IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-7 E-ISSN: 2347-2693

Selfheal Stable Routing Protocol for Ad-hoc Network

Rosy pawar[#1], Ashwani Kush [#2]

[1*]Dept. of CSA, Kurukshetra University, Kurukshetra, India
[2] Dept. of CSA, Kurukshetra University, Kurukshetra, India

**Corresponding Author: rosy_pawar@yahoo.com*

Available online at: www.ijcseonline.org

Received: 22/May/2017, Revised: 07/Jun/2017, Accepted: 12/Jul/2017, Published: 30/Jul/2017

Abstract— Wireless networking is a new emerging era. It has potential applications in extremely unpredictable and dynamic environments. Individuals and industries choose wireless because it allows flexibility of location, whether that means mobility, portability, or just ease of installation at a fixed point. In mobile ad-hoc network, mobile nodes are continuously moving from one location to another. Thus, MANET topology can change often and unpredictably. Mobility of nodes is one of the major issue of concern in mobile Ad- hoc network because it causes a link failure. In this paper, a new scheme has been suggested which would help mobile nodes to maintain routes to destination with more stable route selection. This makes route maintenance and recovery phase more efficient and fast. The performance of the proposed routing protocol named as Selfheal Stable Routing protocol (SSRP) is evaluated some major performance metrics which include Packet Delivery Ratio, throughput and End to End Delay. The study is based on simulation runs adopting CBR traffic pattern taking care of node failure scenarios.

Keywords—Ad-hoc network,self Healing Network(SHN) ,Selfheal Stable Routing Protocol(SSRP) ,AODV

I. INTRODUCTION

The modern era has witnessed wireless networking potential applications in extremely unpredictable and dynamic environment. The challenges of wireless communication are that the environment that wireless communication travel through is unpredictable. In developing broadband digital network, a short service outage such as a link failure can cause a serious effect on network services. This is because of the volume of traffic carried by a single node. If the connection fails, it will take long time to reestablish the connection and it also increase the traffic volume. Self-healing algorithms have been recognized as a major mechanism for providing the fast restoration. A self-healing system [1,2,3] should recover from the abnormal state to normal state and start functioning as it was prior to the failure. One of the key issues associated with self-healing networks is to optimize the networks while expecting reasonable network failures [3,4,5,]. Self-healing network (SHN) [6,7] is designed to support transmission of messages across multiple nodes while also protecting against recursive node and process failures. It will automatically recover itself after a failure occurs.

Critical issues [8] in self-healing systems typically include: Maintenance of system health, recovery processes to return the state from an unhealthy state to a healthy one.

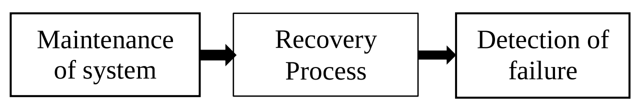


Figure 1: Self-healing cycle

Rest of the Paper is organized as; Section II gives emphasis on self-healing network. It gives an idea of self-healing technologies, proposed self-healing routing scheme has been explained. In Section III Simulations and results are discussed in Section IV and conclusions are in last Section.

II. METHODOLOGY

The proposed Selfheal Stable Routing protocol(SSRP) helps to increase the stability of route in AODV with avoidance of route break. In this the route stability of the node is measured by three parameters as (i) Node energy (ii) Node mobility and (iii) Traffic load

These three parameters help to find out the stable route from source to destination.

I. Calculation of Route Stability in Self-heal Stable Routing Protocol (SSRP)

In order to allow more stable routes for data transmission in MANET we propose to include a new field, called Route

Stability(ROS) route request packet**.** It measures the stability of route during route request phase (RREQ) of AODV. In AODV hello packets are sent periodically to maintain the routing table, so that each node knows about the connected neighbors. Each node broadcast the HELLO packet with Node stability value (NSTV). if node Stability value of a hello packet is larger than the threshold value then node adds the sender of the Hello packet as its neighbor.

Following steps are included for stable route discovery: -

a) The node stability value(NSTV) is added in the Route stability value(RSTV)of RREQ packets by source node and sends it to the neighbor nodes.
b) Neighbor node compare its own node stability value with RREQ packet stability value.
c) The lowest value is selected.

   If NSTV<RSTV then
   RSTV<-NSTV in RREQ
   packet
   Forward RREQ packet to the neighbours and so on.

d) New path is discovered with the lowest NSTV in route stability value.
e) If the destination node receives more than one RREQ packets then in response to the RREQ packet with largest route stability value.

Algorithm 1: Calculation of minimum route stability value of the path

ROS-value (SN, RN)

SN- sending node

RN- receiving node

{if(NSTV[SN]<NSTV[RN])

Update NSTV[SN] in RREQ packet;

}

Based on the above algorithm Path for stable routing is equal to the lowest node stability value.

RSTV-route stability value RSTV(P) = min (NSTV (source node) …. NSTV (Intermediate node) …. NSTV (Destination node));

Where RSTV(p) > value A //value A is selecting value for route stability.

II. Calculation of Node Stability value NSTV(n) in SSRP

Node stability value can be calculated on the basis of 3 different parameters [9]:

a. Level of energy of node (LOE)
b. Mobility of node (MON)
c. Traffic Load (TL)

NSTV of a node is calculated periodically and transmit to the network through HELLO packets

If any node receives larger NSTV value than the predefined threshold value A from some node, it adds that node as its neighbor node.

NSTV of a node is given by

NSTV(n) = LOE+MON+TL

Where NSTV(n) > value B

II.I Level of energy of a node (LOE)

In our model of energy, the level of energy(LOE) of a node refers to the available energy of node n which depends on total initial energy and consumed energy[10].

Available energy = total initial energy + consumed energy

AE = TIE(n) + CE(n**)**

Where AE(n) > Value C

Value C is the threshold energy level for node

The Consumed energy(CE) depends upon the energy used in transmitting and receiving of a packet.

$CE(n) = E_{transmit}(N) + E_{receieve}(N)$

Energy used in transmitting and receiving of a one packet is calculated as follows [11]: -

$E_{transmit}(n) = P_{transmit}(n)*DOT$

$E_{received}(n) = P_{received}(n)*DOT$

Where $P_{transmit}$ is power used n transmitting one packet

$P_{received}$ is power used in receiving of one packet

DOT = Donates the duration of transmission (transmit + received) of a packet at node

In our proposed scheme, the algorithm chooses only those nodes in the route that have higher energy level than Value C

II.II Mobility of nodes(MON)

In a dynamic network such as MANET, mobility of nodes cannot be ignored. They play important role in maintaining stable route. Therefore, mobility of nodes can be considered as the deciding factor for route setup, so that better route stability can be achieved. In our proposed scheme we adopt the policy given in [12], where a node with average lower displacement has a higher chance of being an intermediate node. Weights are assigned to each node which shows their respective displacement value i.e. the node with lower average displacement as a higher weight and nodes with higher displacement has a lower weight.

Mobility of a node is calculated by the average distance covered by mobile nodes in a given time slot

Calculation of mobility of node as an average speed

$$MON_T(n) = \sum_{i=1}^{N} \frac{SP_{\Delta t}(n)}{T}$$

Where SP(n) is a speed of node in time duration T.

$MON_T(n)$ <VALUE D ,the threshold mobility value for a node.
The speed of the node is given by following expression

$$SP_{\Delta t}(n) = \frac{DC_{\Delta t}(n)}{\Delta t}$$

DC is the distance covered by the node n at time slot Δt i.e from time t-1 to t
From position $P_{t-1}(x,y)$ to $P_t(x,y)$
$DC_{\Delta t}(n) = \sqrt{(x(n)_t - x(n)_{t-1})^2 + (y(n)_t - y(n)_{t-1})^2}$

II.III Load Estimation
Traffic load of a node is measure by total cost incurred in sending /receiving packet by node. If time arrival b/w sending/receiving two packets is ΔT seconds and the size of packet is ΔL bits, then traffic load of a node is given by the equation[13]

$$TL(n) = \frac{\Delta L}{\Delta T}$$

Route Discovery in Selfheal Stable Routing Protocol. In the proposed scheme a new field route stability RSTV is introduced in RREQ packet which indicate the route stability value of a path from source node to destination node. Initially all nodes are assigned high stability value.

Algorithm 2: Route Discovery.
Step1: the source node initiates a route discovery process by broadcasting a route request packet to all the neighboring nodes. RREQ packets contains the NSTV of source node.
If (NSTV[S] > value B then

Broadcast the RREQ packet to neighbors with NSTV(S)
Else
Not able to generate RREQ packets

Step 2: Neighboring node n receives RREQ packet. N may be an intermediate or destination node.
If (NSTV[n] > value B then
{
If (n is intermediate node) then
{
N calculate the RSTV from RSTV_value (S,N)

Update RSTV field in routing table, update RSTV field in RREQ packet and forward it to all neighbouring nodes of N.
If (N receives other RREQ packets for same sequence no from other sending nodes) then

Discard these RREQ packets.
}

Else // n is destination node
If (n receives multiple RREQ packets within a time window , which starts from the first arrival of RREQ) then
N picks the largest RSTV of RREQs

If (RSTV[n] > value A) then
{ N sends back reply packet as RREP to the source node S
}
Else
{N discard the RREP packets}
}
Else
{N discards the RREQ packets
}
Route Stability in Self Heal Stable Routing Protocol(SSRP)
Source node starts transferring data packets to destination node once the stable route is discovered and periodically checks the stability of route.
During data transmission via stable route if any node becomes a instable node i.e. having NSTV less then predefined threshold value or link breakage is detected , the intermediate node informs the upper node which initiates the route discovery process. If upper node is unstable to find the new route it sends rerouting request (RERREQ) packets back to the source node.

Route breaking avoidance algorithm
In this algorithm, each node periodically calculates the NSTV and transmit to neighbors through HELLO packets to maintain the connection. During the transmission if any node is having NSTV less than threshold value B then intermediate node (IN) informs the upper node (UP) through unstable node detection packets (UNN). Upper node then reinitiates the route discovery process. A new field Unstable node detection(UNN) is introduce to detect unstable node in route maintenance.

IN- intermediate node
UP- upper node
UNN- unstable node
Algorithm- 3.
Step 1: if (IN. NSTV< value B) then
{IN informs next immediate node UN through UNN packet}

Step 2: if (UN. NSTV <value B) then
{UN declares ROUTE ERROR, UN sends RERR packet to the source node and destination. source node reinitiates the route discovery process.
Else
//UN checks neighbour table.
If (destination node is the neighbour node of UN) then
{UN removes IN from the existing path
UN forwards the all data packets to this updated path.}
Else

{UN initiates the route discovery process to the DN.
}

III. RESULTS AND DISCUSSION

The performance of proposed protocol is evaluated using simulation tool NS-2.35 and is compared with AODV and DSR protocols. The performance evaluation is done on the basis of following performance parameters:

Packet Delivery Ratio: The ratio of the number of the successful arrived packets to the number of all packets transmitted by source. The larger value indicates that the more data packets are successfully delivered to destination.
End – to – End delay: The average time spent on data packets transmission from source to destination, including all possible types of delay during transmission.

Throughput: The throughput is defined as the total amount of data a receiver receives from the sender divided by the time it takes for receiver to get the last packet. The throughput is measured in bits per seconds.

The Performance of Proposed Protocol is evaluated using simulation tool NS-2.35 and is compared with AODV and DSR routing Protocols. The simulation network area is considered as 1000m × 1000m with 20 and 50 nodes in each simulation run. A TCL script has been written using random waypoint model and all efforts has been made to keep it bias less and same for all three protocols under testing. Proposed scheme has been shown as 'NEW' and AODV and DSR are named as it is in graphs. Though the results were calculated using 10,20 and 50 nodes. For this paper 20 nodes scenarios have been discussed. Table shows the parameters used for simulation.

Table 1

ENVIRONMENT SIZE	1000 X 1000
PACKET SIZE	512 BYTES
QUEUE TYPE	DROP TAIL/FIFO
QUEUE LENGTH	50,60
TRAFFIC TYPE	CBR
PROTOCOLS	AODV,DSR, NEW

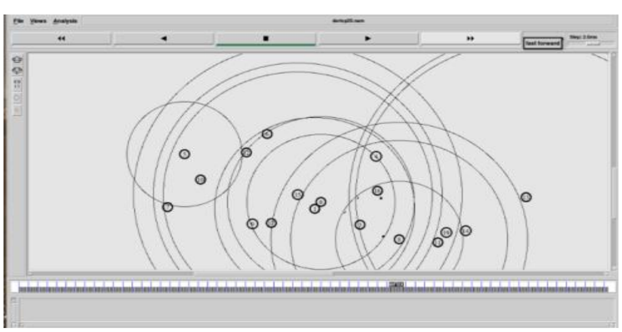
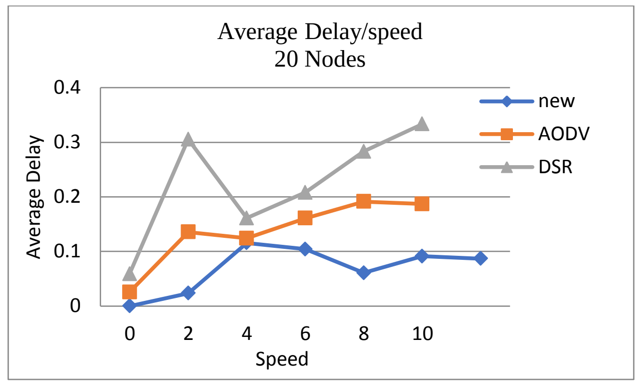


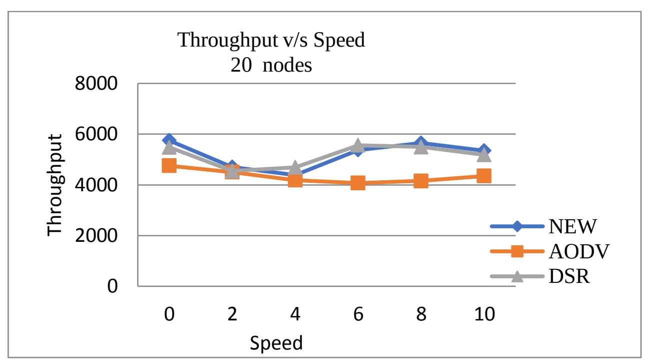
Figure 2: Showing NAM file using pause time as function

Figure 2 shows a snapshot of scenario being run using a TCL script and results are shown using Network Animator tool , which is part of Network Simulator. Trace file is created after executing the simulation. And results are calculated using this trace file. The PDR, Delay and Throughput are calculated using program and the data values have been shown in Graphs.



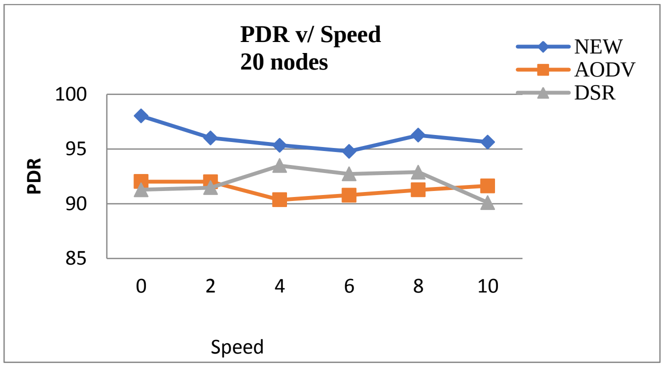
Graph 1

In spite of all the calculations still 'NEW' scheme is able to carry out delay within limits. This is due to the route stability mode. The 'NEW' scheme carries out calculation part before the route repair phase and is able to carry out repair operation faster. The gain is significant and helps in carrying out operation of data transfer at a faster rate.



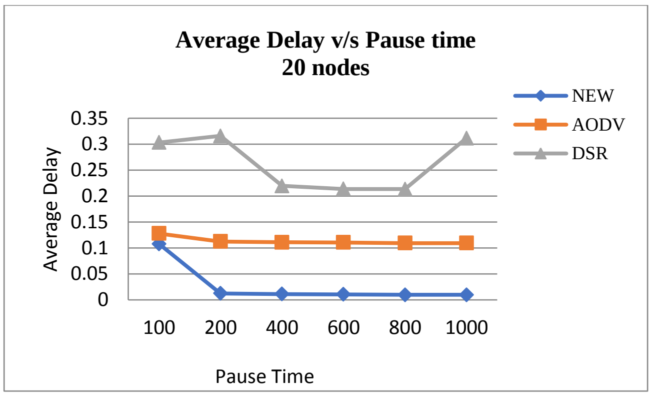
Graph 2

Graph number 2 is representation of throughput with speed as a function. Speed of 10 m/s is almost like a car moving in a street. Though the graphs are almost touching the scales of each other, still it can be said that 'NEW' is almost reaching the maximum value at all the speeds making the target almost same as that of AODV and DSR. Value is higher in almost all cases against AODV.



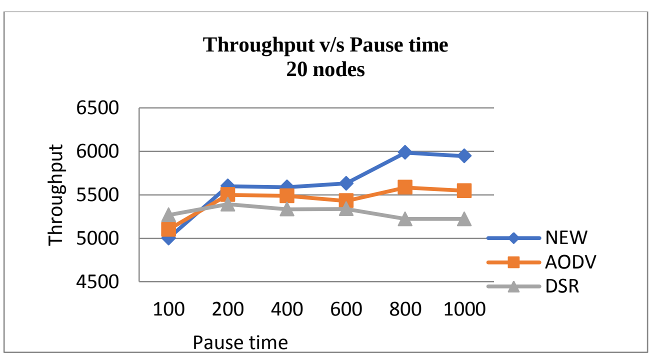
Graph 3

Packet delivery ratio, which is main metrics used has shown improvements in all cases as is evident in Graph 3. It can easily be seen that even at higher speed of 10m/s there is gain in PDR. This parameter clearly makes the algorithm a successful attempt in achieving the stable routing.

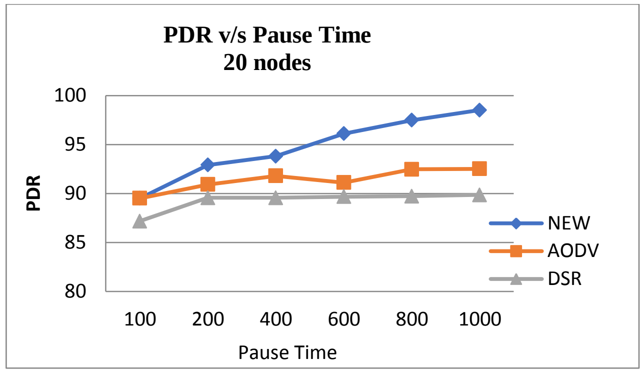


Graph 4

The same scenario was used for pause time as a function in place of speed. Pause time from 0 to 1000 has been used with simulation time increased to 1500 seconds. Pause time of 0 shows maximum movement of nodes throughout the simulation time and 1000 delayed one. As is evident from Graph, throughput is more in case of NEW scheme. Major comparison is cited in terms of AODV as the modifications are done on AODV and it is clear that there is gain all the way from pause time of 100 to 1000.



Graph 5



Graph 6 : PDR using pause time as function

Packet delivery ratio is major parameter for any protocol success. This parameter shows in graph 6, that in all cases PDR is more in all cases. It has a gain of 3% to 7 % which is significant. The process is true for all cases of pause time, whether the movement starts at pause time of 100 or at 1000.

IV .CONCLUSION

A new scheme has been proposed and an algorithm showing repair of AODV has been submitted. The algorithm requires changes in Repair phase of AODV and it has been incorporated on AODV. The comparison has been done using existing schemes ADOV, DSR and the 'NEW'. The simulations have been carried out using NS simulator and results clearly indicate that 'NEW' scheme is more stable and gives much better packet delivery in all cases. The efforts are on to add more features of algorithm in the AODV. These features are energy parameter and fading effects that the protocol causes in many cases.

V. ACKNOWLEDGMENT

Author is thankful to Dr Ashwani kush, Associate professor computer science, University College, for his valuable suggestions in preparation of this article. I am feeling very grateful and Honoured to present this paper in an esteemed Journal "International Journal of Computer sciences and engineering (IJCSE)".

REFERENCES

[1]. Glab, M., Lukasiewicz, M., Streichert, T., Haubelt, C., Teich, J.: *Reliability-Aware System Synthesis*. In: Proceedings of DATE 2007, pp. 409–414, 2007.

[2]. Robert Poor, Cliff Bowman, Charlotte Burgess Auburn, "*Self-healing networks*", ACM Queue, pp.52-59, 2003

[3]. Hiroyuki Fujii and Noriaki Yoshikai. '*Restoration message transfer mechanism and restoration chracteristics of double-search self-healing atm network*'. IEEE Journal on Selected Areas in Communications, Vol.12, Issue.1, pp.149-158, Jan 2004.

[4]. Ryutaro Kawamura, Kenichi Sato, and Ikuo Tokizawa, "*Self-healing atm networks based on virtual path concept",* IEEE Trans. Communications, Vol.12, Issue.1, pp.120-127, Jan 2004.

[5]. K. Murakami and H. Kim. "*Optimal capacity and flow-assignment for self-healing ATM networks based on line and end-to-end restoration",* IEEE/ACM Transactions on Networking, Vol.6, Issue.2, pp.207- 221, Apr 2008

[6]. Amit Gupta and Dhananjay Bisen, "*Review of Different Routing Protocols in Mobile Ad-Hoc Networks*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.5, pp.105-112, 2015.

[7]. Cankay, H.C., Nair, V.S.S.: "*Accelerated reliability analysis for self-healing sonet networks",* SIGCOMM Computer Communications. Rev, Vol.28, Issue.4, pp 268–277, 1998.

[8]. Vishal Paranjape and Vimmi Pandey, "*An Improved Authentication Technique with OTP in Cloud Computing*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.3, pp.22-26, 2013.

[9]. Sanjeev K.prasad and Karamjit Bhatia "*RSAODV: A route Stability based Ad Hoc on Demand Distance Vector Routing Protocol for Mobile Ad hoc Network",* International Journal of Wireless & Mobile Networks(IJWMN) vol.6, no- 6, December 2014.

[10]. Umesh Kumar Singh, Jalaj Patidar and Kailash Chandra Phuleriya, "*On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks*", International Journal of Scientific Research in Computer Science and Engineering, Vol.3, Issue.1, pp.11-15, 2015.

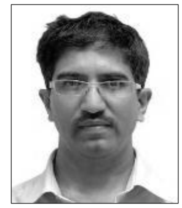
[11]. Virali Girdhar and Gaurav Banga, "*A Comparative Analysis of Different Movement Models in MANET*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.6, pp.9-13, 2015.

[12]. Aditya Singh Mandloi and Vineeta Choudhary, "*Study of Various Techniques for Data Gathering in WSN*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.3, pp.12-15, 2013.

[13]. B.Karthikeyan, S. Hari Ganesh, J.G.R. Sathiaseelan,and N.Kanimozhi, "*High Level Security with Optimal Time Bound Ad-Hoc On-demand Distance Vector Routing Protocol (HiLeSec-OptiB AODV)*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.4, pp.156-164, 2016.

Authors Profile

Ms. Rosy received the Bachelor degree in computer science and application from Panjab University, Chandigarh, Masters in Computer Application from Kurukshetra University and M.Phil in computers Science from Kurukshetra University, Kurukshetra. She is presently pursuing P.hd. from department of Computer Science, Kurukshetra University. Her research interests are in Mobile Ad hoc Networks.



Dr. Ashwani Kush is a member of IAENG. He is working as Head and Associate Professor in Department of Computer Science & Applications, University College, Kurukshetra University, Kurukshetra. He has done PhD in computer science in association with Indian Institute of Technology, Kanpur, India and Kurukshetra University, Kurukshetra, India.He is professional Member of ACM, IEEE, SCRA, CSI INDIA and IACSIT Singapore. He has more than 100 research papers to his credit in various International/National Journals and Conferences. He has authored 15 books in computer science for undergraduate and school students. His research interests are in Mobile Ad hoc Networks, E-Governance and Security. Dr. Kush has chaired many sessions in International Conferences in USA and Singapore.

