Volume 2, Issue 12, December 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Buffers in 802.11-Based Networks

Depavath Harinath
MCA,
Sreenidhi Institution of Science and Technology,
Accredited by NBA, AICTE, New Delhi - Permanently Affiliated to JNTU
Hyderabad, A.P., India.

***Abstract**— Buffers play a key role in 802.11/802.11e Wireless networks.802.11 is a set of standards for implementing wireless local area networks (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by IEEE LAN/MAN Standards Committee (IEEE 802).Buffers are used to accommodate short-term packet bursts so as to mitigate packet drops and to maintain high link efficiency. The use of fixed size buffers in 802.11networks inevitably leads to either undesirable channel underutilization or unnecessary high delays. The main objective of this paper is to maintain high network utilization while providing low queuing delays in 802.11 wireless networks through dynamic buffer sizing mechanism.*

***Keywords**— Buffer sizing, IEEE 802.11, wireless LANs(WLANs).*

I. INTRODUCTION

Buffers play a major role in wireless networks. A buffer contains data that is stored for a short amount of time. The purpose of a buffer is to hold data right before it is used. For example, when we download an audio or video file from the internet, it may load the first 20% of it into a buffer and then begin to play. While the clip plays back, the computer continuously downloads the rest of the clip and stores it in the buffer. Because the clip is being played from the buffer, not directly from the internet, there is less of a chance that the audio or video will skip when there is network congestion.

Buffer size specifies how many seconds worth of video (or any other file format) are buffered (or prepared to play) before the video starts playing. The more seconds we buffer, the smoother the playback should be. If the internet traffic is heavy, the video may take longer to start playing. The default value of 5 seconds is usually a good choice. But we can choose anything from 2 to 60 seconds of buffer. According to the classic rule of thumb the buffer size is set to be the product of the bandwidth and the average delay (round trip time or RTT) of the flows utilizing this link: the Bandwidth-Delay Product (BDP) rule [1]. Here the round trip time (RTT), also called as roundtrip delay. It is the time required for a single pulse (or) packet to travel from a specific source to a specific destination and back again. In this context, the source is the computer initiating the signal and the destination is a remote computer or the system that receives the signal and retransmits it. Having small buffers is attractive as it reduces the amount of memory, required physical space, energy consumption, and price of the router. According to the point of [2], the main advantage of having small buffers is the reduction in queueing delays and jitter. In the current Internet the average number of hops on a random path is about 13 [3].For a single flow with that many hops it is possible to expect several congested links on the path. Thus buffering of several hundreds *ms* at each router would imply very large queueing delays.

Wireless communication in 802.11 networks is *time-varying* in nature; i.e., the mean service time and the distribution of service time at a wireless station vary in time. The variations are primarily due to: 1) changes in the number of active wireless stations and their load (i.e., offered load on the WLAN); and 2) changes in the physical transmit rate used (i.e., in response to changing radio channel conditions). As discussed in [4] that there exists no fixed buffer size capable of ensuring both high throughput efficiency and reasonable delay across the range of physical rates and offered loads experienced by modern WLANs.Any fixed choice of buffer size necessarily carries the cost of significantly reduced throughput efficiency and/or excessive queuing delays. This, therefore, naturally leads to the consideration of adaptive approaches to buffer sizing, which dynamically adjust the buffer size in response to changing network conditions to ensure both high utilization of the wireless link while avoiding unnecessarily long queuing delays.

II. RELATED WORK

This paper is about the buffers in 802.11- based networks. Buffers play a key role in 802.11/802.11e Wireless networks. 802.11 is a set of standards for implementing wireless local area networks (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by IEEE LAN/MAN Standards Committee (IEEE 802). 802.11 and 802.11x refers to a family of specifications developed by IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a server. The IEEE accepted this specification in 1997. Recent work on buffer sizing for wired links [5] shows that the BDP rule can be overly conservative, and suggests sizing buffers to

$$\frac{BDP}{\sqrt{n}}$$

instead where *n* is the number of flows traversing a link. This exploits the statistical multiplexing when many flows share a link. Since real-world traffic patterns are often extremely complex, including a mix of connection sizes, RRTs, etc that change over time, adaptive buffer sizing is considered in [2] [6].

Compared to sizing buffers in wired routers, a number of fundamental new issues arise when considering 802.11-based networks. First, unlike wired networks, wireless transmissions are inherently broadcast in nature, which leads to the packet service times at different stations in a WLAN being strongly coupled. For example, the basic 802.11 DCF (Distributed Coordinated Function) which is a CSMA/CA-based algorithm ensures that the wireless stations in a WLAN win a roughly equal number of transmission opportunities [7], hence the mean packet service time at a station is an order of magnitude longer when 10 other stations are active than when only a single station is active. Consequently, the buffering requirements at each station would also differ, depending on the number of other active stations in the WLAN. In addition to variations in the mean service time, the distribution of packet service times is also strongly dependent on the WLAN offered load. This directly affects the burstiness of transmissions and hence buffering requirements. Second, wireless stations dynamically adjust the physical transmission rate/modulation used in order to regulate noncongestive channel losses. This rate adaptation, whereby the transmit rate may change by a factor of 50 or more (e.g. from 1 to 54 Mb/s in 802.11a/g), may induce large and rapid variations in required buffer sizes. Third, the ongoing 802.11n standards process proposes to improve throughput efficiency by the use of large frames formed by aggregation of multiple packets [8], [9]. This acts to couple throughput efficiency and buffer sizing in a new way since the latter directly affects the availability of sufficient packets for aggregation into large frames.

It follows from these observations that, among other things, there does not exist a fixed buffer size that can be used for sizing buffers in WLANs. This leads naturally to consideration of dynamic buffer-sizing strategies that adapt to changing conditions. The use of fixed size buffers in 802.11 networks inevitably leads to either undesirable channel under-utilization or unnecessary high delays. The main objective of this paper is to achieve high throughput while maintaining low delay across a wide range of network conditions in 802.11 wireless networks through dynamic buffer sizing mechanism.

III. EXISTING SYSTEM

Buffer over flow occurs when a program or a process tries to store more data in a buffer (a temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information which has to go somewhere can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. And the use of fixed size buffers in 802.11 networks leads to undesirable channel under-utilization and unnecessary high delays.

IV. PROPOSED SYSTEM

As I discussed in the existing system that with the use of fixed size buffers in 802.11 networks leads to undesirable channel under-utilization and unnecessary high delays. And due to the buffer overflow overwriting or corrupting the valid data held in them. To overcome these problems one should use dynamic buffer-sizing strategies [10] that adapt to changing conditions.

V. PROBLEMS ASSOCIATED WITH BUFFERS

As we know that buffers play a major role in 802.11 based networks or the wireless networks. But there are also problems which arise in buffers, they are –

(i.) Packet lost:

In the network (a group of systems which are interconnected in a particular manner) data will travel in the form of packets. Due to the buffer overflow there is a possibility of packet lose in the network.

Buffer overflow occurs when a program or a process tries to store more data in a buffer than it was intended to hold. Due to the buffer overflow the remaining data packets which are in a queue, may loss in a network. Then the client may not receive the exact information which a client in intended to. This is one of the security attack(due to the packet loss).

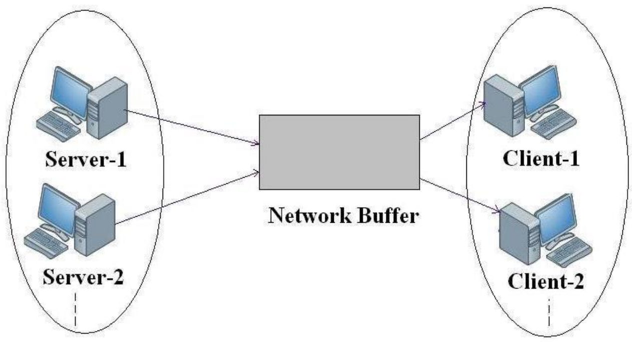

Figure (1) Client-server architecture

The above figure(1) explains the client-server architecture and the figure(2) illustrates the packet loss due to the buffer overflow and this leads to the security attack.

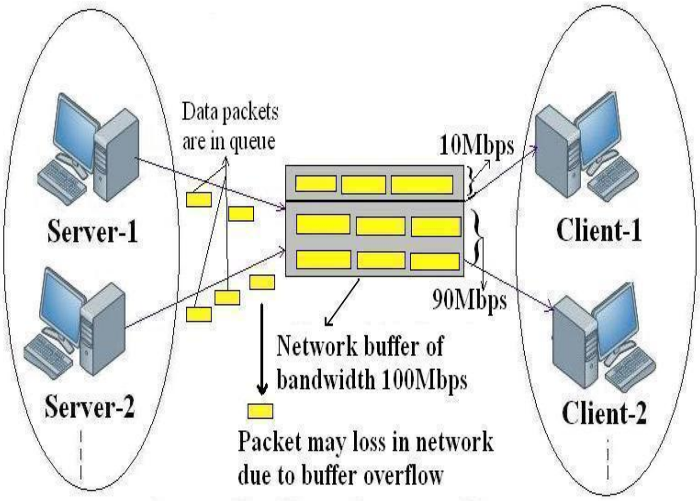

Figure (2) Illustrates the packet loss due to buffer overflow

(ii.) Overwriting the valid data:

Since buffers are created to contain a finite amount of data, the extra information which has to go somewhere can overflow into adjacent buffers. This leads to corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on the data integrity.

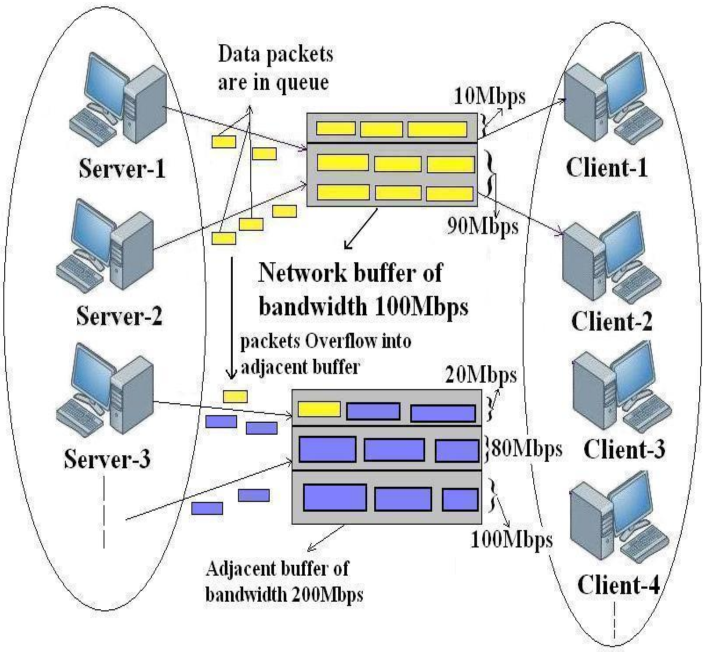

Figure (3) Illustrates the overwriting of valid data

(iii.) High delays:

High delays occur due to the network congestion. Congestion may occurs if the number of packets sent to the network is greater than the number of packets a network can handle. From the above figures, figure(1) and figure(2) we can see that , due to the network congestion high delay occurs and which leads to loss in data integrity.

VI. FIXED SIZE BUFFERS IN 802.11 NETWORKS

With the use of fixed-size buffers in 802.11 networks leads to either undesirable channel underutilization or unnecessary high delays.

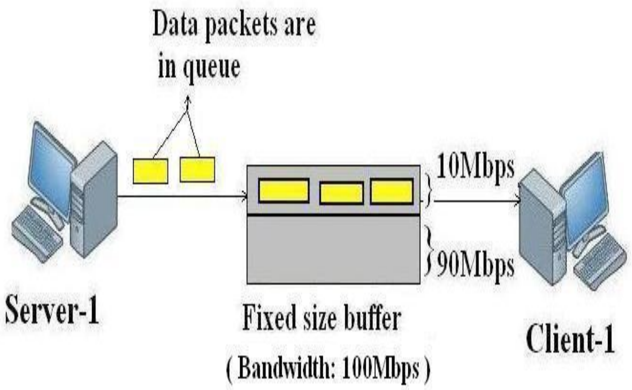

Figure (4) Illustrates the channel underutilization in fixed size buffers

VII. CONCLUSION

Buffers play a key role in 802.11/802.11e wireless networks. Buffers are used to accommodate short-term packets so as to mitigate packet drops and to maintain high link efficiency. Packets are queqed if too many packets arrive in a sufficiently short interval of time during which a network device lacks the capacity to process all of them immediately. The use of fixed size buffers in 802.11 networks inevitably leads to either undesirable channel underutilization or unnecessary high delay across a wide range of network conditions. The main objective of this paper is to maintain high network utilization while providing low queuing delays in 802.11 wireless networks through dynamic buffer sizing mechanisms.

ACKNOWLEDGMENT

My heartful gratitude to almighty God and my parents -father D.Chatur Naik and mother D.Ghammi Bai without whose unsustained support, I could not have completed this paper.

REFERENCES

[1] C.Villamizar and C. Song, “High performance TCP in ANSNET,” *Comput. Commun. Rev.*, vol. 24, no. 5, pp. 45–60, Oct. 1994.
[2] R. Stanojevic, C. Kellett, and R. Shorten, “Adaptive tuning of drop-tail buffers for reducing queueing delays,” *IEEE Commun. Lett.*, vol. 10, no. 7, pp. 570–572, Jul. 2006.
[3] Traffic measurements (online), available at: http://www.caida.org/tools/measurement/skitter/RSSAC/
[4] T. Li, D.Leith, D. Malone, “Buffer Sizing for 802.11-based networks,” *IEEE/ACM Trans. Netw.*, vol. 19, no. 1, Feb. 2011.
[5] G. Appenzeller, I. Keslassy, and N. McKeown, “Sizing router buffers,” in *Proc. ACM SIGCOMM*, 2004, pp. 281–292.
[6] G. Vu-Brugier, R. Stanojevic, D. Leith, and R. Shorten, “A critique of recently proposed buffer-sizing strategies,” *Comput. Commun. Rev.*, vol. 37, no. 1, pp. 43–48, Jan. 2007.
[7] D. Malone, K. Duffy, and D. J. Leith, “Modeling the 802.11 distributed coordination function in non-saturated heterogeneous conditions,” *IEEE/ACM Trans. Netw.*, vol. 15, no. 1, pp. 159–172, Feb. 2007.
[8] S. A. Mujtaba *et al.*, “TGn Sync proposal technical specification,” IEEE 802.11-04/889r6, May 2005 [Online]. Available: www.tgnsync.org
[9] T. Li, Q. Ni, D. Malone, D. Leith, T. Turletti, and Y. Xiao, “Aggregation with fragment retransmission for very high-speed WLANs,” *IEEE/ACM Trans. Netw.*, vol. 17, no. 2, pp. 591–604, Apr. 2009.
[10] Depavath Harinath,“Dynamic Buffer Sizing Algorithms for 802.11-Based networks*” International Journal of Advanced Research in Computer Science*, vol.3, no.7, Nov –Dec, 2012,
[11] A. Dhamdhere, H. Jiang, and C. Dovrolis, “Buffer sizing for congested internet links,” in *Proc. IEEE INFOCOM 2005*, pp. 1072–1083.
[12] D. Wischik and N. McKeown, “Part I: buffer sizes for core routers,” *ACM SIGCOMM Computer Commun. Review*, vol. 35, pp. 75–79, July 2005.
[13] K. Avrachenkov, U. Ayesta, A. Piunovskiy, “Optimal choice of the buffer size in the Internet routers,” in *Proc. IEEE CDC 2005*, pp. 1143-1148.
[14] A. Dhamdher and C. Dovrolis, “Open issues in router buffer sizing,” *Comput. Commun. Rev.*, vol. 36, no. 1, pp. 87–92, Jan. 2006.
[15] K. Kumaran, M. Mandjes, and A. L. Stolyar, “Convexity properties of loss and overflow functions,” *Oper. Res. Lett.*, vol. 31, no. 2, pp. 95–100, 2003.

AUTHORS PROFILE

Depavath Harinath, received the Bachelor of Science degree in computerscience from New Noble Degree college, Affiliated to Osmania University, Hyderabad, A.P, India in 2008 and received Master of Computer Applications degree from Sreenidhi Institute of Science and Technology, Accredited by NBA, AICTE, New Delhi - Permanently Affiliated to JNTU, Ghatkesar, Ranga Reddy, Hyderabad, A.P., India in 2012. My research Interests are Computer Networks, Network Security