Conservation of flow with Lossy Channel in Wireless Mesh Network

Journal of Information & Communication Technology
Vol. 1, No. 2, (Fall 2007) 10-20

Conservation of flow with Lossy Channel in Wireless Mesh Network

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

* 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

© JICT is published by the Institute of Business and Technology (BIZTEK). Ibrahim Hydri Road, Korangi Creek, Karachi-75190, Pakistan.

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 flow accordingly. In directed graph each edge has a capacity, such that the amount of data flow along 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 $(u,v) \in E$ has a capacity, which is non-negative and real-valued. If $(u,v) \notin E$, 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: $f: V \times V \rightarrow R$, 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.

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

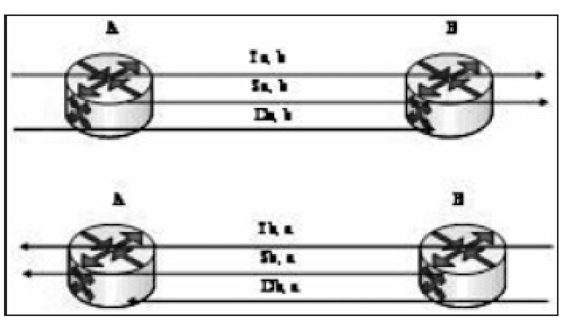
Skew symmetry: The net flow from u to v must be the opposite of the net flow from v to u (see example).

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

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