INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN SCIENCE TECHNOLOGY & ENGINEERING

VOL. 1, ISSUE 1, OCT. 2012 ISSN NO: 2319-7463

Link layer traffic and behavior in congested WLANs

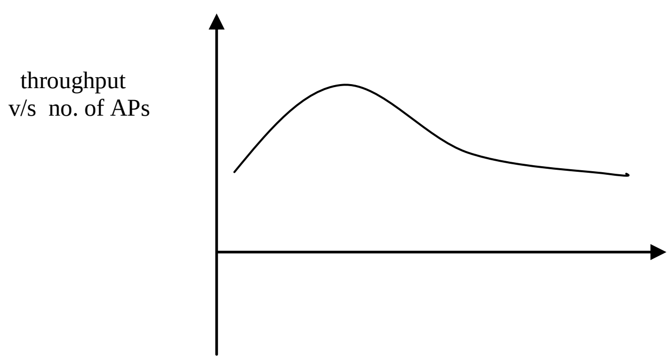
Vikram Singh
NIT Hamirpur, India
kamvikramm@gmail.com

ABSTRACT

In a congested network, the client faces a lot of problem (overhead) to transmit a single frame of useful data. So, the efficiency is reduced. This problem causes a lot of packets to be lost. When packets are lost, the client misinterprets the actual reason for it (whether it was congestion or the error in transmission). Client may even perform Hand-off which may be purely unnecessary, thereby increasing the overhead. The main components which constitute the unwanted traffic are the management frames and the control frames. So, there is a need to reduce the sending and receiving of such frames to an extent that the performance doesn't pay the price.

INTRODUCTION

In a region, the Access Points (APs) need to be deployed smartly so as to provide efficient connectivity. Initially, to support more users, the number of APs is increased so that they meet the requirements of the network. This improves the performance also. But after further increment in the number of APs, degradation in performance can be seen.



The reason is attributed to the increased interference because of the increased APs. Moreover, there is limited number of orthogonal channels which is also a cause of increasing interference. The increased interference can lead to intermittent connectivity, low throughput, and high losses. This can make the network less reliable and can lead to a complete breakdown. So, just to send a single frame of required data can incur a significant amount of overhead on the clients as well as the AP.

Moreover, repeated attempts of association and reassociation can further aggravate the problem. So the whole scenario is as follows: The traffic increases when the number of clients increase and the frames start getting lost which results in missed transmission opportunities and inefficient medium utilization. This will cause the clients to conclude erroneously about the network state and then the client tends to perform a Hand-off.

RELATED PREVIOUS WORK

There has been a lot of work regarding the network performance. Some of them which this paper takes as references are:
Yeo et al: They captured the link layer information and analyzed the performance of a campus network.

VOL. 1, ISSUE 1, OCT. 2012 ISSN NO: 2319-7463

Jardosh et al: They monitored and analyzed link layer traces to understand congestion in wireless networks. Also proposed a queue based user association management (IQU) for WLAN. There is an allotted "work period" in which a client access the medium. "Wait Period" is also there in which the client waits until its "Work Period" is on. The advantage of this scheme is that it avoids the sending of the requests which may result in collision because now the client is allocated a separate "wait period" and "work period". Along with the advantage, comes a disadvantage. The Sybil attack is possible. A client can use multiple identities so that it can access the medium for a longer time and get a lot of "work period".

Rodrig et al: They proposed that both the contention (which is due to congestion) and the errors are the grounds for the retransmission, which leads to an erroneous conclusion.

Mhatre & Papagiannaki: They found that the long-term averaged signal strength results in a better Hand-off decision. They used smart triggers for improving user performance. They also proposed that the clients should be proactive in nature rather than being reactive to the performance degradation and poor performance. The reason for this is the finding that 80% of the entire Hand-off duration is consumed in the scanning stage alone. And being proactive, 50% reduction could be achieved in the average Hand-off delays. Other factors which can help in the Hand-off decisions are:

- Noise level
- Transmitting power
- Potential bandwidth available after Hand-off
- Quality of AP's connection to the Internet
- Round trip time from client to the AP
- Whether encryption on/off
- DHCP success or not, etc

RamyaRaghavendra et al: They found that the major contributors of unwanted traffic are those applications which aggressively try to maintain connectivity and high quality client service. They discussed two mechanisms:

1. Keep-Alive traffic: used to maintain the association between the client and the AP even when there is no data to send
2. Probing Mechanism: used by the clients to frequently collect neighboring AP's information.

Actually, the paper can be seen as the extension of the paper which shows the work done by Ramya Raghavendra et al.

IEEE 802.11 FRAME TYPES

The frames are categorized in three parts:

1. Management frames,
2. Control frames, and
3. Data frames

MANAGEMENT FRAMES

These are used to establish and maintain the connections (associations). The management sub-frames are as follows:

- Authentication frame (AUTH): used by client and AP to authenticate each other and exchange the identities.
- Deauthentication frame (DEAUTH): AP sends to the client to terminate the communication
- Association Request (ARQ): Client sends to AP to connect to it
- Association Response (ARP): sent as a Response to ARQ
- Reassociation Request (RRQ): Client sends to a new AP when connection with the previous AP is lost
- Disassociation (DASS): Used by client or AP to terminate an association
- Beacon (BCN): AP sends this periodically to announce its presence
- Probe Request (PRQ): Client broadcasts to obtain information on neighboring APs
- Probe Response (PRP): AP sends information in response to a PRQ

CONTROL FRAMES

These are used to assist in the data delivery. The control sub-frames are as follows:

- Request to send (RTS): used as the first phase of the two-way handshaking
- Clear to send (CTS): sent as a response to the RTS
- Acknowledgement: used to inform that the data has been received correctly

DATA FRAMES: The frames which contains the required data.

HAND-OFF PROCEDURE

When a client moves, it loses connectivity sometimes. So, it may probe for the available APs. The APs reply to the PRQ and the client receives PRP. The client then sends an RRQ to one of the APs that has send the PRP and gets associated with this new AP. The Hand-off can be understood with four different phases:

- Triggering: When the client feels the need to perform the Hand-off. This is the first stage of Hand-off and may be instigated by
    - Unacknowledged packets
    - Consecutive missed beacons
    - Quality degradation
- Discovery: The clients collect information about the APs in the vicinity in this phase
- AP selection: Selects one of the APs on some criteria. Eg. Received Signal Strength Indicator (RSSI) can be used.
- Commitment: Client disassociates with the current AP and reassociates with the new AP.

It has been found that nearly half the Hand-offs in a congested static network have a negative impact on the throughput.

TRAFFIC ANALYSIS

802.11 protocol uses Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) to manage and reduce the contention. CSMA/CD (Collision Detection) is not used because it may not be possible to hear the collision or even the signals which are at a greater range because the strength of its own transmission would mask all other signals on the air. CSMA/CD is preferred in wired networks instead.

When there is large number of nodes, they come into each other’s Carrier Sense range. In a highly utilized network, large number of frames needs to be sent, so the clients repeatedly contend and hence spend a considerable time in Backing-off instead of sending packet. So, the medium is not utilized efficiently even when the contention is high. Also, denser the APs are deployed; greater are the chances of them operating on the same channel. It leads to increased contention and interference. Because of this, throughput decreases.

PROBE TRAFFIC

It constitutes of the Probe request and the Probe response frames. These frames are sent:

- When the client disconnects, or when it thinks it has (although it has not).
- When client roam from the AP with which it is associated periodically.
- This kind of probing is called aggressive probing.

AGGRESSIVE PROBING BENEFICIAL OR NOT

It is beneficial when the clients are mobile because as the client moves, it loses connectivity with the AP. It is found that there are 100s of msec wasted in the process of scanning and performing Hand-off. This way, the application performance is deteriorated (especially in the delay sensitive applications). So, aggressive probing is beneficial for mobile clients because it facilitates faster Hand-off.

But, in case of static congested networks, aggressive probing is not efficient. The reason is that the probability of reconnecting to the same AP is much higher and hence it poses unnecessary overhead, leading to inefficient medium utilization.

VOL. 1, ISSUE 1, OCT. 2012 ISSN NO: 2319-7463

CONCLUSION

The overhead of management traffic (including Hand-off mechanism) works in lightly utilized network, but can significantly affect the performance in a congested network. Some Hand-offs are unnecessary and may negatively affect the throughput. So, some schemes may be used taking into consideration the network information like network load, network type (mobile or static), etc. Some solutions can be:

- Decrease the rate of periodic keep-alive messages and PRQ (by increasing the time interval at which they are sent) to a threshold that the throughput doesn't suffer.
- PRP may be relayed to the far away clients via multi-hop transmission.
- Information of the APs can be kept in the cache of the clients for some limited period of time, so that the overhead is reduced when it loses the connectivity with the present AP.

REFERENCES

[1]. R. Ragavendra, E.M. Belding, K. Papagiannaki, K.C. Almeroth, "Unwanted Link Layer Traffic in Large IEEE 802.11 Wireless Networks," IEEE Transactions on Mobile Computing, vol 9, no. 9, Sept 2010.

[2]. A.P. Jardosh, K. Mittal, K.N. Ramachandran, E.M. Belding, Kc. Almeroth, "IQU: Practical Queue-based user association management for WLANs," Proc. ACM Mobicom, pp 158-169, Sept 2006.

[3]. R. Raghavendra, E.M. Belding, K. Papagiannaki, K.C. Almeroth, "Understanding Hand-offs in large IEEE 802.11 Wireless Networks," Proc, Internet Measurement conf, (IMC), Oct 2007.

[4]. D.Tang and M. Baker, "Analysis of a Local-Area Wireless Network," Proc ACM Mobicom, pp. 1-10, Aug, 2000.

[5]. J. Yeo, M.Youssef, A. Agrawala, " A framework for wireless LAN monitoring and its application," Proc, Workshop wireless security (Wise), pp. 70-79, Oct. 2004.

[6]. V. Mhatre, K. Papagiannaki, "Using smart triggers for improved user performance in 802.11 wireless networks," Proc. Mobisys, pp. 246-259, june 2006.

[7]. S. Vasudevan, K. Papagiannaki, C. Diot, J. Kurose, D. Towsley, "Improved Access Point Selection," Proc Internet Measurement Conf. (IMC), Oct, 2005.

[8]. A.J. Nicholson, Y. Chawatha, M.Y. Chen, B.D. Noble, D. Towsley, "Improved Access Point Selection," Proc. Mobisys, pp. 233-245, June 2006.

[9]. A.P. Jardosh, K.N.Ramachandran, K.C. Almeroth, and E.M.Belding Royer, "Understanding Link-Layer Behavior in Highly Congested IEEE 802.11 Wireless Networks," Proc. Workshop Experimental Approaches to wireless network design and Analysis (EWIND),pp. 11-16, Aug. 2005.

[10]. M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, J. Zahorjan, "Measurement-Based Characterization of 802.11 in a Hotspot setting," Proc, Workshop Experimental Approaches to Wireless Network Design and Analysis (EWIND), pp. 5-10, Aug. 2005.