Node Selection Strategy for Reliable Data Transmission in Manet using Semi Markov Process for Multicast Routing Protocol

M. Maragatharajan, C. Balasubramanian, S. P. Balakannan

Abstract— Reliable data delivery is essential in the mobile adhoc network (MANET) and the devices change their positions very frequently since they do not have any fixed infrastructure. In this paper, we have used the semi Markov process to select the nodes. Semi Markov process is used to develop the node behavior model for network survivability. Then multicast routing protocols have used to form a group for data transmission. We have used Adaptive demand driven routing protocol which provides routing with fast topological changes and Neighbour supporting multicast routing protocol.

Keywords—MANET, ADMR, Markov Process

I. INTRODUCTION

The mobile adhoc network (MANET) environment in the wireless field has an important constituent called the nodes[1]. By structure and form, nodes are self-arranged and they need less infrastructure. As nodes are movable devices current stream of the Internet heavily depend on them. MANET is characterized by its adaptability in creating a network amidst formless local architecture. MANET is ideal for environments like natural disaster scenario, where defence personnel, fire-fighting personnel and local policemen have to maintain constant communication. In fact, MANET enhances a synchronized communication system in such a situation. However, provision of directly connected cables or a static system is not feasible in such environment, which deprives lagging in searching and rescue operations. Thus, the basic communicative message of an Announcement becomes a hard task. Similar condition is possible in educational institutions, business correspondences and in war fare environments. As a result, MANET acts as a remedial measure as it can enfold any device to travel along any route by modifying the connections in accordance to the specifications of the devices.

Since the nodes of MANET are unstable and also in minimizing the overhead in routing protocols, there are commonly employed protocols such as Adhoc On demand Distance Vector routing protocol (AODV), Dynamic Source Routing protocol (DSR) and Destination Sequenced Distance Vector routing protocol (DSDV).

Revised Manuscript Received on December 05, 2019.

M. Maragatharajan, Assistant Professor, Department of Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil, India.

C. Balasubramanian, Assistant Professor, Department of Computer science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, India

S. P. Balakannan, Associate Professor, Department of Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil, India

Yet, these protocols do not match the operational requirements of MANET [2]. Hence, a protocol is to be designed which can improve the instant reactive capability to the topological modifications within the network and non-interfered delivery of reliable data. Adaptive Demand driven protocol (ADMR) [3] readily and conveniently fills this slot by having two characteristics. ADMR is capable of locating the flexibility regarding the usage of GPS or extra locating data and it is equally capable of changing itself to overflowing in case of brief retaining to the common multicast procedure. ADMR is known for its act of inactive responses to customized tree pruning and does not engage itself in any flooding of control packets at periodic basis. Further, ADMR does not exercise its act on any periodic detection of neighbour nodes or table interactions routing.

Neighbour Supporting Multicast Protocol (NSMP) adapts to the working structure of upgrading the versatility in contrast to portability [4]. NSMP employs hub territory in decreasing the overhead of routing, recuperation and especially the upkeep in a work. Further, it makes elevated effectiveness of course and declined transmissions of information. The effective delivery of packets by NSMP gets demonstrated by recreation, as the process results with decrease in control overhead under various circumstances.

Of late, Network Survivability has found a strong place in organized and reliable communication system[5]. Under standard mode, the topology of an Adhoc network extends its performance of maintaining the conversions in a dynamic manner. This is possible as nodes are mobile and due to channels being random, amidst the absence of collapse to nodes or security threats. An upkeep of a linked topology is an integral part in the Adhoc networks layout; otherwise, there will not be assured operative functions such as forwarding and routing, even to the exhaustion of QoS. Hence, the survivability of a network community is determined by a great volume of outgoing paths and capability of each node to communicate. So, it is beyond doubt to the authors of this paper that in order to keep the associated topology, due focus and importance must be paid towards the survivability of Adhoc network system, by treating as the primary task. Such a consideration will give rise to the scope in cases of malicious adversaries and random disasters in addition to metric being the connectivity factor [6]. This leads to convenient classification of nodes as Cooperative state (C), Malicious state (M), Selfish state (S) and Failure state (F).

II. ADAPTIVE DEMAND-DRIVEN MULTICAST ROUTING PROTOCOL MECHANISM

Improvement of capability to react immediately to topological modifications in the network and dynamic and reliable data delivery without interference requires the Adaptive Demand driven Multicast Routing (ADMR) protocol [6]. It can identify flexibility over the usage of GPS or extra locating data and can change to overflowing for some time already relapsing back to the ordinary multicast procedure. It practice, inactive responses for well-organized spontaneous tree pruning. Also, ADMR does not practice any periodic network-wide floods of control packets, periodic neighbor detecting, or periodic routing of table interactions. In this routing protocol, source-based forwarding trees are produced only when there are single sender and single destination in the network.

ADMR observes the traffic model of multicast sender application, by which notices path breaks in that tree. As a result the source does not transfer any information. In the previous circumstance, protocol begins limitations on repair techniques and then global repair when the local repair flops. In very last-mentioned case, multicast forwarding state is wordlessly invalid but not the requirement to transparent conclusion message. When the source is not sending data temporarily, to enable monitoring link breaks in the multicast forwarding tree, ADMR sends a limited number of keep-alives at increasing inter-packet times. At this point, when the sender does not transmit any information for the time frame, but then establishes a critical aberration from distribution design, there is a routeless lapse in the entire tree. The keep-a lives stops and the whole tree silently repairs. A noteworthy deviation from a sender's message transmitting pattern indicates that the source is probably going to be idle for some time when keeping up routing condition in the system means inefficient. In addition**,** ADMR trims every division of tree naturally, while there is a bit much to forward. These pruning choices depend on the absence of inactive affirmation from downstream, rather than on the acceptance of an express trim data.

Similarly, ADMR recognizes a situation when mobility in a system is very great to permit convenient multicast condition arrangement and upkeep, without the need for GPS or any other situating data or extra regulator movement. At this point, when more mobility is distinguished, ADMR briefly changes to flooding of all information data, and after a short time, the convention again endeavors to work productively by multicast routing, as the portability in the system may have diminished.

ADMR supports the conventional IP multicast services which enable receivers to get multicast packets propelled by any source. The newer source-particular multicast benefit demonstrates in which recipients can link a multicast group just to specific sources. Much akin to multicast benefit models, a node never requires position of the recipient for group to have the capacity to send to the group. Also, sources require no announcements, with expectation for directing multicast packets for gathering. Further, sources need not require declaring their goal of being in multicast sources.

Multicast senders do not identify the recipient which is anywhere in the system that they have found, and beneficiaries do not identify the senders in which the location where they are found. ADMR was outlined under the presumption that nodes in the system can move whenever required and that any packet might be lost due to presence of components; for example, packet impact, remote obstruction, or flag weakening, because of separation. ADMR has planned for systems of gadgets with Omni-directional receivers, wherever a communication by a node gets caught by any node inside the remote transmissions. ADMR is totally appropriated and does not depend on any incorporated coordination or control. In the event of being no other cause or receiver for the multicast group, ADMR cannot transmit any other control packets. In the event that there are no recipients, ADMR sources just flood rare information (to restore packets) and do not transmit other information or control information.

This routing does not utilize any occasional system wide flood of control packets, intermittent neighbor distinguishing, or infrequent routing table trade. No other universally useful multicast convention for impromptu systems planned before ADMR has any one of these things in any routing. For every multicast source ADMR constructs an "amplified" source-established tree, which is called source mesh. Multicast packets are sent along this work from the source to the multicast beneficiaries along the most limited mesh ways inside the work. The convention adjusts its conduct in the light of use sending pattern, permitting productive identification of broken connections and lapse of steering state. In other words there could be a no keep-a live along the multicast work, so as to recognize the absence of information from separation.

Multicast senders and recipients utilize ADMR coordinate for building up and keeping up the sending state in the system to permit multicast correspondence. ADMR adaptively screens the right process of multicast sending state and incrementally repairs it when at least one recipient or sending network winds up noticeably disengaged from the sender. ADMR bolsters the conventional IP multicast benefit model of enabling collectors to get multicast packets sent by any sender and additionally more up to date source-particular multicast benefit display in which recipients may join as a multicast for just particular senders. As in both multicast benefit models, a node requires not being a beneficiary for the gathering to have capacity to send to the gathering. Hence, senders do not require any declaration of their goal in progress of multicast packets. Normally these packets are sent from S along the most limited mesh way through the tree to the recipient individuals from the multicast group.

ADMR performs programmed pruning of branches of the multicast tree that are at no time required for future sending. Pruning of choices depends on the absence of affirmations aloof from downstream, rather than on the receipt of an express pruned message. ADMR is intended for work autonomous of the unicast convention utilized as a part of specially appointed system and can consequently work with any unicast convention or even

without a unicast routing. In fact when valuable data sharing between the unicast and multicast routing is absent, there will no improvement in modularity and transportability.

Within the multicast sending state for a multicast group G, S as the sender in ADMR S is represented as a sender to refer a loosely structured multicast sending tree. Each multicast packet is progressively sent from S besides the most limited mesh way through the tree to the recipient individuals from the multicast gathering. ADMR achieves programmed trimming of divisions of the multicast tree which are never again required to send information. Trimming choices depend on the absence of inactive affirmations since downstream, rather than on the acceptance of express crop data. ADMR is intended for autonomous doing of unicast convention utilized as a part of the impromptu system and may consequently be doing it along with unicast convention or deprived of a unicast convention. In spite of the fact that it might be helpful to transfer data among unicast and multicast conventions, this does not, as such, enhance particularity and mobility.

The surge of a packet in Figure 1 shows the node in which the multicast sending tree is a tree flood, and to a lot of broad kind of surge of a packet finished all nodes as a network flood. This utilization of flooding inside the multicast sending tree is like the "forwarding group" idea presented in the FGMP convention and utilized likewise in ODMRP, with the exception that the sending state is particular to every sender as opposed to being shared for the whole gathering.

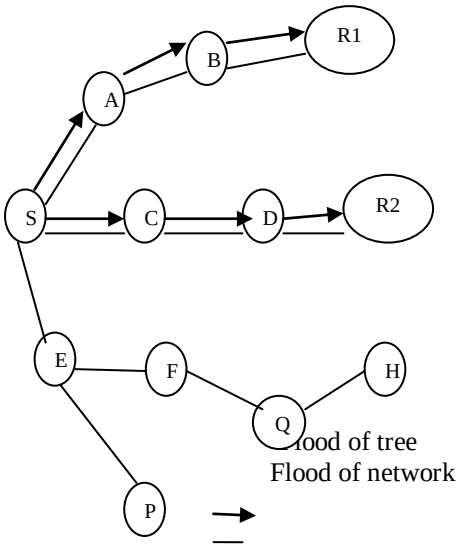

Fig 1 Tree flood Vs Network Flood

ADMR performs programmed cutting down of branches (pruning) of the multicast tree which is no more needed for forwarding. Pruning decisions are focused majorly on the loss of inactive acknowledgment from downstream, as a substitute for counting on the receipt of an explicit short message. ADMR is planned to work self-governing of the unicast protocol used inside the Adhoc network and work with any unicast protocol or even without a unicast protocol. Presently, ADMR functions only bidirectional links. Also the ADMR has designed to enlarge the provisions to contract with unidirectional links as adequately.

III. NEIGHBOUR SUPPORTING MULTICAST PROTOCOL

Neighbor-Supporting Multicast Protocol (NSMP) is a rugged process delivering reduced overhead and enhanced productive convention. The framework of this protocol acts upon the sustainability strength against untoward calamities and this framework turns out to be the hallmark of the multicast routing. Generally, under impromptu pattern communication proves to be a costly affair, but NSMP provides considerable reduction of control message in communication process. Communication gets its utility in initiating a course foundation or a parcel repair system while control messages does the job of sending hubs and the neighbouring hubs as a part of common and select upkeep work systems. In case of selecting other course, NSMP proceeds with a move towards the path containing current sending hubs. This emanates the reasonable increase in the course productivity and decreased volume of sending hubs.

As such, NSMP performs two kinds of course recuperation namely flooding course revelation and nearby course disclosure. Of these two, course revelation is constrained with limited arrangement of efficient hubs, being identified genuinely in tune with the multicast gathering. Thus, NSMP employs this recuperation in case of routine and ordinary system support way. On the other hand, flooding disclosure is employed by NSMP for a course foundation of underlying nature or parcel repair of a system. This is because, in the flooding disclosure all the nodes avail communication by receiving the control packets. Comparatively, in case of extensive association, system way of upkeeps occurs more frequently than the underlying foundation. Further, there sparing is facilitated by the routing way systems through restrained and moderate support. The work of multicast gathering includes sources, recipients, sending hubs, and connections associating them. Such functional hubs are thus called as work hubs.

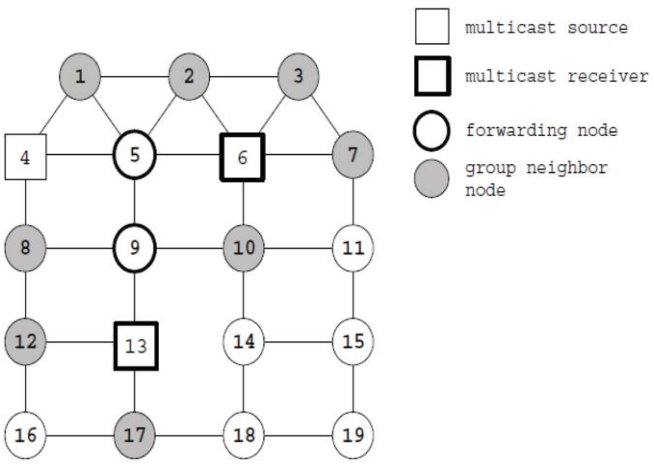

Figure 2 Multicast Mesh Creation

From Figure 2 it can be inferred the acceptance of nodes 6 and 13 as beneficiaries of a multicast gathering. Further, it can be seen that a FLOOD REQ parcel is communicated by hub once it joins the gathering and in turn, node 5 receives the packet and communicates to hub 6. Once hub 6 receives FLOOD REQ parcel, it sends a REP packet to node 5 as a response in an upstream manner. As node 5 receives the REP packet from hub 6, it immediately transmits the packet to its upstream hub 4 as a part of multicast task. This serial of sending and receiving occurs in case involved by hub 13 and subsequent nodes until the packet reaches hub 9, which ultimately forwards the packet to the sending nodes.

When a DATA packet broadcast by a sender, at a given point of transmission, the sending nodes send the packet in an assertion that the parcel is sure to reach the recipients irrespective of the set-up in the work. In the current work, neighbour nodes of the multicast work are taken under assumption. When it is mentioned that neighbour nodes, it indicates those nodes specified to associate with minimum one work hub. Figure 2 displays the neighbour hubs 1,2,3,7,8,10,12 and 17. There can be drop in the capacity by sending hubs and gathering neighbour nodes, if only there is an invigoration within the prescribed time slot.

IV. SEMI MARKOV PROCESS

Any system is free from flops, flaws, lapses or snags if the system is designed to achieve the desired performance goal in a proper and efficient manner. In this field, such a perfection is termed as Network Survivability [7]. This necessitates the provision of distinguished, apparent and prompt strategy or model based on mathematical accuracy for devising Adhoc networks. The standardized mode refers to the topology of an Ad hoc network which maintains conversions in a dynamic way. This is, as mentioned earlier, due to the node mobility and randomness among the channels, despite being prone to disasters or collapses. Keeping a linked topology happens to be the foremost concern in laying out the Adhoc networks. When there is no point of this concern, then there could be no routine operations, which include forwarding and routing, leading to the deprival of QoS. This purports to the view that a network community's survival highly depends on the existence of large scale outgoing paths that could be flooded to each node for routine communication. Again, these factors bring the network survivability as the core issue and the primary task in devising the Ad hoc system, to get an associated topology.

In this work, two kinds of node behaviour are focused viz. Black-hole attack and Jelly-fish attack[8]. The circumstances of the node define the type of nodes, which are signified as {C, S, M, F}. For evaluating the disclosed outcomes of these nodes, Xing and Wang [9] created the stochastic model.

The diagram below represents the state transition of the homogeneous Semi-Markov Process (SMP) is exhibited in Figure 3 cited below:

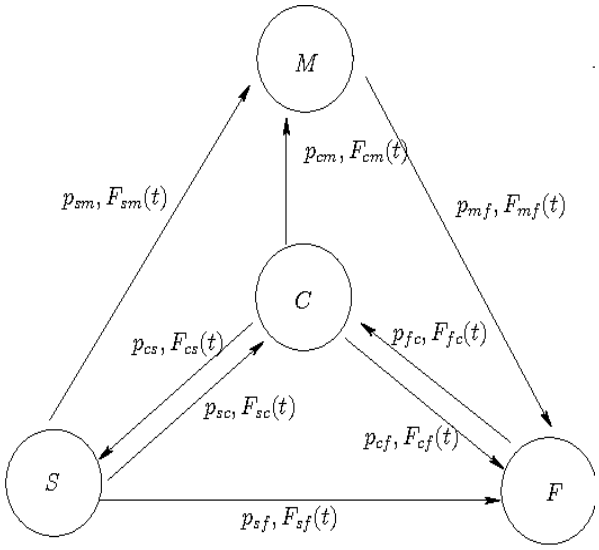

Figure 3 The SMP for node behavior evolution

The solution for node misbehavior is found in the form of Node Isolation and routing information adduces the failure due to the communication between nodes. The cooperative probabilistic matrix can be constructed by using Figure 2 and the following equation:

$$PM = \begin{pmatrix} 0 & 0.525 & 0.071 & 0.404 \\ 0.756 & 0 & 0.022 & 0.222 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Since the P_{ij} value is known value and based on the equations the $E[T_{ij}]$ [4] [9], [10] is

$E[T_c] = 142.2$ $E[T_m] = 51.7$
$E[T_s] = 45.9$ $E[T_f] = 60.$

The limiting probability of various states of the node can be derived by using these values as,

$P_c = 0.6877$ $P_m = 0.0207$
$P_s = 0.1167$ $P_f = 0.1750$

Factually, the accuracy of heuristic technique lies on the effectiveness of the established heuristics. Such a heuristic approach readily offers an efficient method to analyze the influence of any specific non-static factor, in addition to the movement of node within the stochastic domains of node behaviour. It has already been proved that the conduct of state distributions determine the network survivability. Based on this presumption, the limiting probability executes excellent performance in gulfing the space among the network survivability. The limiting probability gets additional possibilities when the delay influences are prevented by a dynamic and unique approach. Thus, it is asserted that the Semi-Markov node behaviour model employed in this research study is capable of delivering widened mathematical framework to demonstrate the node behaviour.

In addition, the model is ideal for calculating the impact of a ruggedness of a random dynamics related to the network survivability, as it is provided with state behaviour distribution.

V. NODE SELECTION STRATEGY

Figure 4 demonstrates the process of selecting a node. The process of creating a MANET starts by using a group of devices under the military surroundings by providing a dynamic mobility of devices. The creation of the multicast group is done at once the deployment of node gets over. Here, probability is limited for identifying the group node. To be more specific, 0.6877 shall be the probability state for a node to in a cooperative state. This means that any node selected should fall within the probability value of greater than or equal to this 0.6877. When this value is not maintained, there is a possibility for a node to choose some other node in a forwarder direction.

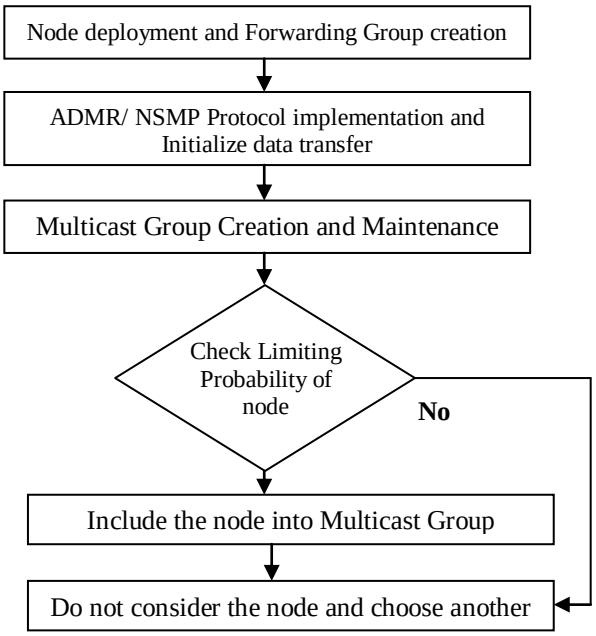

Figure 4 Flow diagram illustrating Node Selection

VI. SCENARIO STUDY AND SIMULATION RESULTS

Simulation Setup

The performance of ADMR and NSMP with Markov process was analyzed by simulating the algorithm in NS-2 and comparing the simulation results of both. During the simulation, it was assumed that there could be 100nodes present within the simulation surrounding. The random waypoint became the mobility model enabling the free mobility of the nodes. However, the task could be completed with 900 nodes when the constant bit rate taking up the role of traffic pattern. The parameters estimated under the simulation of performance analysis were packet delivery, average end-to-end delay and throughput.

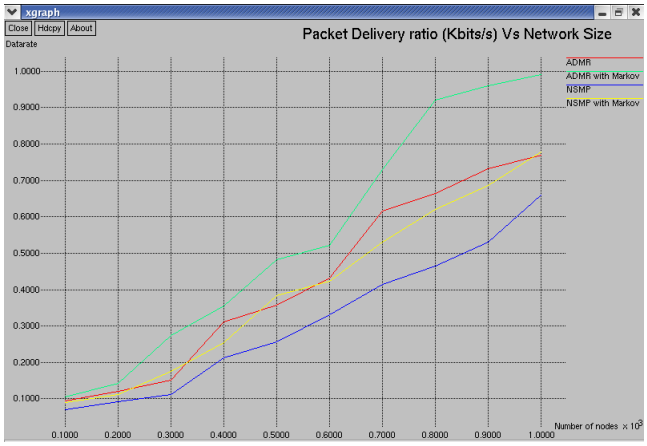

Figure 5 Packet delivery ratio

Fig 5 exhibits the performance of multicast routing protocol. The comparative better performance can be observed when Markov chain in ADMR and NSMP method was included by offering better Package transfer ratio.

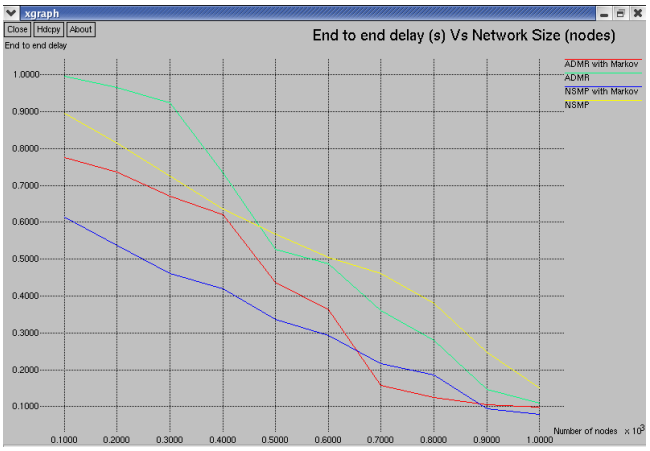

Figure 6 End to end Delay

Figure 6 shows The performance comparison of delay between the proposed protocol and the multicast routing protocols is illustrated in Figure 6. From the figure, an overall reduction of delay of MANET can be observed when the Markov chain process was incorporated.

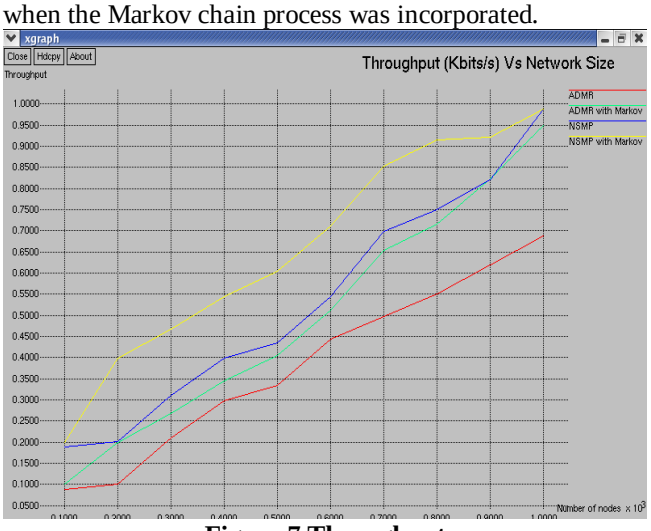

Figure 7 Throughput

Figure 7 illustrates the comaprative analysis of throughput between multicast routing protocol with the proposed protocol / method. With the incorporation of the proposed model, there is a linear increase in the Throughput with corresponding increae in the the number of nodes. Hence, it is summed up that multicast protocols prove their worth in outperforming regarding the parameters of Throughput, End-to-End delay and Packet Delivery Ratio.

VII. CONCLUSION & FUTURE WORKS

In this paper a solution for node selection technique for MANET is proposed. According to the analysis, both ADMR and NSMP offer better performance in terms of packet delivery ratio, Throughput and delay. This work may further be focused on trust based model and Multicast routing protocol to yield more robustness and less control overhead.

REFERENCES

1. Durka Devi K, Maragatharajan M, Balakannan S P "Reliable Data Deliversy for highly Dynamic MANETs Using Adaptive Demand Driven Multicast Routing Protocol(ADMR)," International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014), Vol. 2 Issue Special 1 Jan-March 2014
2. Mattias Halvardsson, Patrik Lindberg, " Reliable group communication in a mlitary Mobile Ad hoc Network", Report from MSI, School of Mathematics and Systems Engineering, Vaxjo University, 2004.
3. Jorjeta G. Jetcheva, David B. Johnson, "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks", ACM Transactions , 2001
4. Maragatharajan M, Balakannan SP, A Secured MANET using Multicast Routing Protocol and Semi Markov Process, Journal of Cyber Security and Mobility, Vol 7.1, 53-68, 2018
5. Fei Xing, Wenye Wang, " On the survivabilty of wireless Ad hoc networks with node misbehaviors and failures", IEEE Transaction son Dependable computing, Vol.7, No.3, 2010
6. Lusheng JI and Scott Corson M, "Explicit Multicasting for Mobile Ad Hoc Networks" Journal of Mobile networks ans applications, pp-535-549, 2003
7. Paul K, Choudhuri R R, and Bandyopadhyay S, "Survivability Analysis of Ad Hoc Wireless Network Architecture," in Mobile and Wireless Communications Networks, LNCS 1818, C. G. O. (Ed.), Ed. Springer, , pp. 31–46, 2000
8. Mannie E and Papadimitriou D., eds Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS), IETF RFC 4427, http://www.ietf.org/rfc/rfc4427.txt, Mar.2006.
9. Xiang-Yang LI, Peng Jun Wan, Yu wang, Chih-wei "Fault Tolerant Deployment and Topology Control in Wireless Networks," in Proc. of ACM MobiHoc '03, pp. 117–128, Jan. 2003
10. M. Maragatharajan, C. Balasubramanian, SP. Balakannan, A Secured MANET using position based oppotunistic routing and Semi Markov Process, Journal of concurrency and computation: Practice and Experience, DOI: 10.1002/cpe.5047
11. Maragatharajan M, Balakannan SP, Analysis of multicast Routing Protocol for Secure MANET, IEEE International conference on Intelligence Techniques in Control, Optimization and Signal Processing.

AUTHORS PROFILE

Maragatharajan M received his Bachelor degree in Electronics & Communication Engineering from Anna University by 2007. He has received his Master degree in Information Technology from Kalasalingam University, 2010 and completed his Ph.D in the area of MANET. He has worked as a Project Associate in TIFAC CORE in Network Engineering, Kalasalingam University from 2007 to 2008. Currently, He is working as an Assistant Professor in the Department of Information Technology, Kalasalingam University. His areas of interest are Ad-hoc Networks, Wireless Networks, and Network Security.

Bala Subramanian C received his Bachelor of Engineering in Electronics and Communication Engineering from Anna University, Chennai by 2006. He received his master of Engineering in Applied Electronics from Anna University, Chennai by 2008. He is working as an Assistant Professor in the department of Information Technology, Kalasalingam University. His areas of interest are Sensor Networks, Adhoc Networks and Signal Processing.

Balakannan S.P received his Ph.D. degree from the Department of Electronics and Information Engineering at Chonbuk National University, South Korea (2010). He has received his master degree (5 years integrated) from the Department of Computer Science and Engineering, Bharathiar University, India, in the year 2003. He has worked as a Project Assistant in Indian Institute of Technology (IIT), Kharagpur, India from 2003 to 2006. Currently, he is working as Assistant Professor in the Department of Information Technology, Kalasalingam University, Tamilnadu, India. His areas of interest include Wireless Network, Network Coding, Cloud & Green Computing, Cryptography, and Mobile Communication.