Journal of Information & Communication Technology
Vol. 1, No. 2, (Fall 2007) 60-70

Identification of a Lossy Channel in Wireless Mesh Network using Conservation of flow

Faraz Ahsen [*]
Khalid Hussain [*]
Nyla Khadam [*]
Muhammad Sharif [*]
COMSATS Institute of Information Technology Islamabad, Pakistan

Noor Zaman [*]
Faculty of CS & IT, Institute of Business and Technology, Karachi, pakistan

ABSTRACT

Wireless communication is technically broadcast in nature. Therefore, data transfer and communication between two nodes are not reliable and secure. This arises the need that there should be some mechanism to check the successful transaction between two or more than two nodes. Packet loss in wireless mesh network can be either due to malicious node or lossy channel, and both can degrade the Quality of Service and network performance.

In terms of lossy channel, there does not exist a cutting edge on the basis of which a lossy channel is identified. Once, identified we can later further investigate what was the underlying reason for the loss of packets; through different existing algorithms for specific purposes. In this study, authors present a method to identify a lossy channel within a wireless mesh network. Later, simulation scenario is presented in evidence of our assumption.

Inspec Classification: A4760, B1110, B6150P

Keywords : Wireless network, Hope count, AODV

1) INTRODUCTION

In a traditional wireless network, mobile devices connect to a single access point where each device has to share a fixed pool of bandwidth. With mesh technology and adaptive radio devices; only able to connect with other devices that are in a set range. Nodes act as repeaters to transmit data from nearby nodes to peers that are too far away to reach resulting in a network that can span large distances; especially over rough or difficult terrain. Mesh networks are also extremely reliable, as each node is connected to

[*] The material presented by the authors does not necessarily portray the viewpoint of the editors and the management of the Institute of Business and Technology (BIZTEK) or COMSATS Institute of Information Technology Islamabad, Pakistan.

[*] Faraz Ahsen : faraz_jaf@yahoo.com
[*] Khalid Hussain : khalidusmani_65@yahoo.com
[*] Nyla Khadam : nyla958@yahoo.com
[*] Muhammad Sharif: muhammadsharifmalik@yahoo.com
[*] Noor Zaman : noor@biztek.edu.pk

several other nodes, ensuring multiple path diversity. If one node drops out of the network, due to hardware failure or any other reason, its neighbors simply find another route through another neighboring node. Extra capacity can be installed by simply adding more nodes. Mesh networks may involve either fixed or mobile devices. The solutions are as diverse as communications in difficult environments such as emergency situations, tunnels and oil rigs to battlefield surveillance and high speed mobile video applications or real time racing car telemetry.

The advantage is that, like a natural load balancing system, the more devices the more bandwidth becomes available; provided that the number of hops in the average communications path is kept low. However, the more devices add to access a shared medium the chances of error in a normal flow increase. For example if the selected communication link is damaged, an alternate one is chosen and retried for successful data communication in the network. However, if the selected link is not identified as defective but it is malfunctioning, then there should be some metric to identify and avoid it. This paper is substantially extended version of (Khalid Hussain, 2007).

2) RELATED WORK

In the context of graph theory, amongst the network each edge must be connected with the other so that data should travel accordingly. In directed graph each edge has a capacity, such that the amount of data flow along an edge does not exceed its capacity. A flow must suit the restriction that the amount of flow into a node must equal the amount of data flowing out of it, except when either it is a source, which has only outgoing flow(s), or sink, which has only incoming flow(s).

According to (www.amazines.com, Sep 2007), in a finite directed graph G(V,E) where every edge (u,v) ∈ ¸ E has a capacity, which is non-negative and real-valued. If (u,v) ∉ E, then we assume that c(u,v) = 0. Further, we make a distinction in two vertices. One is the source 's' and the other sink 't'. A flow network can be represented as a real function like: f: V x V → R, for all nodes u and v, characterizing the following three properties.

$$f(u,v) \leq c(u,v)$$

Capacity constraints: The flow along an edge cannot exceed its capacity.

$$f(u,v) - f(v,u)$$

Skew symmetry: The net flow from *u* to *v* must be the opposite of the net flow from *v* to *u* (see example).

$$\sum_{\upsilon \in V} f(\upsilon,\omega) = 0$$

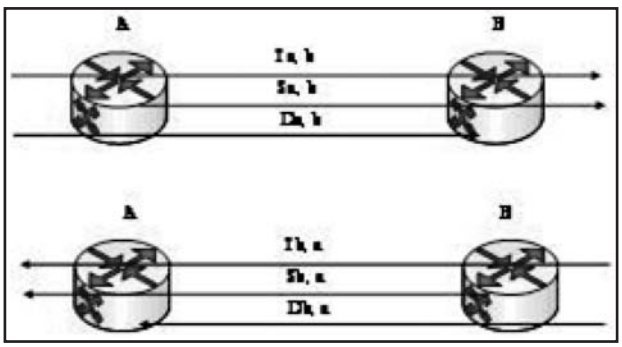
Flow conservation: unless $u = s$ or $u = t$. The net flow to a node is zero, except for the source, which "produces" flow, and the sink, which "consumes" flow.

Notice that $f(u,v)$ is the net flow from *u* to *v*. If the graph represents a physical network, and if there is a real flow of for example 4 units from *u* to *v*, and a real flow of 3 units from *v* to u, we have $f(u,v) = 1$ and $f(v,u) = -1$. The residual capacity of an edge is $c_f(u,v) = c(u,v) - f(u,v)$. This defines a residual network denoted $G_f(V,E_f)$, giving the amount of available capacity. See that there can be an edge from *u* to *v* in the residual network, even though there is no edge from *u* to *v* in the original network. Since flows in opposite directions cancel out, decreasing the flow from *v* to *u* is the same as increasing the flow from *u* to *v*. An augmenting path is a path $(u_1,u_2,\ldots, u_k)$, where $u_1 = s$, $uk = t$, and $c_f(u_i,u_{i+1}) > 0$, which means it is possible to send more flow along this path. (www.en.wikipedia.org/wiki/Net_flow, August 2007)

There are already many protocols being presented for the sake of analyzing incoming and outgoing packet flows for the sake of load balancing and security purposes. However, WATCHERS (Khalid Hussain, 2007) is the one that specially talks about conservation of flow in the network which states that an input must either be engaged or sent on as an output. The Conservation of Flow (CoF) is a passive monitoring scheme, which analyzes the flowing traffic at designated routers in a network. Inconsistencies between the aggregate incoming and the outgoing traffic volumes at these designated routers indicate prospective problems.

This is an attractive tool with which to analyze network protocol for security purposes. The functionality of the WATCHERS' algorithm (Khalid Hussain, 2007) is to detect malicious routers. In this regard, every router has to maintain a set of six vectors for each neighbor node. As shown in figure 1, these vectors are based on either all the data that is passing through that router, or all information which are being sent by that router or the data which is intended for that router.

Figure 1:
Transit packet byte counter [1, 2]



Each router performs this test on its neighbors, having received the counters from each neighbor's neighbors. The number of incoming packets minus packets destined for that router is compared to the number of outgoing packets minus packets originating with that router. If this difference exceeds some specified threshold, the tested router is diagnosed as malicious. In order to detect groups of malicious routers that conspire to hide their misbehavior, maintenance requirements are heavily increased. However, the WATCHERS protocol had many limitations in both its traffic validation mechanism and in its control protocol, many of which were documented by Hughes et al.

Fatih (Detecting and Isolating Malicious Routers) is also based on CoF, but considers other types of attacks for detection of malicious routers including packet modification, fabrication, re-ordering etc. But its main contribution is a detection algorithm for malicious routers in the network, especially adjacent routers playing faulty.

In this study, authors have not stressed on malicious routers, rather present a scheme that integrates or incorporates error rate in wireless channel for mesh network environment. The proposed idea is based on error rate in a wireless channel that can affect conservation of flow. Additionally, an ideal channel bit rate for wireless mesh network has also been implemented to achieve maximum CoF.

3) BACKGROUND: AD-HOC ON-DEMAND DISTANCE VECTOR (AODV)

In our simulation we have used Ad-hoc On-Demand Distance Vector (AODV) (C. E. Perkins, 2003). It enables dynamic, self starting, multi-hop routing between participating

mobile nodes wishing to establish and maintain a wireless mesh network. AODV allows all nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication.

One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination for any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node always selects the one with the greatest sequence number.

AODV is a routing protocol, and it deals with route table management. Route table information must be kept even for passing routes, such as are created to temporarily store reverse paths towards nodes originating RREQs. AODV uses the following fields with each route table entry:

- **Destination Address**

The address of the node for which a route is desired.

- **Destination Sequence Number**

The greatest sequence number received in the past by the originator for any route towards the destination.

- **Interface**

The interface over which packets arrive must be known to AODV whenever a packet is received. This includes the reception of RREQ, RREP, and RERR messages. Whenever a packet is received from a new neighbor, the interface on which that packet was received is recorded into the route table entry for that neighbor.

- **Hop Count**

The Hop Count as indicated in the node's route table entry for the originator

- **Last Hop Coun**t

If the hop count of the newly determined route to the destination is greater than the hop count of the previously known route, as recorded in the last hop count field, the node should create a RERR message for the destination Next Hop.

4) EXPERIMENTS

4.1. Simulation Scenario:

Initially, simulation was set up for ideal conservation of flow in a wireless mesh network, where random numbers of packets are sent by any sender node to any other node in the network being the destination. Selection of packet originator and final destination nodes are also random. In this regard, if there exist multiple paths to reach the destination node, with equal hop counts; selection of a path amongst all possibilities is also random. For a transaction between two nodes, i.e. for ‘n’ number of packets to be sent from node ‘X’ to node ‘Y’, the path chosen will remain the same, for those ‘n’ packets. However for another transaction between the same sender and receiver nodes having ‘m’ packets, the path may differ.

In wireless network communication, factors like packet loss will be present and so will be the re-transmission of a packet, till it times out. Such factors are generally catered in the implementation of the routing protocol in simulation environment. So is the said simulation, which runs over a routing protocol. The successful packet delivery is achieved through the routing protocol, which may require one or more re-attempts. In the next sub-section, we discuss the variable parameters of the simulation.

4.2. Simulation Parameters:

The standard parameters which are the basis of this simulation are mentioned as under:

- **Total Hosts:**

Total hosts indicate that how much nodes are there in the mesh network. For our simulation we select 8 or more nodes to form a wireless mesh network.

- **Simulation time:**

To get the appropriate results a simulation requires a specific time to run, by giving the simulation time the simulation will run at that particular time.

- **Channel Error rate:**

Channel error rate defines the probability that a packet will drop. Theoretically, all packets should reach at the desired destination in the first attempt. But practically a network drops packets, which may be due to various reasons. In simulation, this aspect is handled via channel error rate.

- **Channel delay:**

Channel delay has been used in simulation for updating the routing table. After a period of time every node should update its routing table.

- **Routing algorithm:**

The underlying routing algorithm being used is AODV.

To achieve the successful conservation of flow the above parameters are interlinked in the simulation as follows:

The simulation starts up with an ‘n’ nodes network. The simulation time is taken as ‘t’ seconds. Channel error rate of 0.01% is taken into account. Additionally, 20% of error is applied on a specific channel between nodes 1 and 7. i.e. this particular channel will act as a lossy channel in our simulation. As the simulation starts, AODV protocol establishes its routing table by sending route discovery message. In the perspective of this activity a channel delay time is also accommodated in this simulation, so that routing tables are timely updated. Once the routing tables are established by each node, data transmission is initiated.

Furthermore, the output of simulation is a set of matrices and an array, which are discussed in the following sub-sections.

4.3. Sender (S) Matrix:

Shows the number of packets being sent by each node to other nodes on the network. Rows represent the senders whereas columns represent the intended

destinations. Each cell of the matrix shows the amount of packets being sent by the sender “X” (corresponding row) for “Y” (corresponding column). Regardless of whether the packet arrived successfully at the destination or not, S-matrix logs the packet as soon as it leaves the originator node.

4.4. Destination (D) Matrix:

Logs the number of packets being received by each node in the given simulation time. Rows represent the intended destination “Y”, whereas columns represent the originator of the packet “X”. Each entry shows the successful arrival of the packet at the destination.

4.5. Transition (T) Matrix:

A packet being sent from node "X" intended for node "Y" is in transition unless it does not reach "Y". S- Matrix only shows that packet has left successfully from "X" and D-Matrix shows that packet successfully arrived. But what happened to the packet while it was in transition? To cater for this question and have traceability of each and every packet we should know the intermediate stages / hops that a packet is routed through till it reached the final destination. In this regard, each node in the simulation is maintaining a T-matrix. Each entry in the matrix represents a packet in transition. For each packet, rows show the last sender (it may be the originator, too) and columns represent the next receiver (which may be the final destination node).

4.6. Lossy (L) Array:

Contains the entries of packets that were initiated in the simulation by any node, but failed to reach the destination. Since, wireless network protocols are connection oriented in nature and rely on acknowledgements for successful delivery of the packet, even by an intermediate hop. Therefore, if a node is unable to collect the packet or it's corrupted but a resending message never showed up; that packet would not proceed to destination further and is treated lost. All such lost packets are treated as failure and the corresponding node that collected it successfully but could not forward it would get an entry in the L-array. In short, it contains list of failure packets by each node in the whole simulation.

By using the entries in an above mentioned matrices and array, we can trace a cumulative of packets that participated in all the transactions. Theoretically, for all transactions that occurred between two nodes, following statement should be true:
Ideally:

$$\text{S-matrix} = \text{D-matrix}$$

In context of the discussed simulation, it becomes:

$$\text{S-matrix} = \text{D-matrix} + \sum (L1+L2+\ldots Ln)$$

Where 'L' is the nodes' entry from L-array and applies to such nodes only which acted as intermediate hops, in a transaction.

5) RESULTS AND DISCUSSION

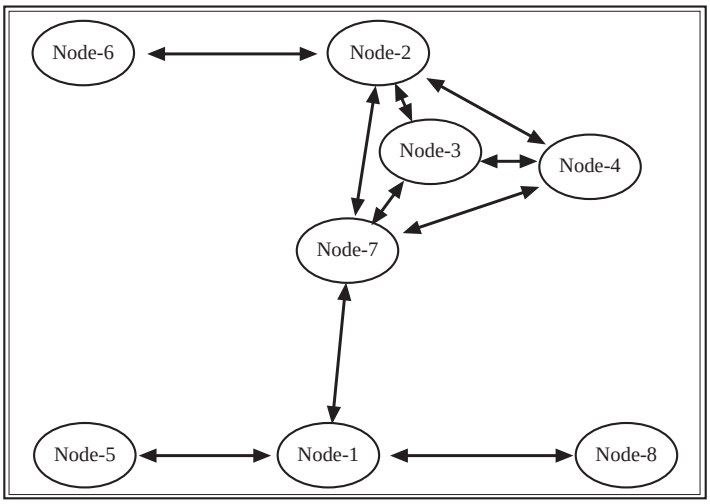
The first phase of the simulation discusses with an ideal scenario, where there are negligible amount of packet drop; which is unavoidable in case of a wireless network. Whereas the second phase of simulation involves a bad channel. For the sake of simulation, we have transplanted a packet drop rate on a certain channel. Next, we once again run our simulation and compare the results with earlier ones. Through this we will try to analyze the impact of a lossy channel identification mechanism in an environment. The threshold level being considered in this scenario is 20% error rate (Khalid Hussain, 2007).

Since, the selection of originating node, destination node and the number of packets to be sent are all random, therefore two cases for different set ofparameters is discussed, separately. The figures in each case show the node-wise packet delivery rate. The red portion shows the percentage of packets that were intended for the corresponding node, but failed to reach.

5.1 Case-I:

For a network of 8 nodes a simulation of 3000 seconds was manipulated. Channel error rate for CoF scenario is taken as 0.01%. The network diagram is illustrated in figure-2.

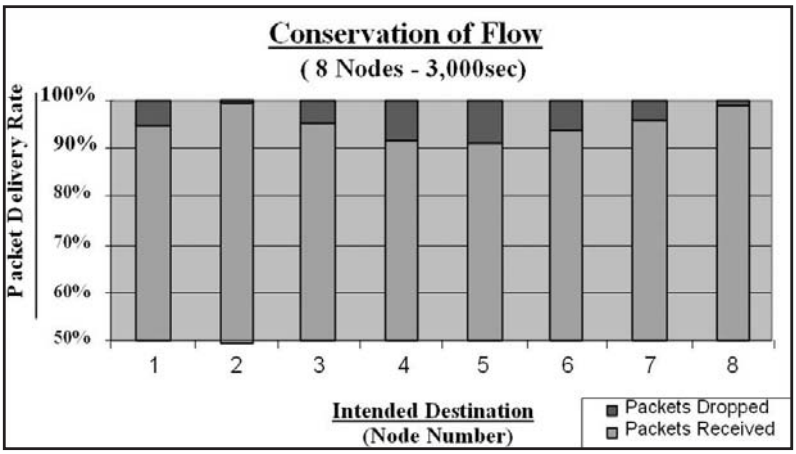
Figure-2:
8-Nodes Network



5.1.1 Conservation of Flow

The sum of data packets that traveled on the network in this duration were approximately 33,000. Figure 3 shows the overall number of packets dropped by each node in different transactions; which makes around 2% of all the data packets.

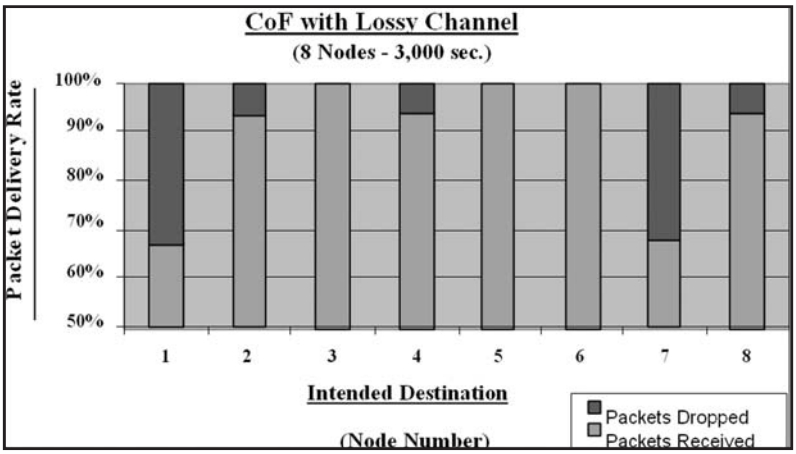
Figure-3:
CoF with 8 nodes



CoF with Lossy Channel

The total data packets that traveled on the network in this period were approximately 28,000. Figure 4 demonstrates the number of packets dropped by each node in different transactions; which makes around 13% of all originated data packets. However, on the channel between node 1 and node 7, approximately 22% of the packets that passed through this link were lost. Amongst the total initiated data packets 11% were lost, on average.

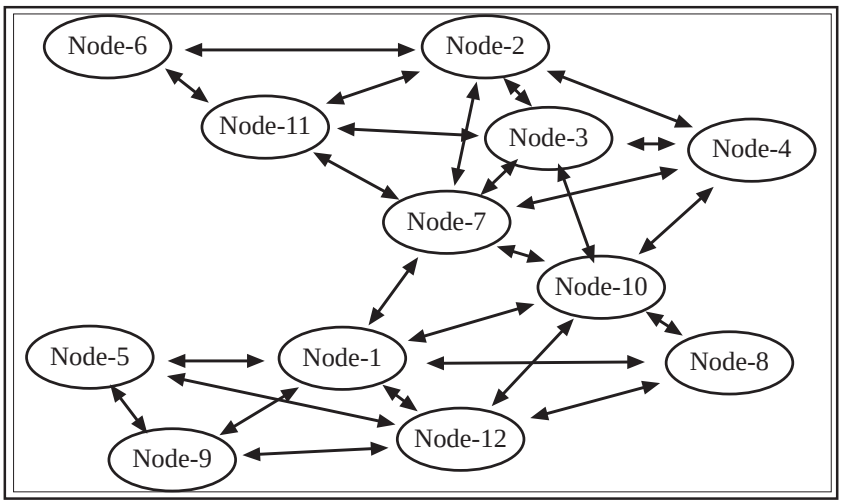
Figure-4:
CoF with 8 nodes having a lossy channel



5.2 Case-II:

The scenario was extended further to a network of 12 nodes. The simulated time was also increased to 5,000 seconds. The placement of nodes is shown in figure-5.

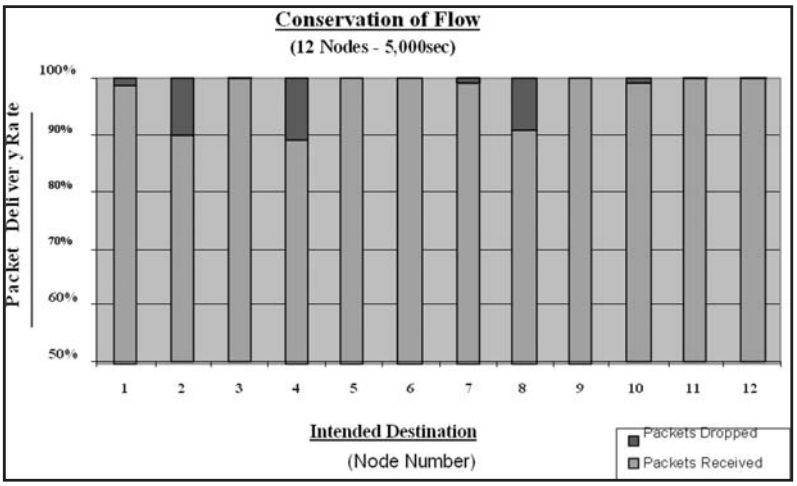
Figure-5:
12-Nodes Network



5.2.1 Conservation of Flow

The sum of data packets that traveled on the network in this duration were approximately 53,000. Figure 6 shows the corresponding packets being dropped by each node, while it was acting as an intermediate router. This makes roughly 2% of the total initiated data packets.

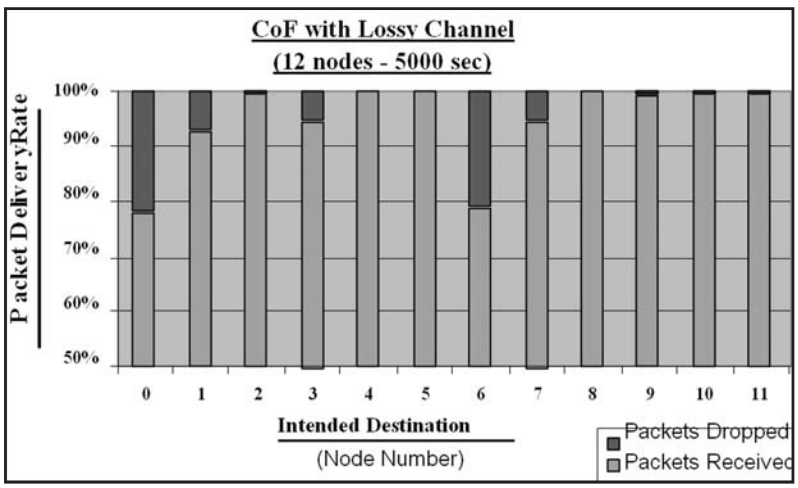
Figure-6:
CoF with 12 nodes



5.2.2 CoF with Lossy Channel

This time more than 55,000 data packets were sent on the network. In figure 7, red portion of the graph against each node represents the percentage of packets which the node failed to deliver to its neighbor in the first attempt. Additionally, on the link between node 1 and node 7, the cumulative packets being dropped during transactions were approximately 15% of the total traffic, on that link, by both the nodes. i.e. roughly 6% of the total initiated data packets were lost on the lossy link.

Figure-7:
CoF with 12 nodes having a lossy channel



In implementing and running the above scenarios repeatedly, it was observed that approximately 2-3% of the total data packets being sent were lost in case of CoF. However,

with existence of a lossy channel in the network, the packet drop rate is proportional to the traffic flowing through it. This may be due to congestion, collision, channel error, etc. In realcommunication environment, such dropped packets are re-sent by sender, till it reaches the destination or session is timed out. For the sake of conservation of flow, the dropped packets in first instance are re-sent due to protocol implementation requirement, but are not taken into account in this study. i.e. if it is dropped on the first instance, it is logged by the node dropping it and thus any packet with an incremented re try counter is not logged in D-matrix even if it is successfully delivered.

The difference of S-matrix with D-matrix, gives the number of dropped packets. L-array shows the corresponding bifurcation of the packets dropped by each node. Hence, conservation of flow in cumulative end-to-end data delivery in a network is achieved using the presented metrics as:

$$\text{S-matrix} = \text{D-matrix} + \sum (L1+L2+\ldots Ln)$$

For each node there exists a T-matrix, i.e. T0 for node-0, T1 for node 1, etc. Each Ti shows the number of packets for which the node acted as an intermediate hop in a transaction. For every received packet that is to be forwarded, each node increments a counter in the cell of a particular row and column. Row denotes the originator of the packet and column indicates the final destination of the packet. Thus, for each packet flowing on the network, cumulative traceability with respect to each path is catered through T-matrices.

6) CONCLUSION

Due to lack of collusion detection mechanism, even in an ideal wireless environment, there is collusion and packet drop. However, there are a number of factors on which successful packet transmission relies, mainly the environmental factors and limited resources of wireless devices. Both the said factors result in congestion and packet drop. To overcome such factors, first thing is to properly identify the nature of the problem. In broader aspect, this thesis presents a mechanism to classify packet drop rate in terms of varying channel error grading.

In this study, authors have presented a scheme that integrates or incorporates error rate in wireless channel for mesh network environment. The proposed idea is based on error rate in a wireless channel that can affect conservation of flow. Additionally, an ideal channel bit rate for wireless mesh network has also been implemented to achieve maximum conservation of flow.

This Simulation study has revealed that in usual communication there is a 3-5% error rate in packet delivery. However, in case of 10% of channels being

lossy, an increased dropped rate is observed, which can be determined with respect to the number of packets being dropped versus the percentage of channels being lossy. As we increase the simulation time, the dropped rate becomes stagnant on the lossy channel. But the traceability of packets becomes complex, while increasing the number of nodes. The scenario presented in this study has been tested with different parameters, but only a couple of them are presented.

7) FUTURE WORK

Authors intend to extend the presented metric of end-to-end data delivery along with transaction based metric, to be implemented with mobile nodes. This can help to identify a particular faulty area on the map, or a frequency in a specific region. This extended model would be useful in terms of traffic analysis and load balancing algorithms in wireless networks.

REFERENCES

KHALID HUSSAIN, FARAZ AHSAN 2007.Conservation of Flow in Wireless Mesh Network NCICT-2007 University of Science and Technology, Bannu, NWFP, Pakistan.

KHALID HUSSAIN, FARAZ AHSAN, KHALID MAHMOOD AWAN AND SALEEM AHMED Conservation of Flow with Lossy Channel in Wireless Mesh Network BIZTEK Cyber technology-issues, challenges, and development Karachi, Pakistan, June 2007.

http://www.amazines.com/Network_flow_related.html, Sep 2007.

http://www.en.wikipedia.org/wiki/Net_flow, August 2007.

ALPER TUGAY MÝZRAK, YU-CHUNG CHENG, KEITH MARZULLO AND STEFAN SAVAGE FATIH: Detecting and Isolating Malicious Routers

C. E. PERKINS, E. M. BELDING-ROYER, AND S. R. DAS. AD-HOC on-demand distance vector (AODV) routing. Internet draft, February 2003. draft-ietf-manet-aodv-13.txt.