The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 11 || Pages || PP -39-47|| 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Region Based Time Varying Addressing Scheme For Improved Mitigating Various Network Threats In Mobile Adhoc Networks For Qos Development

[1]Mrs. C. JAYANTHI , [2]Dr. M. PRABAKARAN
[1]*Research Scholar, Department of Computer Science, Government Arts College, Ariyalur, Tamilnadu, India.*
[2]*Research Advisor, Department of Computer Science, Government Arts College, Ariyalur,Tamilnadu, India.*

----------**ABSTRACT**----------
The mobile adhoc network has threat towards variety of attacks due to the changing topology and the behavior of mobility. In particular the Manet uses different routing protocols, which uses the location parameters and energy parameters, which is prone for different routing attacks. To overcome this issue, there are number of addressing schemes has been discussed earlier but suffers with poor accuracy. In this paper, we propose a novel region based dynamic time varying addressing scheme which assigns and computes address for each node of the network in dynamic manner. The method splits the regions into number of quarters and when the node enters into the network, the network controller identifies the region through which the node enters and assigns address accordingly. In the routing phase, the method performs the time varying address mitigation scheme which verifies the trustworthy of address of all the nodes present in the selected routes. By verifying the addresses of all the nodes the possibility of network threat has been reduced in marginable rate. The proposed method improves the performance of the network and reduces the time complexity also.

Index Terms:
Manet, Network Threats, Addressing Scheme, Region Based Time Variant Dynamic Addressing, QoS.

Date of Submission: 25 September 2015 Date of Accepted: 10 November 2015

I. INTRODUCTION:

The mobile adhoc network as the name suggests, has large number of mobile nodes which has no restriction for their mobility and speed. The mobility behavior makes the network to be changed in dynamically and the topology changing behavior introduces more change of routing attacks. In Manet, the node performs cooperative transmission, where the packets are forwarded through number of intermediate node to reach the destination. What happens at the middle is the presence of malicious node, captures the incoming packet and performs eaves dropping, modification, and Sybil attacks. This spoils the throughput of the network and the source has to retransmit the same packet for many times. Such attacks could not be identified, because of the cooperative transmission, because the routing protocol chooses an efficient path to reach the destination and does not verify the trustworthy of the routing protocol.

To increase the throughput of the network and to avoid the packets being captured and malformed by the malicious nodes, the protocol has been adapted with intelligent addressing schemes. There are number of addressing schemes has been recommended earlier for the development of mobile adhoc networks. Some of them uses the location information and some of them uses the sequence numbers. In many cases, the malicious node generates number of fake addresses to participate in the transmission and performs various attacks. Also the malicious nodes can generate N number of malformed address and they give to the neighbors which could not be verified or handled by the previous methods.

In order to identify and verify the address of the neighbors or the nodes present in the selected routes, there must be an efficient scheme has to be employed. By employing such efficient addressing scheme, the presence of malicious node can be identified and transmitting the packet through the network can be avoided. The identified malicious node and its details can be flood to the region where it located. Not only this can help to mitigate the routing attacks in mobile adhoc networks, the malicious node can generate dynamic address with various parameters, so in order to identify the malformed address, the address verification scheme also has to perform intelligent approach.

The quality of service of mobile adhoc network is highly depend on various factors like the throughput, latency, packet delivery ratio. By implementing efficient address verification scheme, the malicious nodes can be identified in efficient manner and the number of packets being transferred through the nodes can be reduced to nill. This could help throughput to be improved and packet delivery ratio also can be improved. Also the latency of the network also affects the quality of service of the network. By identifying the presence of malicious nodes in the regions, the transmission of packets through the malicious nodes can be avoided which removes the necessary of retransmission and could increase the throughput with reduced latency.

To achieve all such parameters, in this paper we propose a, region based dynamic time varying addressing scheme, which assigns the address to the nodes at entry and the intermediate node can verify the address according to the location parameters and can perform approximation to verify the address of any node before transmitting through the selected route. The detailed description of the proposed mitigation protocol will be given in the section III of this paper.

II. RELATED WORKS:

There are number of routing protocols and mitigation protocols for the development of mobile adhoc network has been described earlier. In this section, we discuss about the set of methods related to the problem of routing attacks.

Survey - Secure Routing Protocols of MANET [4], identify the existent security threats where an ad hoc network faces, and some of the issues and challenges of MANET, we have done literature survey and gathered information related to various types of attacks and solutions. However in short, we can say that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET.

A Survey On Security Issues In Routing In MANETS [5], address the various security issues and various attacks and challenges faced by the routing protocols in MANETs. There is still ongoing research on mobile ad-hoc networks and the research may lead to even better protocols and will probably face new challenges. Current goal of this paper is to find out the security issues and challenges of routing in MANETs.

An Assessment of Frequently Adopted Security Patterns in Mobile Ad hoc Networks: Requirements and Security Management Perspective [6], discusses the security which is the most important concern in Mobile Ad hoc Network. Due to its limited physical security, energy constrained operations and lack of centralized administration; Ad hoc Networks are more vulnerable to attacks than a wired networks or traditional networks. With the proliferation of cheaper, small, and more powerful mobile devices, mobile ad hoc networks (MANETs) have become one of the fastest growing areas of research. In this paper we are attempting to analyze the security attacks in Ad-hoc environment and focusing on various areas of security requirement, different types of active and passive attacks in Ad-hoc networks.

Bio Inspired Approach to Secure Routing in MANETs [7], the author explore the challenges with respect to the security aspect in MANETs and propose a new approach which makes use of a bio-inspired methodology. This paper elaborates various attacks which can be perpetrated on MANETs and current solutions to the aforementioned problems, and then it describes a Bio-Inspired Method which could be a possible solution to security issues in MANETs.

Shared information based security solution for Mobile AdHoc Networks [8], proposes security mechanism dependent upon Random Electronic Code Book (RECB) combined with permutation functions. The proposed mechanism has low time complexity, is easier to implement, computationally inexpensive and has very high brute force search value. It can be used as the temporary security guard during the trust growth phase. The impetus behind the proposed design is the reliance upon shared information between the peers in the ad hoc networks

In Mitigating Multiple Cooperative Black Hole Attack using DRI in Mobile AdHoc Networks [9], a defense mechanism is presented against a coordinated attack by multiple black hole nodes in a MANET. The simulation carried out on the proposed scheme has produced results that demonstrate the effectiveness of the mechanism in detection of the attack while maintaining a reasonable level of throughput in the network..

An Efficient Secure AODV Routing Protocol in MANET [10], proposed an efficient secure AODV routing protocol. Simulation results show that our proposed routing algorithm provides a better level of security and performance than existing works. The simulation results show the improvement of the network performance, in terms of overhead, and end to end delay to the secure AODV routing protocol.

An Efficient Trusted Computing Base for MANET Security [18], presented a module (TMM). TMMs are deliberately constrained to demand only modest memory and computational resources in the interest of further reducing the attack surface. The specific contribution of this paper is a precise characterization of simple TMM functionality suitable for any distance vector based routing protocol, to realize the broad assurance that "any node that fails to abide by the routing protocol will not be able to participate in the MANET.

All the above discussed methods has the problem of more latency and less throughput which has to be reduced to overcome the issue of routing attacks in mobile adhoc networks.

III. REGION BASED TIME VARIANT DYNAMIC ADDRESSING SCHEME:

The method assigns the address for the incoming node at the time of entry into the network. The method assigns address which has four parameters like region, number of nodes currently present in the region, location of the node, displacement speed of the node. Using all the four parameters the base station assigns the address to the node and will be approximated by the nodes of the network at the time of address verification. The address verification scheme performs approximation of all the addresses in each route, using the four parameters and the node will get new address when it changes between regions. The entire protocol can be split into number of stages namely RTD Addressing, Address Verification Scheme, Address Approximation, Route Discovery. Each stage will be detailed in this section briefly.

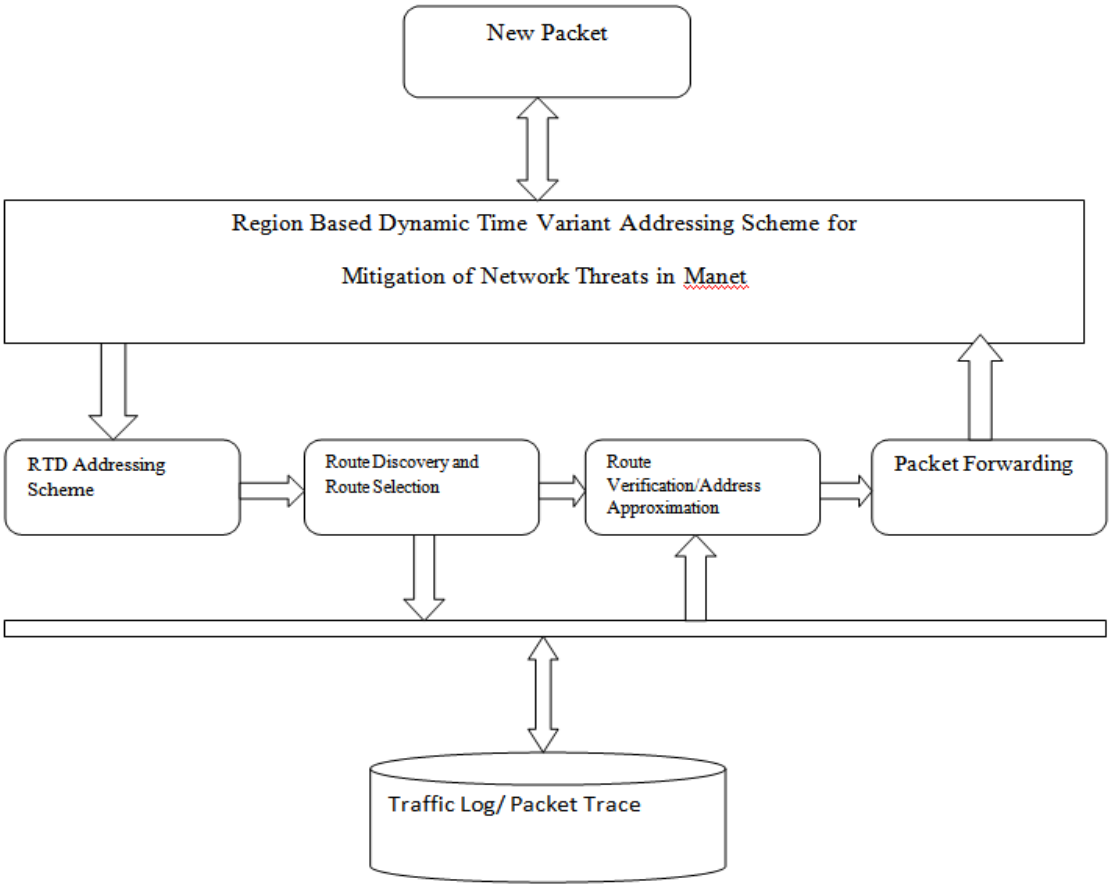


Figure 1: Proposed System Architecture.

The Figure 1, shows the architecture of the dynamic region based time variant addressing scheme and its functional components.

3.1 RTD Addressing Scheme:

Whenever a new node approaches the network, the node sends the handover request to the base station. Upon receiving the handover request the base station assigns the address as follows: First the base station identifies the location of the node and the region in which it located and extracts the displacement speed. Then using the node trace available in the node detail matrix, the method computes the address as follows: First the region is obtained, the number of nodes in the region has been identified, the location parameters as the third bit and finally the displacement speed of node. All the four parameters are used to compute the address. Generated address will be given to the node and has to be used by the node to participate in any of transmission after this.

Algorithm:

Input: Node Trace Nt

Output: Node Address NA.

Step1: start

Step2: Read node trace Nt.

Step3: Receive hand over request HORequest.

Step3: Identify the location of the node.

$$Ln = \int Loc \in HORequest$$

Step 4: Identify the region of the node

Nr = $\sum_{i=1}^{size\ (Region)} Lo \in Region(i)$

Step 4: Count number of nodes present in the region identified

NN = $\sum Nodes \in Nr$

Step5: Initialize address Ad with five fields RID,NN,Loc,DS.

Here RID-Region id
NN – Number of nodes under the coverage of base station
Loc – Node Location
Ds – Displacement Speed

Step6: compute node address Naddr = {RID,NN+1,Loc,Ds}.
Step6: Send to the user.
Step7: stop.

The above discussed algorithm handles the user's handover request performed by the base station and it computes the new address for the newly arrived node of its coverage using the region, location, speed properties of the mobile node.

3.2 Route Discovery and Route Selection:

To mitigate the routing attacks an efficient routing scheme is proposed here in this section. The source node performs route discovery using the popular AODV (Adhoc On demand distance vector) routing protocol. From the set of discovered routes the node chooses the shortest route and based on the selected route the verification of the node is performed. To perform verification the node sends the neighbor verification request and receives the reply accordingly. Once the base station gives positive reply about the node then the packet forwarding will be performed through the selected node.

Algorithm:
Input: Neighbor details Nd.
Output: Selected Route SR.
Step1: start
Step2: Initialize Route Request RREQ

RREQ = {Seq.No, NodeID, Destination Address, TTL}
Unicast the route request to all its neighbors.
for each Neighbor Ni from Nd
send RREQ.
Receive reply RREP.
Extract routes from RREP message.
Ri = Reverse(Route$\in RREP$)
Rd = $\sum(Ri \in Rd) + Ri$
End.

Step3: Sort routes according to hop count.

S-routes = Sort(Rd,Hc).
Here Hc specifies the hop count of the route Ri.

Step4: for each route Ri from S-Routes

Perform Route Verification.
if true then
else
remove routes from the list.
end

End

Step5: Choose the shortest route from the available routes.

Sr = $\int_{i=1}^{size\ (S-routes)} S - Routes(i) \in MinimumHop\ Count$

Step6: stop.

The above discussed algorithm identifies the set of all routes available to reach the destination and the from identified routes, the method verifies each route using one-step scheme with the base station which performs route approximation and returns a result in turn. Based on the result from the base station the source node selects a single route to reach the destination.

3.3 Route Verification Scheme:

The node address verification is performed by the base station upon receiving the verification request from the source node. The base station maintains the list of traces about the node details which are generated at the entry of node into the network and verification performed earlier at different time window .The trace has information about the neighbor location when it enters the network, and the current location is being extracted from the request and the address verification is performed from the list of addresses maintained by the base station. For each region of the network the base station maintains different address set and from the verification request, the method identifies the region and from the list of regions the method identifies whether the address has been assigned earlier. If the address has been assigned earlier, then it verifies the location and speed parameters by approximating the address. If the approximation is matched with the location parameters it has given and the region in which the node exist then it will be approved and a new address will be generated according to the current position of the node and will be sent. In other side, the verification result will be given to the source node which will be used at the next transmission and the details will be added to the region properties.

Algorithm:
Input: Network Trace Nt
Output: Boolean Reply
Step1: start
Step2: Receive verification request VREQ.
Step3: Extract the route information Rt= Route$\in VREQ$
Step 4: for each hop Hi from Rt
Extract AddressHaddr = HAddr∈Rt.
Extract Region ID from HaddrRID = RID $\in Haddr)$
For each address Ai from Rp
if Ai$\in Rp$ then
else
return false.
end
Extract Location CL = Loc $\in VREQ$
Perform Address Approximation (H-addr, Loc).
ifLoc==ALoc then
Extract Number of nodes NN = NN $\in Ri$
Reframe Address Naddr = {RID, NN, Loc, DS}
send to node.
Return True.
else
Return False
end
End
End

Step5: Generate log to the trace.
Nt = $\sum Nti(Nt) + Daddr$

Step 6: stop.

3.4 Address Approximation Scheme:

The address approximation scheme performs the verification of the hop address according to the location given in the verification request and helps to set a new address for the node being given. By assigning dynamic address to the nodes of the network, the address of any node will be changing periodically and the nodes cannot generate their own identity to perform different routing attacks. Using the location parameter from the address and the current location, the method computes the approximation and if it has been closure then it will return the positive values otherwise the node will be identified as a malicious node and return a false value.
Algorithm:
Input: Address Ad, Location Loc
Output: Boolean, Loc
Start

Extract location from address.
Nloc = Loc$\in Ad$
Extract displacement speed from address.
Sp = Ds$\in Ad$
Perform Approximation newloc = $\int \frac{Nloc \times Sp}{Time}$
if New$loc \equiv Loc$ then
return true, Newloc.
else
return false
end
Stop.

The above discussed algorithm performs the approximation of address of the hop address according to the location and the displacement speed. Based on the value obtained the method will return the new location and results.

V. RESULT AND DISCUSSION:

The proposed region based dynamic time variant addressing has been implemented in Network simulator NS2. We have designed network topology with different scenarios with different number of nodes. The proposed methodology has been evaluated with different density networks with multiple network threats. The following table 1 shows the simulation parameters used to evaluate the proposed method. NS-2 has written using C++ language and it uses Object Oriented Tool Command Language (OTCL). It came as an extension of Tool Command Language (TCL). The simulations were carried out using a WSN environment consisting of 71 wireless nodes over a simulation area of 1000 meters x 1000 meters flat space operating for 60 seconds of simulation time. The radio and IEEE 802.11 MAC layer models were used.

Table 1 The parameters used in our simulation

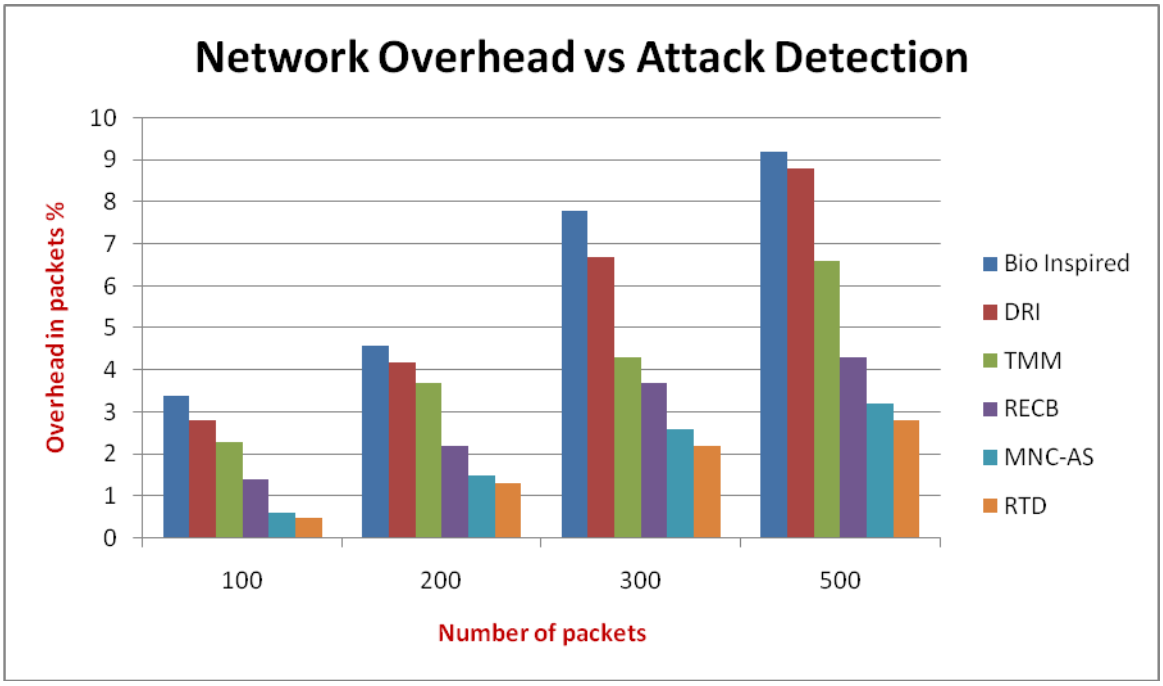
Parameters	**Value**
Version	NS-allinone 2.34
Protocols	**RTD**
Area	1000m x 1000m
Transmission Range	250 m
Traffic model	UDP,CBR
Packet size	512 bytes

The number of packets being received from nodeN_i can be computed using the following equation.
$NP_{Tw} = \sum_1^N Rec(N_i)$ ---------- (1).
The equation (1) shows the number of packets being received by any single node N_i at each time window Tw.
The energy depletion occurred at each neighbor of base station is computed using the following equation.
$EF_{Tw} = \sum_1^N (\mu \times Pl)$ ---------- (2).
μ - energy source constant for each byte.
Pl – payload of the packet.

S.No	Number of Nodes	Protocol	Detection Rate		Throughput	PDF
			False +ve	False -ve		
1	71	BIO INSPIRED	3.8	3.1	87	83.5
2	71	DRI	3.5	2.5	92	86.70
3	71	TMM	3.2	2.3	93.5	88.20
4	71	RECB	2.1	1.7	95	90.05
5	71	MNC-AS	0.9	0.8	97.8	93.50
6	71	RTD	0.6	0.5	98.6	95.60

Table2: shows the comparison results

The Table 2, shows the comparison of various quality of service parameters and the result produced by different methods.

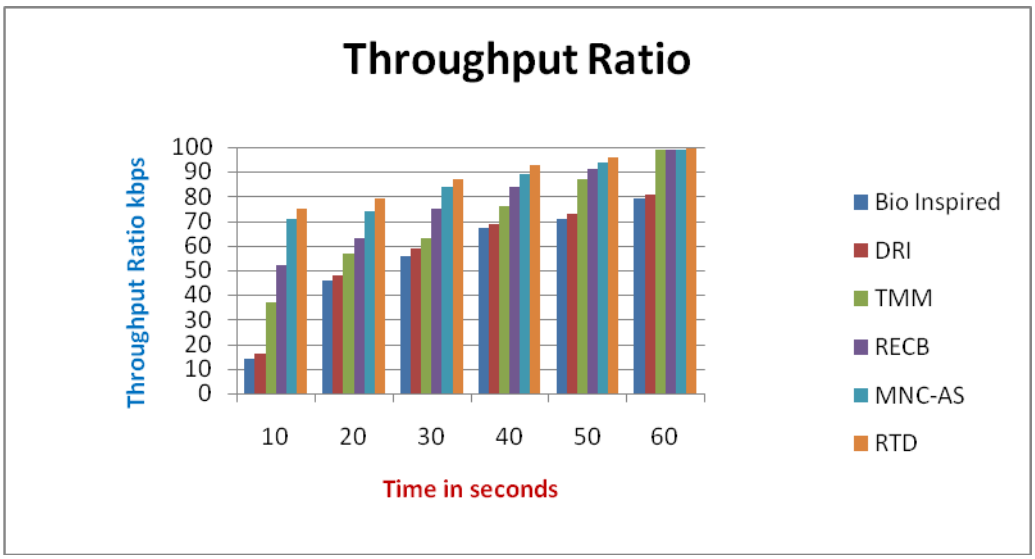


Graph1: shows the overhead generated by attack detection.

The overhead generated by detecting different network threats has been shown in graph1. It shows that the proposed approach has produced less overhead than other methods while performing various network threat detection process.

4.1 Throughput performance:

Throughput is the rate of packets received at the destination successfully. It is usually measured in data packets per second or bits per second (bps). Average throughput can be calculated by dividing the total number of packets received by the total end to end delay.



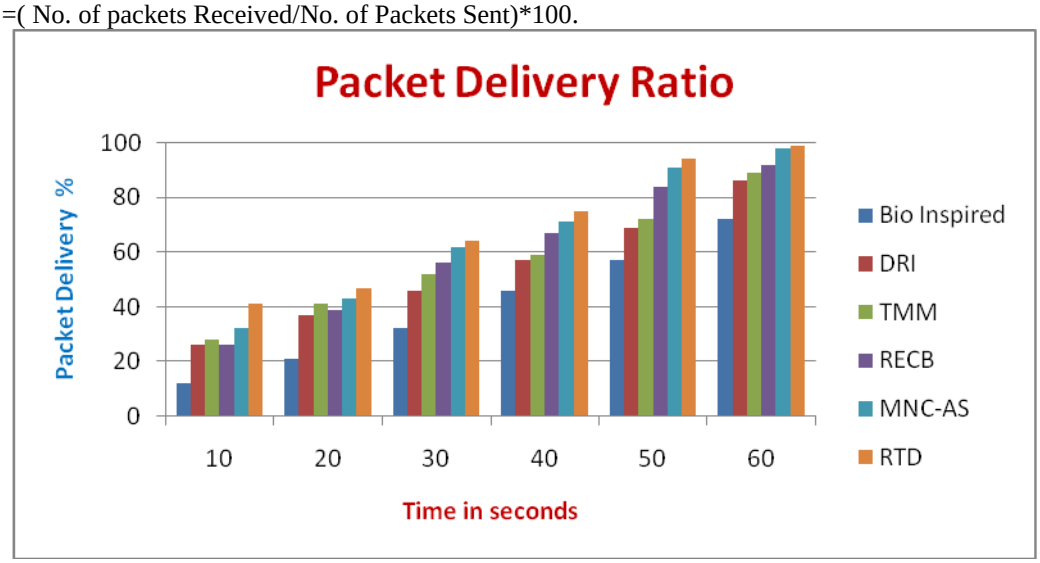
Graph.2 Throughput ratio of different methods

The Graph2 shows the overall throughput ratio of different methods and it is clear that the proposed RTD method has achieved higher throughput than other methods.

4.2 Packet Delivery Fraction:

The packet delivery ratio defines the rate of data packets received at a destination according to the number of packets generated by the source node. The packet delivery ratio (PDF) is computed as follows.

PDF =(No. of packets Received/No. of Packets Sent)*100.

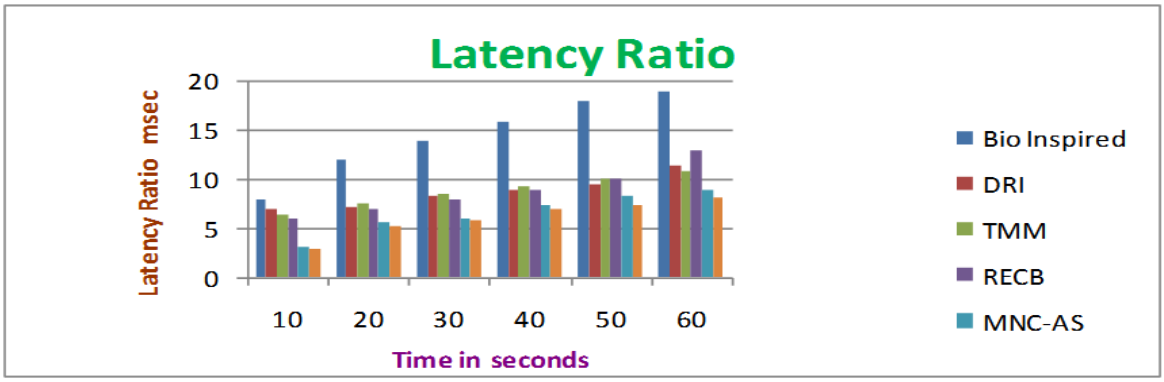


Graph3: Packet Delivery Ratio

The Graph 3: shows the performance of packet delivery ratio of different algorithms and it shows that the proposed multi model method has higher packet delivery ratio than other methods.

4.3 Average End-to-End delay:

Average end to end delay includes all possible delay caused by buffering during route discovery latency, queuing at the interface queue, and delay at the MAC due to retransmission, propagation and transfer time. It is defined as the time taken for a data packet to be transmitted across a Manetfrom source to destination.



Graph4: End-to-end delay

Delay = t_R - t_S

Where t_R is the receiving time and t_S is the sent time.

The Graph4 shows the latency ratio of different methods and it shows clearly that the proposed method has lower latency ratio than others.

VI. CONCLUSION:

We proposed a region based dynamic time variant addressing scheme for the mitigation of network threats in mobile adhoc networks. The base station assigns addresses for each node when it enters in the network using four different parameters like region id, number of nodes present in the region, location and displacement speed of the node. The same address will be verified by the source node when it performs route selection and at the time the base station performs address approximation according to the current location obtained and the location present in the address given. Based on the result an new address will be assigned to the intermediate node if it founds a fair node. Otherwise it will be concluded as a malicious node and ignored. The proposed method improves the performance of mitigating the different attacks in mobile adhoc network and improves the performance of the network.

REFERENCES

[1] C.BaqueroP.Almeida, R.Menezes, P.Jesus, Extrema propagation: Fast distributed estimation of sums and network sizes, IEEE Transactions on Parallel and Distributed Systems 23(4)(2012)668–675.

[2] A. Abdelmalek, M. Feham and A. Taleb-Ahmed. On Recent Security Enhancements to Autoconfiguration Protocols for MANETs: Real Threats and Requirements. International Journal of Computer Science and Network Security, Vol.9, No.4, PP.401–407, April 2009.

[3] M. Thoppian and R. Prakash, "A distributed protocol for dynamic address assignment in mobile ad hoc networks," IEEE Transactions on Mobile Computing, pp. 4–19, 2006.

[4] Jayashree A Patil and NandiniSidnal. Article: Survey - Secure Routing Protocols of MANET. *International Journal of Applied Information Systems* 5(4):8-15, March 2013

[5] C Sreedhar ,VarunVarmaSangaraju . "A Survey On Security Issues In Routing In MANETS" . ***International Journal of Computer & organization Trends (IJCOT)***,V3(9):399-403 october 2013

[6] Jayraj Singh, Arunesh Singh, Raj Shree "An Assessment of Frequently Adopted Security Patterns in Mobile Ad hoc Networks: Requirements and Security Management Perspective, Journal of Computer Science and Data Mining ,Vol. 1,No. 1-2,December 2011

[7] V. VenkataRamana, **Dr. A. Rama Mohan Reddy, and ***Dr. K. Chandra Sekaran, Bio Inspired Approach to Secure Routing in MANETs, International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, No.4, July 2012

[8] Shailender Gupta and Chander Kumar, (2010), "Shared information based security solution for Mobile AdHoc Networks". International Journal of Wireless & Mobile Networks, Volume:2.

[9] JaydipSen1 ,Sripad Koilakonda2 , ArijitUkil, (2011), "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", International Journal of Computer Science and Technology Vol.2, Issue2.

[10] DurgeshWadbude, VineetRichariya, An Efficient Secure AODV Routing Protocol in MANET, International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012

[11] R. S. Mangrulkar, Pallavi V Chavan and S. N. Dagadkar, "Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for MaNeT", International Journal of Computer Applications (0975 – 8887) Volume 7– No.10, October 2010, pp 36-39.

[12] Shilpa S G, Mrs. N.R. Sunitha, B.B. Amberker, "A Trust Model for Secure and QoS Routing in MANETS", INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY & CREATIVE ENGINEERING (ISSN:2045-8711) VOL.1 NO.5MAY 2011, pp 22-31.

[13] Suchita Gupta, Ashish Chourey, " PERFORMANCE EVALUATION OF AODV PROTOCOL UNDER PACKET DROP ATTACKS IN MANET", International Journal of Research in Computer Science eISSN 2249- 8265 Volume 2 Issue 1 (2011) pp. 21-27.

[14] A.MenakaPushpa M.E., "Trust Based Secure Routing in AODV Routing Protocol", IEEE2009. [5] Songbai Lu1, Longxuan Li and Kwok-Yan Lam, LingyanJia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", IEEE 2009 International Conference on Computational Intelligence and Security, pp 421-425.

[15] Ming Yu, Mengchu Zhou, and Wei Su, "A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009.

[16] Victor, C., Francisco, J., Pedro, M. 2009, Simulation-based Study of Common Issues in VANET Routing Protocols. IEEE 69th Vehicular Technology Conference, VTC2000.

[17] Wenjing, W., X. Fei, et al. 2007, TOPO: Routing in Large Scale Vehicular Networks, IEEE 66th Vehicular Technology Conference, and VTC-2007.

[18] Somya D. Mohanty[1], Vinay Thotakura[2], MahalingamRamkumar, An Efficient Trusted Computing Base for MANET Security, *Journal of Information Security*, 5, 192-206.