AN INTELLIGENT FAULT MANAGEMENT SYSTEM USING ANSRS FOR WIRELESS MESH NETWORKS

Nirmalkumar S. Benni[1], Sunilkumar S. Manvi[2]

[1]*School of Electronics and Communication, REVA University, Bengaluru-560064. India*

[2]*School of Computing and Information Technology, REVA University, Bengaluru-560064. India*

ABSTRACT

Wireless Mesh Network is an extension of multi-hop Ad-Hoc networks, in which each node can communicate directly or indirectly with one or more peer nodes. It can leverage backhaul links to provide low cost access services. Centralized access points are not needed to mediate the wireless connection in WMN and also its multi-hop feature increases the coverage area and link robustness of existing Wi-Fi's. However this mesh network may subject to a variety of faults that are hard to diagnose manually. In this paper, an Autonomous Network Self Reconfiguration System (ANSRS) is proposed which continuously monitoring network condition to automatically manage many of the faults. This scheme uses Enhanced Destination Sequence Distance Vector Routing Protocol that enables a multi radio wireless network to autonomously recover from malicious activity to preserve network performance. We review challenges and possible solutions for three important components of an ANSRS: network measurements, fault diagnosis, and fault recovery. The simulations are done in network simulator 2 and the parameters such as throughput, packet loss, delay and overhead are analyzed and compared with previous schemes.

Keywords- ANSRS, DSDV, Fault Diagnosis, Fault Recovery, NS2 and WMN

I. INTRODUCTION

Wireless Mesh Network (WMNs) is a network within it's the nodes automatically establishing and maintaining mesh connectivity among themselves dynamically. In WMN, each client can communicate directly with one or more peer routers. The word "mesh" refers that all clients were connected to all other clients, but most modern meshes connect only a sub-set of clients to each other [1] [2]. The only different of mesh network from wireless networks are it must need centralized AP's to mediate the wireless connection. For example let us consider the two nodes with physical-interface 802.11b deployed in infrastructure mode needs to transfer the data to each other via access point only. The wireless mesh network are consists of mesh routers and mesh clients. Figure 1 shows that system model of Wireless Mesh Networks. In this network each node operates not only as a host but also as a router and also transferring packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations [2] [3]. A wireless mesh router contains additional routing functions to support mesh networking [5]. It is equipped with multiple wireless interfaces built on either the same or different wireless access technologies. A wireless mesh router can achieve the same coverage as a conventional

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

router but with much lower transmission power through multi-hop communications. By allowing mesh-style multi-hopping, the WMN can extends the range and link robustness of existing Wi-Fi's. Every client becomes a relay point or router for network traffic [5] [6]. Mesh networks consist of multiple wireless devices equipped with COTS802.11 a/b/g cards that work in ad-hoc fashion 802.11 capable antennas placed on rooftops allow a large area coverage [4].

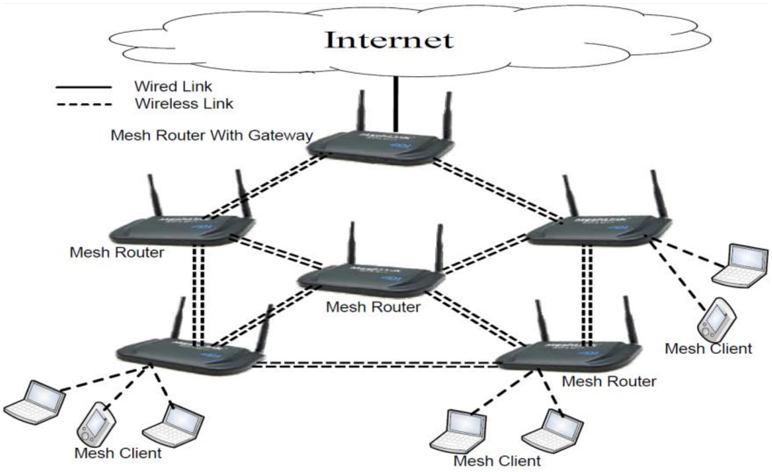


Figure 1. Wireless Mesh Networks

Fault tolerance in Wireless Mesh Network is an important property to improve the performance of the network. The mesh network may subject to a variety of faults that are hard to diagnose manually. In this research work, an Autonomous Network Self Reconfiguration System (ANSRS) is proposed which continuously monitoring network condition to automatically manage many of the faults. This scheme uses Enhanced Destination Sequence Distance Vector Routing Protocol that enables a multi radio wireless network to autonomously recover from malicious activity to preserve network performance. Also this research work reviews the challenges and possible solutions for three important components of an ANSRS: network measurements, fault diagnosis, and fault recovery. The simulations are done in network simulator 2 and the parameters such as throughput, packet loss, delay and overhead are analyzed and compared with previous schemes.

This paper is organized as follows: The first part was the introduction. The second part includes the various works done in fault tolerant in WMN with the literature survey. In the third part, we describe our proposed approach for dealing with the failures in WMN. The fourth part contains the conclusion and future work

II. LITERATURE REVIEW

Nan Li and Guanling Chen (2012) had proposed an Autonomic Fault Management scheme. The network condition is continuously monitored to automate the fault management tasks by self-awareness, self-diagnosis & analyzing the fault when it is detected and self-recovery by taking adaptation actions [1]. This AFM scheme reduces the human errors and responds to faults faster. Kalyani Pendke and S.U.Nimbhorkar (2013) had proposed cost aware reconfiguration scheme that enables WMNs to recover from link failures. These link failures are occurred due to the following factors such as interference, obstacles in motion and bandwidth requirements of the application [2]. The quality of links of each node is monitored & all possible reconfiguration plans are generated. Sweety Patel and Ketan Tandel (2016) had proposed different methods for detection of link failure in wireless mesh networks and also presents the survey of various link recovery technique for WMNs. This author also discussed the metric components that can be utilized to compose a routing metric for multi-channel wireless mesh networks [3]. N.N.Krishnaveni and Dr.K.Chitra (2015) had proposed a Cost efficient Fast Autonomous Reconfiguration System which provides the multiradio Wireless Mesh Networks to recover from link failure automatically to maintain the network performance [4]. In order to recover from failures this scheme generated necessary changes in local radio and channel allocations. G. Murugaboopathi and T.K.S.Rathishbabu (2012) had analyzed several reconfiguration techniques used for recovering link failures of wireless mesh network and their issues to maximize the network performance [5]. To recover mesh networks from link failures several reconfiguration schemes make using the link changes such as channel and route switch operations. Murugaboopathi and G., Sharmila (2013) had proposed exhaustive analysis of various reconfiguration techniques used to recover wireless mesh network from link failures and the issues to be addressed in order to maximize the network performance [6]. Abolfazl Akbari et al, (2011) have analyze the unactive nodes miss their communication in network a fault recovery corrupted node and Self Healing is proposed [7]. It designs the techniques to maintain the cluster structure in the event of failures caused by energy-drained nodes. Initially, node with the maximum residual energy in a cluster becomes cluster heed and node with the second maximum residual energy becomes secondary cluster heed. Later on, selection of cluster heed and secondary cluster heed will be based on available residual energy. This method must require a self healing property that’s also the drawback in this method. Ing-Ray Chen, et al (2011) had proposed scheme a WSN can be either source-driven or query-based depending on the data flow. In source-driven WSNs, sensors initiate data transmission for observed events to interested users, including possibly reporting sensor readings periodically [8]. In query-based wireless sensor networks, a user would issue a query with quality of service requirements in terms of reliability and timeliness. The general approach is to apply redundancy to satisfy the quality of service requirement. It does not provide more detailed analysis of the effect of network dynamics on Mean Time to Failure.

III. PROPOSED SYSTEM

The proposed system uses Autonomous Network Self Reconfiguration System (ANSRS). This system uses an auditor which continuously monitoring network condition to automatically manage many of the faults. Also Enhanced Destination Sequence Distance Vector Routing Protocol is used that enables a multi radio wireless network to autonomously recover from malicious activity to preserve network performance. In the proposed scheme the network is a failure tolerance wireless mesh networks. The proposed Wireless Mesh Network consists of mesh clients and mesh routers with fault tolerance property. An auditor monitors the traffic flow in its network.

Diagnosis of fault in WMN typically includes isolation of fault (that is location of fault), identification of fault (type of the fault) and cause of fault occurrence. With the help of auditor we can locate the fault and knows whether the fault is a link or node failure or traffic congestion. However a big challenge is to find the cause of the fault and autonomic recovery decisions to correct the fault.

The Enhanced Destination Sequence Distance Vector (EDSDV) protocol is based on Bellman – Ford routing algorithm where each node or client maintains a routing table that contains the shortest path to every possible receiver in the network and number of intermediate hops to the receiver. The sequence numbers allows the client to distinguish routes from new ones and avoid routing loops. The routing packet consists of destination address, number of hops to reach the destination, sequence number of the information about the destination and a new sequence number unique to broadcast. Pseudocode of algorithm is shown below. The update in routing table is done periodically to maintain table consistency. The routing table maintains the following details such as destination address, next node, number of hops and sequence number. The flowchart of proposed scheme is shown in Figure 2.

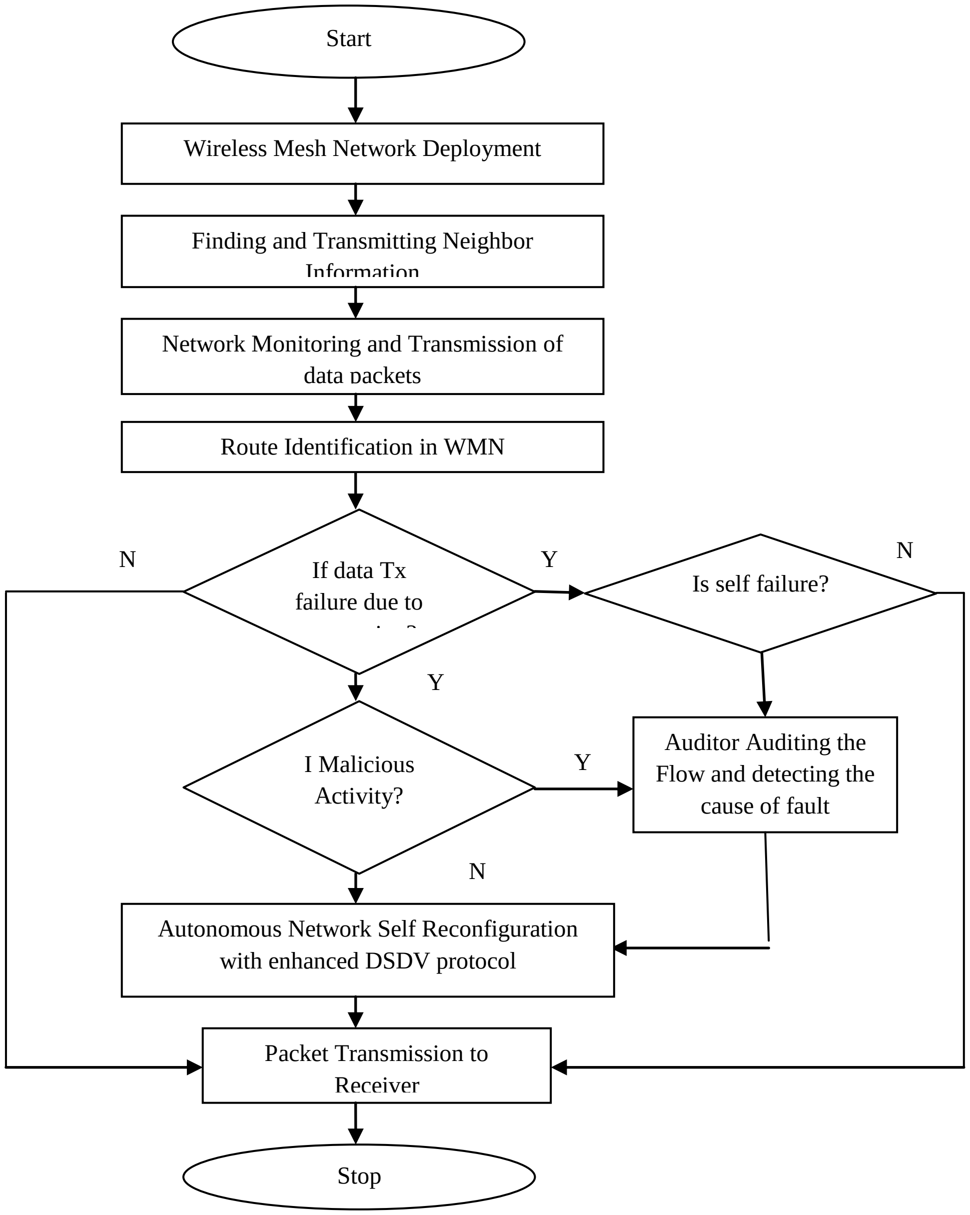


Figure 2. Flowchart of Proposed Scheme

Pseduocode of Algorithm 1:

Sender Mesh Client sends RREQ with sender address, destination address, number of hops to reach the destination, sequence number of the information about the destination

The neighbor clients check the RREQ packet and routing table. Neighbor node replies with RREP

Initialize MR, $\forall$ v $\in$ V, the set of data flow D(v) = φ, counter $C_{congestion}$ = 0, find the neighbor set N (v), Interference set I = φ;

Auditor will monitors the Data Flow after starting of data flow. For any data flow f_k, P = {v_1, v_2, ... , v_j},

for k (1 : 1 : j) < j , do

{

if (f_i start) then {

$D(v_k) = D(v_k) \cup \{f_i\}$

For ($\forall$ $v_p \in N(v_k)$)

if(|D(v_k)| == 1) &&(|D(v_p)| > 0)) then { /*if |D(v_p)| = 1 D(v_k) $\neq$ {f_i} It says Fault is occur*/

$C_{congestion} = C_{congestion} + 1$

I = I $\cup$ {(v_k, v_p)} }}

if (f_i end) then {

$D(v_k) = D(v_k) - \{f_i\}$

for($\forall$ $v_p \in$ N (v_k))

if((|D(v_k)| = 0) && (|D(v_p)| < 0)) then { // if |D(v_p)| = 1 D(v_k) $\neq$ {f_i} It says Fault is not appear*/

$C_{congestion} = C_{congestion} - 1$

I = I - {(v_k, v_p) | (v_p, v_k)} }}

}

Calculate τ, update D(v), $C_{congestion}$, I to other MRs.

Fault in networks leads to poor performance in network, it is the basic principle to reduce data communication that is generated by fault detection algorithm. The autonomous network self reconfiguration based fault detection algorithms are proposed to solve the fault in wireless mesh networks. Fault may be occur due to congestion or interference between nodes with different data flows. The major reason of this congestion is that the load excesses the capacity of network. The algorithm of fault detection due to congestion described as pseudocode of algorithm 1. The information involved in the algorithm is presented in routing layer and transportation layer. The traffic is initiated by mesh routers. Therefore the information about data flow f_i and routing path P = {v_1, v_2, ... , v_j} is stored and calculated in the MR and maintained in auditor. The pseudocode of algorithm1 maintains three sets. Data flow set D(v) is the set of the data flows that flow through node v. Neighbor set N(v) is the set of neighbors of node v. Interference set I is the set of the edges where whose the different flows flow through those two end nodes and the two flows interference each other. When the data flow starts or ends, set D(v) and the I should be updated. If there is only one data set D (v) and there is not less than one data flows in set D(p), where p $\in$ N(v) add the (v, p) to the set I. On the contrary, if there is no data flow in the set D (v), and there is not less than one data flows in set D(p), where p $\in$ N(v) delete the (v, p) or (p, v) from the set I.

According to the fault detection algorithm, we can get the information about congestion. Congestion rate is found by $\tau = k.\frac{C_{congestion}}{\|I\|}$, Where k is $2/D_{network}$ as correction factor, $D_{network}$ is the average neighbor nodes. The operation $\|I\|$ is to take the node number in set I. Then congestion ratio is interpreted as the ratio of the number of interference nodes to the number of neighbors. Congestion ratio value is 0 or 1. Value 0 means no fault occurs in network and value 1 denotes there is a fault in network. In addition, the congestion ratio reflects the status of the local network. The decision is made by auditor node.

IV. RESULT & DISCUSSION

This section describes the simulation results of fault tolerance in wireless mesh networks. Here the simulations are done using network simulator 2. Network Simulator (NS2) is a discrete event driven simulator tool which is developed at UC Berkeley. The main goal of NS2 is to support networking research and education. It is mainly suitable for designing new protocols, comparing different protocols and for traffic evaluations. The field configurations used is 1000m X 1000m with different number of nodes. Simulation runs for 60 simulated seconds. The fixed number of packet sizes (512-bytes) will be used in experiments. The parameters used in the simulation are listed below. The performance analysis is compared with dynamic source routing protocol.

Table 1 Simulation Parameters

Parameter	Value
Channel Type	Wireless
Routing Protocol	Enhanced DSDV
Queue Length	50 Packets
Number of Nodes in Topography	20,40,60,80
Node Placement	Random
Simulation End Time	60 sec
MAC Protocol	IEEE 802.11
Packet Size	512 bytes
Traffic Type	CBR

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Path Loss Model	Two Ray Ground
Energy	500J
Transmission Power	1.0
Receiving Power	0.5

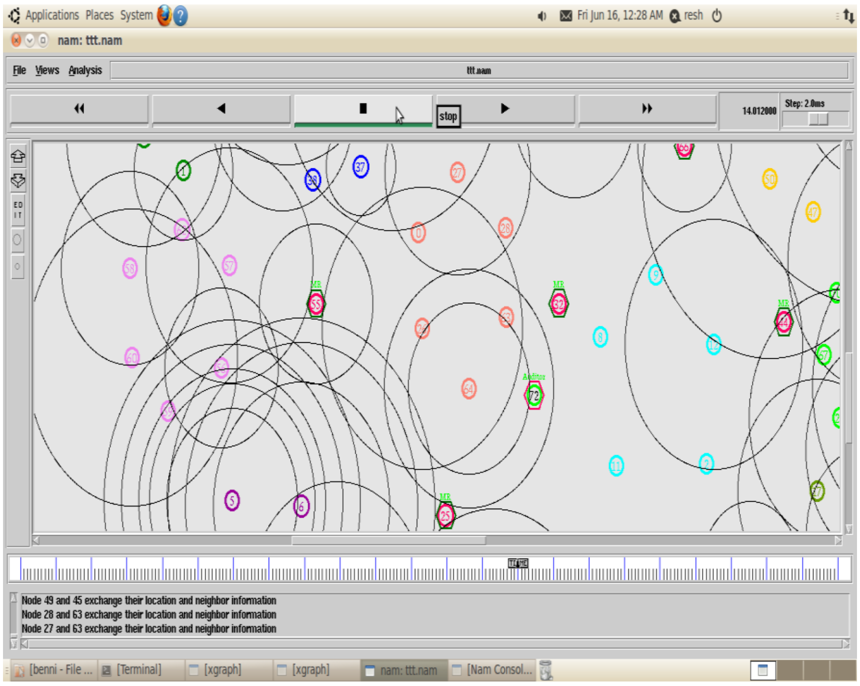


Figure 3. Mesh Network Formations and Exchange of Neighbor Information

Figure 3 shows that snapshot of mesh network formation and exchange of neighbour information. Here the mesh network consists of mesh client and mesh router. Here totally 75 nodes are deployed randomly and the mesh clients are grouped with each other in different area with corresponding mesh router. Each mesh router will having information about nearby mesh clients. Auditor is used in this simulation to monitor the traffic flow of each packet. The mesh clients share each other's information through mesh routers.

IJARSE
ISSN: 2319-8354

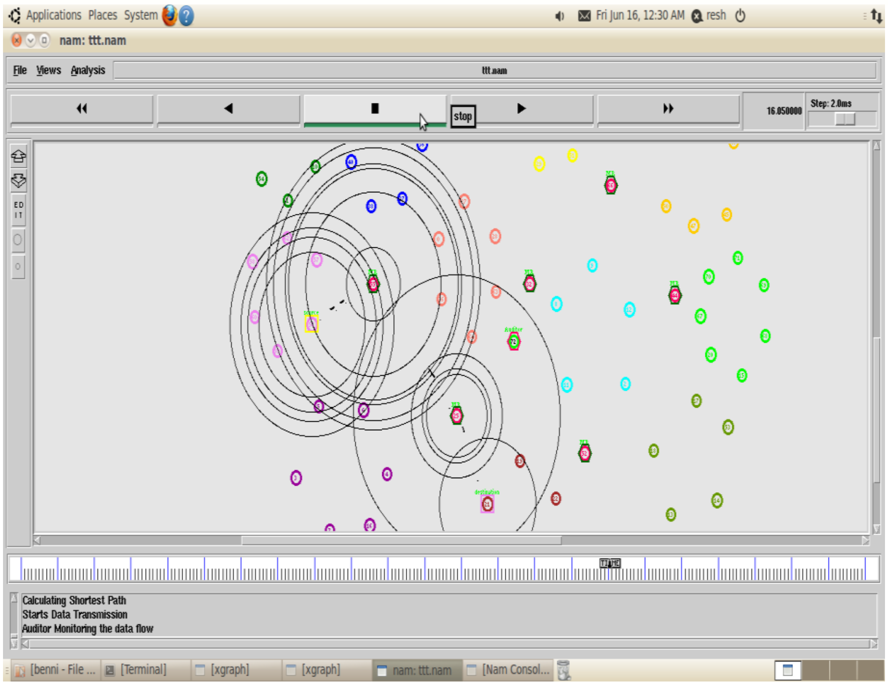


Figure 4. Data Transmission

Figure 4 shows the snapshot of data transmission. Here the sender in one mesh area will transmit the data to the client in another mesh area. In this simulation source node 52 wants to send their data packet to its destination node 21. So that first it will send the RREQ packet via Mesh Routers. After getting the RRPLY from the destination it will send the data packet via the chosen path. Here the data packet is carried over two mesh routers 55 and 25 to 21. After the starting of data transmission the auditor monitors the flow rate.

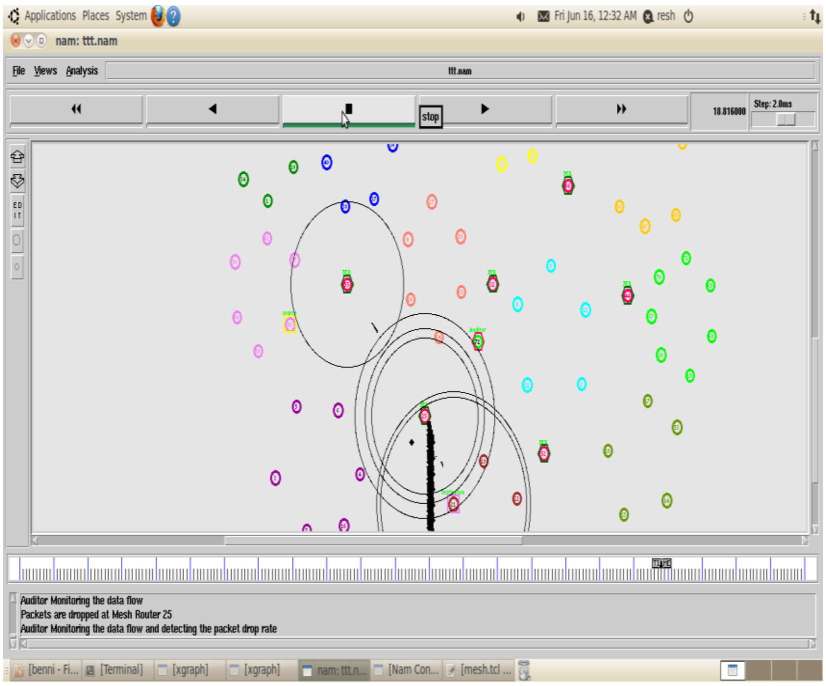
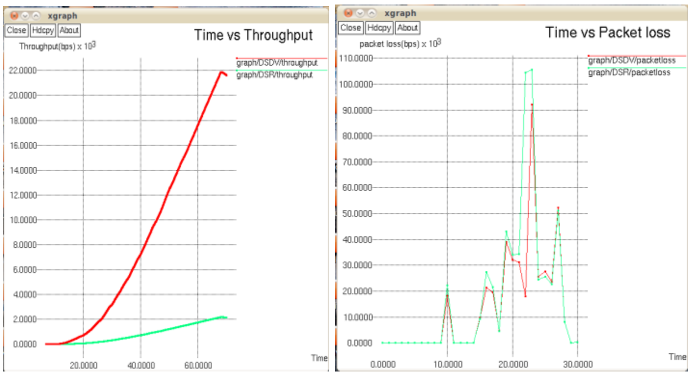


Figure 5. Fault Detection

 IJARSE
ISSN: 2319-8354

Figure 5 shows that snapshot of fault detection. Here the data transmission starts from node 52 to 21 via mesh routers 55 and 25. During the data transmission the Mesh Router will drops the packet suddenly due to malicious activity. The auditor will monitors and detect the fault nodes as mesh router 25.



(a) (b)

Figure 6. (a) Throughput (b) Packet loss

Figure 6 (a) and (b) shows that throughput and packet loss of the wireless mesh network. In this Network throughput is the amount of data moved successfully from one place to another in a given time period and typically measured in bits per second (bps).The above graph proves that the throughput of the enhanced DSDV is higher than the DSR. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. In other word when congestion or fault occurs in network also leads to packet loss. Packet loss is measured as a percentage of packets lost with respect to packets sent. The graph shows that the packet loss of the proposed enhanced DSDV is lower than the existing DSR.

(c) (d)

Figure 6. (c) Delay (d) Overhead

Figure 6 (c) and (d) shows that the snapshot of delay and overhead. The delay of a mesh network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes. The graph shows that the delay of the proposed enhanced DSDV is lower than the existing DSR. Overhead is any combination of excess or indirect computation time, memory, bandwidth or other resources that are required to perform a specific task. The proposed enhanced DSDV has less overhead compared to existing DSR.

V. CONCLUSION

In this paper, we proposed an Autonomous Network Self Reconfiguration System with Enhanced Destination Sequence Distance Vector Routing Protocol to detect the fault, cause of fault and fault recovery. Compared with existing works, in our approach low communication overload is introduced. Moreover, this algorithm can detect fault effectively. From the simulation results the algorithm introduce low computation and message overhead to the network, higher throughput rate and low end to end delay which is quite suitable for WMN.

REFERENCES

[1] Nan Li, Guanling Chen and Meiyuan Zhao "Autonomic Fault Management for Wireless Mesh Networks" 2012

[2] Kalyani Pendke and S.U.Nimbhorkar "Reconfiguring Wireless Mesh Network Using Link Recovery Technique", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.3, Issue 3, June 2013

[3] Sweety Patel, Ketan Tandel "Link Failure Detection in Wireless Mesh Network: Survey", International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2016

[4] N.N.Krishnaveni and K.Chitra "Cost Efficient Fast Autonomous Reconfiguration System in Wireless Mesh Networks" ICIT 2015 The 7th International Conference on Information Technology doi:10.15849/icit.2015.0035 © ICIT 2015 (http://icit.zuj.edu.jo/ICIT15)

[5] G. Murugaboopathi, T.K.S.Rathishbabu and R.Venkatesh "An Analysis of Reconfiguration Approaches for Recovery in Wireless Mesh Networks", International Journal of Computer Applications (0975 – 8887) Vol. 50, Issue 5, July 2012

[6] Murugaboopathi, G., Sharmila, P., Partibhan, P.A and Sivakumar R "Feasibility Based Reconfiguration Approach For Recovery In Wireless Mesh Networks", International Journal of Recent Scientific Research Vol. 4, Issue, 5, pp. 592 - 596, May, 2013

[7] A. Akbari, A. Dana, A. Khademzadeh, and N. Beikmahdavi, "Fault detection and recovery in wireless sensor network using clustering," IJWMN Vol. 3, Issue 1, pp. 130–138, Feb. 2011.

[8] I. Chen, A. P. Speer, and M. Eltoweissy, "Adaptive fault tolerant QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks," IEEE Trans. Dependable Secure Comput., Vol. 8, Issue 2, pp. 1–35, Mar./Apr. 2011.