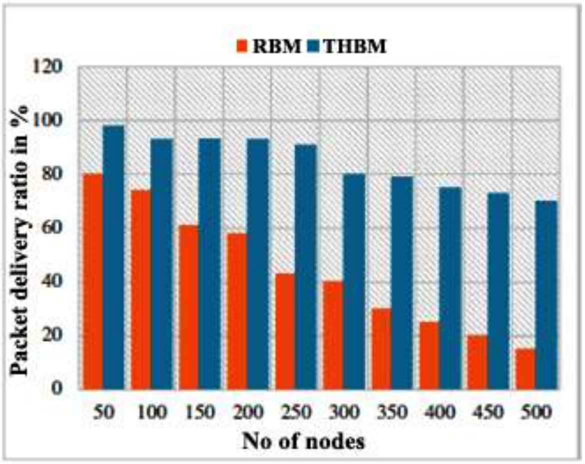

FIGURE 3: THE PACKET DELIVERY RATIO (PDR)

C. *Egocentric Node Detection in Triangular Vision View Framework*

In the triangular vision view framework the act of Egocentric node detection is significant concern in MANET; therefore the current investigation researches the detection of egocentric nodes in a proficient way by means of THBM technique. By using THBM detection, the detection rate for the behaviour of the egocentric node is examined. In Comparison to the RBM method, in the proposed framework the THBM method drastically augments the detection ratio. The virtual analysis in triangular vision view framework between the RBM and the THBM method is shown in Figure 3. The numbers of nodes are represented by x-axis and in terms of percentage the detection ratio is represented by y-axis.

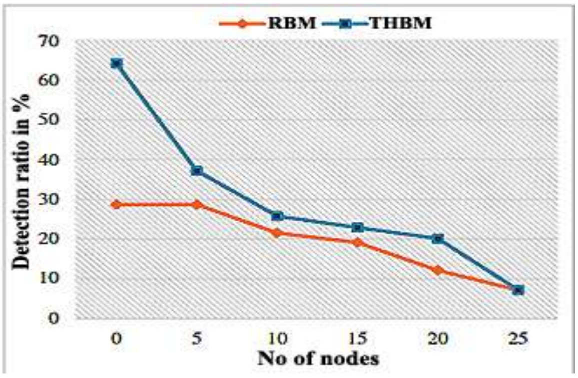

FIGURE 4: EGOCENTRIC NODE DETECTION RATIO

D. *Misbehaving Node Detection in our Framework*

Using THBM and RBM the time taken to detect the misbehaving nodes is accomplished in this paper. From the figure 4, of our proposed framework, where it is detecting the misbehaving nodes in the network, Report based method acts upon more powerfully in the detection of the malicious node in the network than the Trace and Hope based method.

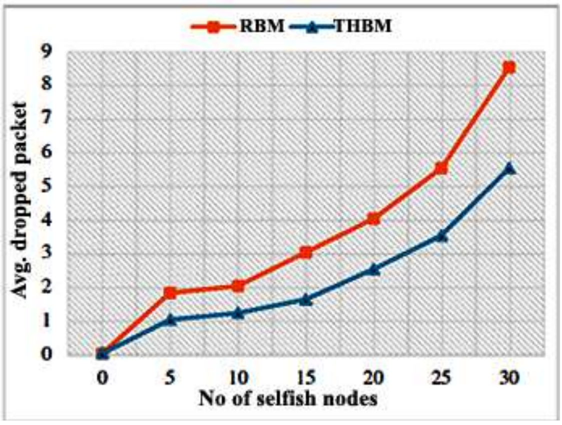

FIGURE 5: MALICIOUS OR MISBEHAVING NODE DETECTION

E. *Latency Deduction in our framework*

The latency is comparably two times efficient in the query time, the acknowledgement is received when the request is send by the sender node and it starts the transferring of the data to the first answering node. Using this THMB egocentric node deduction method controls the latency of the network. In contrast to the RBM method, THBM has extensively lower latency. The time taken from the source node to the destination node by the packet is called as Latency. Depending on the location of the communicating nodes, the fluctuation takes place. Figure 5 illustrates the comparative analysis between the THBM technique and the RBM technique in the triangular vision view framework. The numbers of nodes are represented by x-axis the average latency is represented by y-axis of the graph.

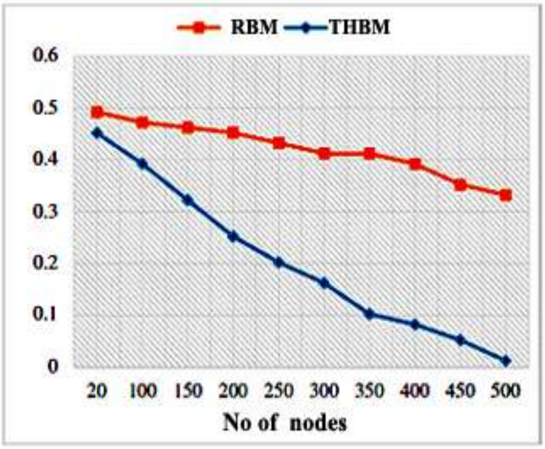

FIGURE 6: DEDUCTION OF LATENCY OF THE PROPOSED FRAMEWORK

VI. CONCLUSION

In the course of current investigation it is explored that Denial-of-Service attack is an attempt that makes the network resource and machine unavailable to the intended users. The attacks transpire when the services are blocked by another user deliberately. In the routing process, when the packet is dropped or delayed intentionally, then the egocentric node do not take part in the process of routing. The efficiency, fairness and reliability of the network are affected these misbehaviours of the egocentric nodes. For the own purpose, the resources are tapped by the egocentric node and that deserts to share the resources to the other nodes. Therefore, it is important to detect the egocentric nodes in MANET. And the malicious node is also very essential to detect for MANET. The major reason in the proposed method is to generate the reasons for the DoS attack in the network. In this research paper, we proposed a new framework called Triangular Vision view model for the structure where the packet can travel in MANET to reach the destination. Through our proposed model, we develop two techniques called Report based method and Trace and Hope based method in distinguishing the egocentric and malicious nodes to prevent the DoS attacks in MANET. From the above observation, we can wrap up that THBM method performs effectively for the detection of egocentric node in the proposed framework whereas RBM increases their detection for the malicious node. The proposed framework advances the deduction latency for both the methods but RBM gives better result than the THBM.

REFERENCES

[1] Saleh Ali K.Al-Omari, Putra Sumari, "An Overview of Mobile Ad Hoc Networks For the Existing Protocols and Applications", International Journal on Applications of Graph Theory in Wireless ad hoc Network and Sensor Network (Graph-Hoc), Vol.2, No.1, March 2010, pp.no: 87-110.

[2] Parulpreet Singh, Ekta Barkhodia, Gurleen Kaur Walia, "Evaluation of various Traffic loads in MANET with DSR routing protocol through use of OPNET Simulator", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.3, May 2012, pp.no: 75-83.

[3] Fei Xing Wenye Wang, "Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks", pp.no:1-7.

[4] Vishnu Kumar Sharma and Dr. Sarita Singh Bhadauria, "Mobile Agent Based Congestion Control Using Aodv Routing Protocol Technique For Mobile Ad-Hoc Network", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, No. 2, April 2012, pp.no:229-314.

[5] Yi-an Huang and Wenke Lee, "Attack Analysis and Detection for Ad Hoc Routing Protocols", pp.no:1-21.

[6] Punya Peethambaran and Dr. Jayasudha J. S., "Survey Of Manet Misbehaviour Detection Approaches", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014, pp.no:19-29.

[7] A.Rajaram and Dr. S. Palaniswami, "Malicious Node Detection System for Mobile Ad hoc Networks", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010, pp.no:77-85.

[8] Martin Schütte, "Detecting Selfish and Malicious Nodes in MANETs", SEMINAR: Sicherheit In Selbstorganisierenden Netzen, Hpi/Universität Potsdam, Sommersemester 2006, pp.no:1-6.

[9] Mieso K. Denko, "Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme", SYSTEMICS, CYBERNETICS AND INFORMATICS, VOLUME 3 - NUMBER 4, pp.no:1-9.

[10] Aishwarya Sagar Anand Ukey, Meenu Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 1, July 2010, pp.no: 12-17.

[11] Vaishali B. Mewada, Viral Borisagar, "Modified Dsr For Mitigating Blackhole Impact In Manet", International Journal For Technological Research In Engineering, Volume 1, Issue 9, May-2014, pp.no:985-990.

[12] Anna Scaglione, Dennis L. Goeckel and J. Nicholas Laneman, "Cooperative Communications in Mobile Ad-Hoc Networks: Rethinking the Link Abstraction", pp.no:1-38.

[13] Isha V. Hatware, Atul B. Kathole, Mahesh D. Bompilwar, "Detection of Misbehaving Nodes in Ad Hoc Routing", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 2, February 2012, pp.no: 6-11..

[14] Usha Sakthivel and S. Radha, "Misbehaving Node Detection in Mobile Ad Hoc Networks using Multi Hop Acknowledgement Scheme", Journal of Computer Science, 2011, pp.no: 723-730.

[15] Rakesh Kumar, Manoj Misra and Anil K. Sarje, "A Proactive Load-Aware Gateway Discovery in Ad Hoc Networks for Internet Connectivity", International Journal of Computer Networks & Communications (IJCNC) Vol.2, No.5, September 2010, pp.no:120-139.

[16] Shinde Sandeep A, Dr. Bakal J. W, "Review on DDoS Attack Traceback Mechanism in MANET", International Journal of Computer Science Engineering and Technology(IJCSET), May 2014,Vol 4, Issue 5, pp.no:161-163.

[17] S.B.Aneith Kumar, S.Allwin Devaraj and J. Arun kumar, "Efficient Detection of Denial of Service Attacks in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 5, May 2012, pp.no: 470-476.

[18] Rabia Ali and Dr. Fareeha Zafar, "Bandwidth Estimation in Mobile Ad-hoc Network (MANET)", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011, pp.no: 331-337.

[19] Alireza Shams Shafigh, Alireza Soleimany, Hekmat Mohammadzadeh and Shima Mohseni, "A Persuading Approach for Cooperating Nodes in Mobile Ad Hoc Networks", World Applied Sciences Journal, 2011, pp.no: 921-932.

[20] Krishna Gorantala, "Routing Protocols in Mobile Ad-hoc Networks", pp.no: 1-36.

[21] Elizabeth Daly and Mads Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs", MobiHoc'07, September 9–14, 2007, ACM, pp.no:32-40.

[22] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang, "Security In Mobile Ad Hoc Networks: Challenges And Solutions", IEEE Wireless Communications, February 2004, pp.no: 2-11.

[23] Ajana J., Helen K. J, "Mitigating Inside Jammers in Manet Using Localized Detection Scheme", International Journal of Engineering Science Invention, Volume 2 Issue 7 July 2013, pp.no: 13-19.

[24] Sugata Sanyal, Ajith Abraham, Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia and Nirali Mody, "Security Scheme for Distributed DoS in Mobile Ad Hoc Networks", pp.no:1-12.

[25] Patil V.P, "Efficient AODV Routing Protocol for MANET with enhanced packet delivery ratio and minimized end to end delay", International Journal of Scientific and Research Publications, Volume 2, Issue 8, August 2012, pp.no: 1-6.

[26] Francisco J. Ros and Pedro M. Ruiz, "Implementing a New Manet Unicast Routing Protocol in NS2", pp.no: 1-35.