# Reliable Data Delivery in Manet using Adaptive Demand Driven Routing Protocol and Semi Markov Process

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

***Abstract— Reliable data delivery is an essential feature or element in the mobile adhoc network (MANET) and the devices often change their locations as they are not allocated any fixed infrastructure. In this paper, multicast routing protocols for military communications is proposed. Data security is a serious concern in military communications with MANET. This paper attempts to prove that data security can be achieved, by applying one of the most widely used algorithms, Adaptive demand driven routing (ADMR) protocol which provides routing done with rapid topological changes. For network survivability the node behavior model is devised by incorporating Semi Markov process. On the whole, the paper shows that reliable data delivery for MANET can be obtained by estimating the current performance of the network and by using Semi-Markov process when the forwarder node is isolated.***

***Keywords—MANET, ADMR, Markov Process***

## I. INTRODUCTION

The field of wireless mobile ad hoc network (MANET) and nodes are complimentary that both are crucial issues for discussion. Nodes [1] are primarily self-organized moveable electronic devices and require less infrastructure. Due to their large scale application, nodes have become the topic of discussion in the Internet field. MANET, similarly, has received lot of attention in special applications since they possess the ability to create network despite damage done to the built-in architecture. MANET has been a boon to policemen, fire-fighters and defence personnel at the time of casualties and emergency communication. On such complicated situations, MANET enables uninterrupted communication among people involved, thereby evoking a synchronized exchange of information.

In a wireless communication, the announcement in a network among the members or the hosts of the network and deprived of a static set-up are the issues to be addressed. These invoke a state of assistance during searching and rescuing operations, academic meetings and exchanges, business dealings and conferences, and more important, in the war-fare fields. The devices incorporated into the MANET are capable of mobility to anywhere at any specifications and are compatible to several devices for getting connected for operations. The armed forces heavily depend this MANET since the features are much feasible yet complicated on some occasions [2].

War field is always a place of various activities of animosity and secrecy in addition to safety. This condition creates a need for considering certain factors since MANET offers less features to armed forces than to the academic or commercial fields. A war field is a sensitive and restricted environment with regard to information security. So, it is natural that there must be accurate and authentic routing process in terms of bandwidth, range of radio waves, consumption of power and preservation of security.

A major scene in the war fare is the movement of a military tank moving around the places in an enraged manner. MANET ensures proper and perfect communication despite the movement of the tanks. Information exchanged are to be protected in such a way that the conversation is not intercepted by the enemies. The reason behind this is that any slippery of information through miscommunication process would be a severe threat. Even a minor lapse on the communication stream would result with heavy casualties and may end up with lot of unpleasant happenings. Minefield communication is the main means during such situations to divert or face the fighting enemies. For these sort of requirements, certain protocols are ideally applied and some of them are Hostile enemy, Trust models, QoS control, Radio power usage restrictions and Robustness.

Usually, the nodes found in MANET are unstable and minimization of is carried out by employing certain key protocols. They are overhead of routing protocols, Adhoc On demand Distance Vector routing protocol (AODV), Dynamic Source Routing protocol (DSR) and Destination Sequenced Distance Vector routing protocol (DSDV). However, there is a constraint with these protocols in the form of inadequacy. In addition to these protocols, the Adaptive Demand driven protocol (ADMR) is needed for improving the capability to instant reaction on modifications applied in topologies. This is because the approach involves the network modifications and delivery of data in a reliable and dynamic manner without any interference [3]. The ADMR is known for its act of identifying huge flexibility over the utility of GPS or any other additional locating data. Further, it is able to transform to the overflow mode for certain moments thereby retaining its state of common multicast procedure. For spontaneous and perfectly planned tree pruning, ADMR is ideal with inactive responses. ADMR is not involving any sort of periodical running such as whole network flooding of control packets or detection of neighbour nodes or table interaction routing.

Network Survivability plays a pivotal role in communication services liability [4]. The standard feature of the topology of an Ad hoc network is to maintain conversions in a dynamic manner. This is necessitated as a result of node mobility, randomness among the

Revised Manuscript Received on December 16, 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

*Retrieval Number: B11191292S219/2019©BEIESP*
*DOI: 10.35940/ijitee.B1119.1292S219*

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

channels, irrespective of the existence of node disasters or attacks to the security system. Ad hoc networks always insist on an essential layout in the form of a linked topology. Failure of this need results with no assured operations, especially forwarding or routing. The case is meant for QoS as well. This purports to the demand of survival among the community for heavy load of outgoing paths, so that each node engages in routine communication. Hence, it is propagated that the primary task for a network ability is the survivability of an Ad hoc system. If this is considered duly, then there will be an assured security for an associated topology. Such a consideration keeps the point of metric to be deemed on the common existence of malicious adversaries, disasters at select frequency and connectivity [5]. By keeping these factors on view, the nodes are categorized into four states viz. Cooperative state (C), Malicious state (M), Selfish state (S) and Failure state (F).

The rest of this paper is designed with following sections: Section II discusses various steps applicable with ADMR while Section III makes a brief describes the Semi Markov process and the classification of nodes based on the behaviour model. Section IV presents the investigational arrangement and effects, and Section V sums up the discussion with Conclusion and recommendation for future works.

## 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 [4]. 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.

The traffic model of multicast sender application is observed by ADMR in order to monitor the path breaks in the pruning tree. This results with the source withholding the information from sending to the network or the nodes. During the earlier occasions, protocols did the act of securing the limitations on repair techniques. When the flop occurred in the local repair, the global repair was alternatively employed. With regard to global repair, multicast forwarding state becomes null and void yet the necessity for effecting transparent conclusion message retained its validity. On certain occasions, the source may refrain from sending data temporarily so that there could be a breakage of monitoring link in the multicast forwarding tree. During these conditions, ADMR comes to the rescue by sending a restricted amount of keep-alives to enrich the inter-packet timings. When there is no transmission of information from the sender within the time frame and instead critical aberrations from distribution design are established, possibilities are there for a routeless lapse within the pruning tree. Thus, there will be a complete stoppage of keep-alives and repairing of the whole tree. Nevertheless, there could be occasions of inefficiency in keeping the routing condition in the system. On those moments, a significant deviation regarding the sender's message transmitting pattern will be indicated, exposing the probable idleness of the source. ADMR does the additional task of trimming every division of tree, though a bit much would be meant for forwarding. It is to be noted that the pruning choices heavily rely upon the absence of any inactive affirmation from downstream, instead of accepting the express trim data.

ADMR is able to locate the condition of mobility system being viewed as superior in letting convenient multicast condition arrangement and upkeep. This is possible even at the absence of GPS or locating data or extra regulator mobility. ADMR chooses the option of flooding the information data as a result of large scale mobility being distinguished. Sooner, once the portability diminishes, the multicast routing resumes the productive job. In fact, ADMR plays a strong role by supporting the conventional IP multicast services. This naturally endeavours the receivers to be ready to get multicast packets which may be transmitted by any source. From these new loads of source particular multicast there originates an advantage for a recipient to get link between a multicast group to specific source. This is same with the nodes, like multicast benefit models, there is no requirement of recipient position within a group. Sources, for instance, do not seek any announcements based on a perception that gathering occurs with multicast directing packets. In addition, sources do not require to pronounce their existence as a part of multicast source.

Recipients may be located anywhere in the system that they may not be identified by multicast senders within a specific group. Similarly, the beneficiaries do not identify the location of the senders. The outline of ADMR is based on the assumption that there could be a mobility of nodes in the system on demand. Also, the presence of components may end up with loss of any packet during the transmission. Packet impact, remote obstruction and weakening of flag due to loss or separation are few examples. The design of ADMR is in view of the systems built out of gadgets, having omni-directional receivers. This enhances the function of communication being caught by a particular node within the remote transmission. Hence, ADMR is uniquely patterned that it is fully appropriated and independent from any stipulated coordination or control.

When multicast group does not get any cause or receiver, then control packets are not transmitted by ADMR. Similarly, when there is no recipient for any information, ADMR just propagates and spreads sensitive or rare information. This is to regain the packets instead of transmitting or controlling the information with it.

The routing is not in need of any momentary system full flood of control packets. Nor there is any need for distinction of neighbour or non-frequent routing table trade. These factors prove the superiority of ADMR that none of the previous multicast convention in the world has matched ADMR in this regard.

In practice, an amplified source-established tree is constructed by each of the multicast ADMR sources. This is called a source mesh, through which the multicast packets are sent from the source to the multicast beneficiaries. Multicast convention adapts itself by adjusting to the sending pattern and it allows productive identification of broken connections and flaws in steering state. This leads to the presumption that there would not be any keep-a live during the multicast task, which enables sensing of information from separation.

In a system, multicast correspondence is effected when the sending state is built and kept up. This is achieved by multicast senders and recipients when they utilize ADMR coordinates. ADMR involves in adaptive screening of the right process of multicast sending state. It acts to repair such a state gradually during the time when at least one recipient or even a sending network openly ceases to function with the sender. The conventional IP multicast benefit model of enabling collectors is bolstered by ADMR. By this, multicast packets sent by any of the senders could be gathered displaying a multicast benefit update in source-particular. This is because, any of the recipients may include itself as a multicast to the particular sender. In both the models of multicast benefit, node does not seek to be a beneficiary for gathering the packets since it is not sure of the capacity to send them. Therefore, senders desist from declaring their intention or goal with regard to increase of multicast packets. In normal conditions, S sends these packets along the limited mesh via the tree so that the individual recipient in the multicast group can easily gather. ADMR is noted for its performance of programming the pruning of branches of the multicast tree, which is not mandatory for future purpose.

The absence of affirmations aloof from downstream instead of the receipt of an express pruned message determines the pruning of choices. ADMR tends to work independently in the unicast convention and is exploited as a segment of specifically designed system. ADMR is capable of continuous work execution with any unicast convention or even in the absence of a unicast routing. It is apparent that there cannot be any progress or improvement in modularity and transportability when there is at the absence of valuable data sharing between multicast routing and unicast routing.

When G represents the multicast group among the multicast sending state, S refers the sender in ADMR. Thus, S represents any sender, which is otherwise, referred as a loosely designed multicast sending tree. As with these references, S sends individual multicast packet along with the most limited mesh way via the tree. The individual recipient among the multicast gathering, in turn, collects the packet. Thus, ADMR performs the function of programmed trimming of multicast tree divisions, since such divisions will not be required for sending information in future. The choices of trimming occur when inactive affirmations are absent not at the receiving of express crop data. As mentioned earlier, ADMR is capable of independent activity, as it can get along with or without unicast convention. Despite having this flexibility of transferring data either among unicast or multicast convention, ADMR still lacks particularity and mobility.

Figure 1 shows the packet surge wherein the tree flood in the node is represented by a multicast sending tree. This is proportionately increased depending upon the number of nodes and number of packet surges, leading to flooding of packets. Hence, the flooding in the multicast sending tree takes up the role of a forwarding group, as illustrated in the FGMP convention. In addition, this phenomena is common in ODMRP yet with an exception that the sending tree is individual not shared one among the gathering.

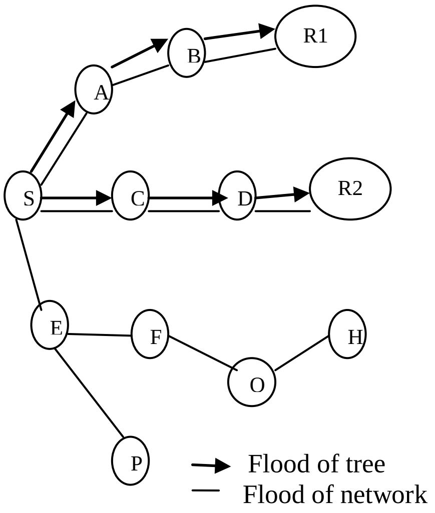

Fig 1 Tree flood Vs Network Flood

ADMR's task is to trim or pruning the branches of the multicast tree when such tree is not needed anymore for forwarding the packets. Pruning is the result of downstream indication of inactive acknowledgment, which paves way for facilitating receipt of short messages actively. ADMR is an integral segment of an Ad hoc network, being designed to be self-styled over the unicast protocol. ADMR, as mentioned previously, is capable of performing with or without unicast protocol and current usage finds ADMR in bidirectional links. Nevertheless, ADMR is unique in that it is designed to be compatible with unidirectional links in an appropriate manner.

A data packet having a broadcast or multicast end address engages in flooding the ADMR header. This ADMR header has a flag which indicates the pattern or type of flooding and in case of extreme packets, the flood flag type will expand to a tree flood of the packet. This results with the promotion of the best among the nodes which can be forwarded to the multicast promoting tree. In such cases, the packets are endorsed with the source address (creative address) and the destination address (the multicast group address). Once the node receives any such packet, then it verifies the authenticity of the source and genuineness of the membership of that packet. Then only it decides to send to forward the packet. This makes the packet to move along the tree from the sender till it reaches the receiver group. Further, the tree does not have any schematized movement within the tree or self-styled progress in its movement (Figure 6.1). The flooding of the packet to all the nodes depends upon the classification of the flood type flag and indication of the network flood by the ADMR header. Node table of each node and scheme of ADMR packet header undergo checking in both types of flooding. Ultimately, the packet is sent at least once by the ADMR header.

Whenever a packet is received by a node, it is forwarded. Then, the receiving node makes an attempt to equal the sum of hop in both the ADMR header of the received packet and the hop recall on the source of the packet, as specified by the node's entry table. When the new hops turn out to be less than the hops accounted inside the node's table entry, then the node makes an appraisal of the quality of the new hop count number. Further, the prior hop address is set in the entry to MAC-layer source address, which sends the packet normally. Also, there will be an increase of hop count field in the packet's ADMR header whenever ADMR receives the packet forwarded by the node. As a result, the packet's MAC-layer source address is copied into the ADMR header found in the earlier hop address field.

When a node S creates a multicast packet for a group G ( though it is not a dedicated sender), then S cannot maintain a sender table access for G. This is to mention that S involves in creating and employing a new sender table entry for G. All these tasks bring out the avoidance charge, occurring out of the entry of inter-packet time. This avoidance charge or time entry can be assumed as a creation from an IP port numbers and are used within the specified packet. In case an API becomes accessible, then the port number may be transferred by using the transfer application. To be more specific, ADMR header is inserted into the packet by Node S and subsequently flagged to forward the packet for flooding in network.

Once this packet is sent, node S buffers for a long time to ensure the multicast packets patent with group G. Hence, there is no act of sending the packets as soon as they are generated. In another way, this task enables the formation of routing state in the network among the interested receivers within the group, as well as the senders. Once S gets at least one receiver join the packet, then other shielded packets are sent to the group by S. These packets turn out to be the multicast packets. The exchange of packets avails a fresh section with the conversion of a brand new substance. Majority of subsequent multicast packets from S, getting entry into G, undergo flooding only with the existing members of multicast forwarding tree, which would be known to this group and sender as well.

Such authentication is done by node S by using a network flood instead of a tree flood belonging to the subsequently sent multicast data packets. The time allocated for sending or forwarding each of the nominated packet, possibly as a grid flood, is longer until a measured past rate of time is noted down. This calculation of time depends upon certain factors like recurrent wireless meddling or fleeting screen of the Adhoc network. The research examination was carried out to calculate the time pattern for each information packet. The results showed that it took 5 seconds for the first network flood packet sent as network flooding. The next first data packet was sent after every 10 seconds to forward the network flooding. Then, the process was examined to calculate after every 30 seconds. The examination showed that the forwarding of municipal floods was subjected to pass through S to reach G.

Multicast routing in wireless Adhoc networks encompasses a number of rules. Some of them are bound with on-demand tools to be demonstrated with proper evidences, while others rely upon the periodic and updated functional devices. This research study is designed to fall on the lines of the earlier one thereby the discussion surrounds over the multicast protocols.

Multicast Adhoc On Demand for Distance Vector Protocol (MAODV) has a “Group leader” inside it for each of the multicast architecture. This group leader takes up the act of overflowing a hello control communication throughout the Adhoc group normal ADMR process. However, this happens occasionally and not regularly. Once this hello communciation is received by the multicast capitals and receivers, they respond with a reply message, allowing the forwarding state of the group at all the paths of message supply. The tree thus formed gets rooted on the group leader. This tree is much similar to the one created for On Demand Multicast Routing Protocol (ODMRP). It is in that tree that packets transmitted with the assistance of source has the travel path, and proceed closer to receivers of the group. In ODMRP the tree can be restructured by active supply overflows, which is in contrast to MAODV in which the multicast receivers and sources turn out to be the collection leaders. As such, when there are no senders for any group, the multicast receiver starts flooding the network occasionally. MAODV seeks detection of neighbour nodes periodically, for the sake of hyperlink breaking discovery. When the node withholds sending of any additional broadcast packet during the break period, this neighbour detection forwards the occasional hello messages to every node within the group locally.

Temporarily Ordered Routing protocol (TORA) is an on-demand protocol for unicast routing in Adhoc networks. The elevation of this protocol is the determiner for Lightweight Adaptive Multicast (LAM) protocol, whose layout got inspiration from a core-based protocol, since a core assists every group in this LAM. Receivers are a part of multicast group, which is formed by setting up a route to the centre node of the group, to which the nodes intend to enter into. The core is a crucial element that each source forms a route towards the core, in order to unicast all its packets to the core. The core, in turn, forwards these packets to the receivers of multicast.

LAM's description does not consist of Core voting procedures. TORA does the function of discovery and renovation of link, as a part of its even unicast operation. The results derived out of LAM and TORA invoke fresh expectations that could be employed in subsequent processes. The interesting facts derived thus are: there is a swearing by decrease-layer protocol on each node having whole neighbour realities; all communicated packets are dealt with properly much in abeyance to the broadcast; each node is capable of broadcasting to all its neighbours. It should be asserted that detection of tree breakage is made through sensing of neighbour periodically, as in MAODV.

## III. SEMI MARKOV PROCESS

Any task is prone to face or counter threats, accidents, untoward situations, lapses or flaws, during the process of achieving the goal. However, such factors can be overcome if the capabilities are employed properly. In this research study, these hindrances and constraints play their role in the structured system, inviting Network Survivability [7]. Hence, it is of paramount importance that network survivability should be provided with distinction, clarity and concrete approaches. More specific, there should be mathematical accuracy with regard to Adhoc networks. The standard structure of an

AdHoc network is equipped with conversions in a dynamic manner. This is due to the nodes mobility and randomness with channel despite the nodes are protected from any disasters or attacks. The most essential layout to be concerned with Ad hoc networks is the linked topology, the deprival of which lead to inoperative results (regarding forwarding and routing), more so to QoS. Thus, the survival of this network community lies heavily on the decision of having an outgoing path for each node, to ensure proper communication. These prime factors evoke the thought of network survivability on the basis of associated topology. It is this topology through which the malicious adversaries, random disasters and misappropriation of connectivity as metric can be controlled or wiped out. The entire study in this research approach centred around two sorts of behaviours, namely black –hole attack and Jelly-fish attack [8].

The type of node determine the circumstances of the node and they are signified as {C, S, M, F}. The stochastic model for the evaluation of the disclosed outcomes of these nodes was proposed and devised Xing and Wang [9].

The diagram given below illustrattes the state transition of the homogeneous Semi-Markov Process (SMP).

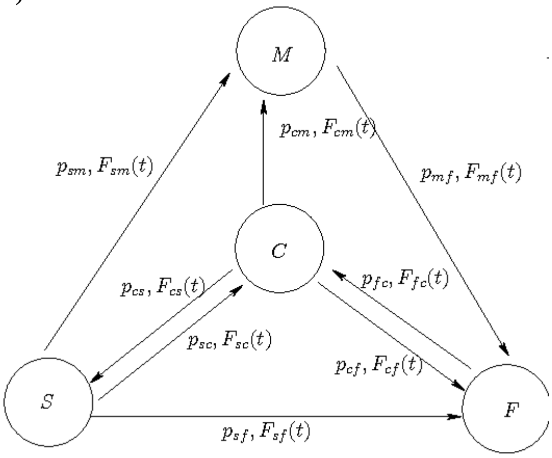

Figure 2 The SMP for node behavior evolution

Node Isolation is a remedy for failure and misbehavior occurring in the node, due to routing information determining the communication between nodes.

The cooperative probabilistic matrix can be constructed by using Figure 2 and as follows:

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

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

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

Using these values the limiting probability of various states of the node can be derived as,

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

The stochastic assets of node behaviour are governed by several factors and phenomenon. The application of heuristic technique, based upon the effectiveness of the heuristics evolved in that particular heuristic approach. If there is an efficiency in the approach, then it will facilitate the analysis on the impact of a specific non-static aspect. Further, it partakes node movement as well. It is a well-known presumption that the survivability of a network depends upon the process of state distributions. This has an impact or influence upon the limiting probability’s performance in cementing the difference among the network survivability. The limiting possibilities are influenced by unique and dynamic factors. Thus, it is shown that the Semi-Markov node behaviour model, as designed and employed in this research work is capable of offering a vast mathematical framework to illustrate the node behaviour. The same model enhances the scope of calculating the effect of a large scale random dynamics prevailing in the network survivability, aided by its state behaviour distribution.

## IV. IMPLEMENTATION OF ADMR WITH SMP

The process of ADMR with SMP is clearly illustrated in Figure 3. Initially, a whole lot of specific number of devices in the military areas with a dynamic movement of devices is used to create MANET. The multicast group is created after the completion of the node deployment. The group node is identified by limiting the probability. According to this, the probability of a node being in a cooperative state is 0.6877. So, the limiting probability value of a group node chosen should be greater than or equal to 0.6877. If not, the node will select some other node as a group node in the forward direction.

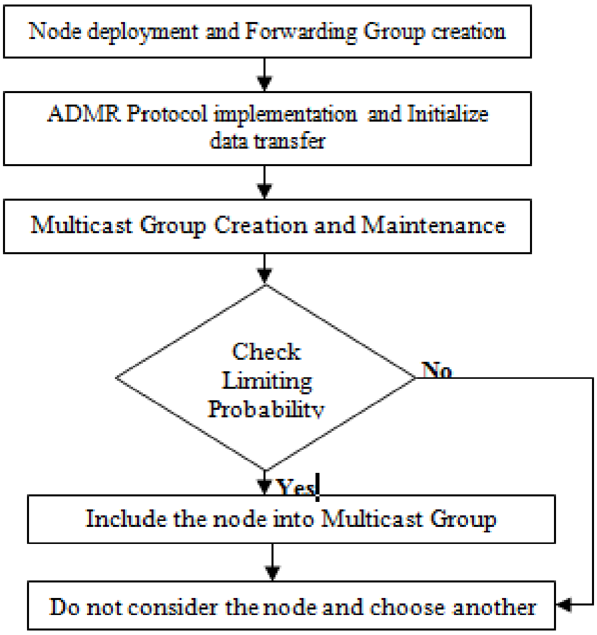
Node deployment and Forwarding Group creation
ADMR Protocol implementation and Initialize data transfer
Multicast Group Creation and Maintenance
Check Limiting Probability
No
Yes
Include the node into Multicast Group
Do not consider the node and choose another

Figure 3 Flow diagram illustrating ADMR with SMP

.

## V. SCENARIO STUDY AND SIMULATION RESULTS

Simulation Setup The performance of ADMR with Markov process was analyzed by simulating the algorithm in NS-2 and comparing it with ADMR protocol [13]. To evaluate The individual performance of ADMR and the ADMR with Markov process, was analyzed by simulating the algorithm in NS2 and comparing both the results. From the simulation observation, based on an assumption there could be 100 nodes in the simulation area. Random waypoint was formed in the mobility model, to enable the nodes move freely. The simulation results showed that minimum 900 nodes would be required to complete the task. The bit rate was replicated by setting the traffic pattern as constant. The estimation of performance was made upon the parameters such as packet delivery ratio, average end to end delay and throughput.

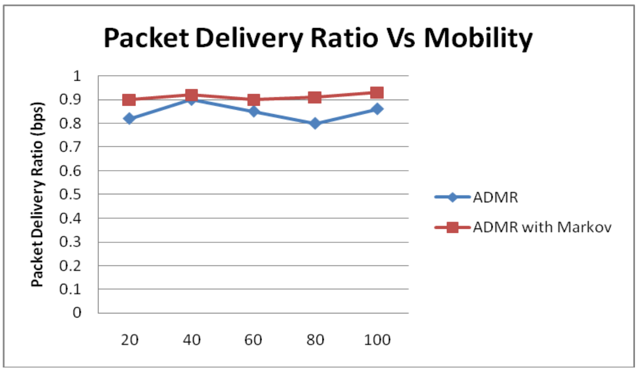

Figure 4 Packet Delivery Ratio

Fig 4 illustrates the comparative performance of ADMR and ADMR with Markov process. It can be observed that there is an improved performance and better packet transfer ratio when Markov chain was included in ADMR method.

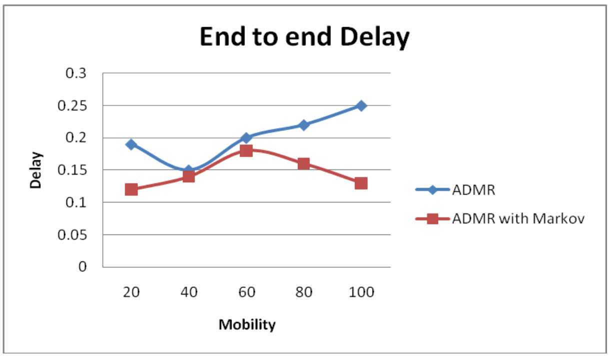

Figure 5 End to end Delay

Figure 5 shows the comparative analysis of delay factor, between ADMR and ADMR with Markov process. From the figure, it can be observed that there is a considerable reduction of overall delay of MANET when the Markov chain process is incorported with ADMR protocol.

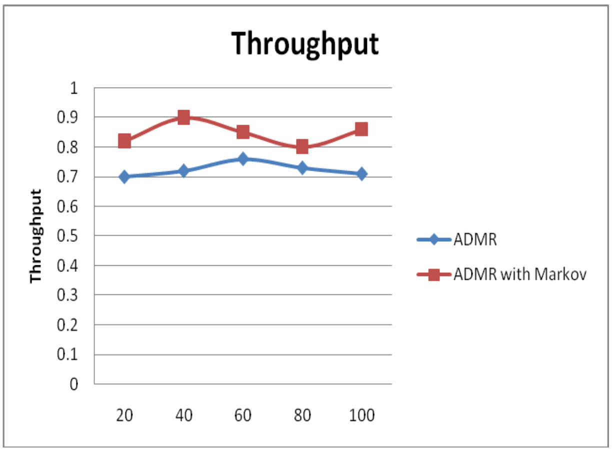

Figure 6 Throughput

Figure 6 illustrates the throughput comparative analysis of throuhgput, between ADMR and ADMR with Markov process. The figure proves that there is a liner increase in Throughput of ADMR with Markov process with the increase in number of nodes.

To sum up, ADMR and Markov process outperforms normal ADMR process with respect to Throughput, End-to-End delay and Packet Delivery Ratio .

## VI. CONCLUSION & FUTURE WORKS

In this paper, a solution for consistent data delivery for MANET is proposed. From the study, it was observed that the position based opportunistic routing method offered better Packet delivery ratio and throughput. Markov chain process is added for improving the security services of MANET. The identification of the malicious node and selfish node was carried out by employing ADMR protocol. The simulation results proved that ADMR with Markov process yields comparatively better performance than normal ADMR protocol. This Adaptive demand driven routing method is basically a tree-based multicast routing protocol. This work may further be expanded with any kind of mesh Multicast routing protocol for availing better robustness and reduced control overhead.

## REFERENCES

[1] Durka Devi K, Maragat harajan M, Balakannan S P “Reliable Data Delivery 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] 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

[5] Lusheng JI and Scott Corson M, “Explicit Multicasting for Mobile Ad Hoc Networks” Journal of Mobile networks ans applications, pp-535-549, 2003

[6] 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

Retrieval Number: B11191292S219/2019©BEIESP
DOI: 10.35940/ijitee.B1119.1292S219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

[7] 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.

[8] 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

[9] 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.

[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 he has 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.