Edith Cowan University
Research Online

ECU Publications Pre. 2011

2008

Self-restraint Admission Control for Ad-hoc WLANs

Hushairi Zen
Edith Cowan University

Daryoush Habibi
Edith Cowan University

Iftekhar Ahmad
Edith Cowan University

10.1109/ATNAC.2008.4783320

This article was originally published as: Zen, H. , Habibi, D. , & Ahmad, I. (2008). Self-restraint Admission Control for Ad-hoc WLANs. Proceedings of Australasian Telecommunication Networks and Applications Conference, 2008. ATNAC 2008. (pp. 186-191). Adelaide, Australia. IEEE Press.
Original article available here
© 2008 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ecuworks/1238

Self-restraint Admission Control for adhoc WLANs

Hushairi Zen, Daryoush Habibi, and Iftekhar Ahmad
School of Engineering
Edith Cowan University
Joondalup, WA 6027
Australia
Email:hzen@student.ecu.edu.au

Abstract— **Admission control is an important mechanism for sustaining throughput and supporting quality of service (QoS) for real-time traffic in a wireless local area network (WLAN). In an adhoc WLAN scenario where no access point (AP) is available, admission control has to be self-managed by each node. We propose a self-restraining admission control mechanism that works by monitoring the congestion level of the network in the adhoc WLAN. Wireless nodes can listen to all nodes within their range and be aware of the collision rates. A node wishing to join the network measures the current collision rate, and predicts the post-admission collision rate, on the basis of which the self-restraining mechanism in the node decides if it can join the network. We analyse the impact of key parameters, such as the collision threshold level, on the performance of the self-restraining mechanism and show that this mechanism works effectively in sustaining traffic in an adhoc WLAN.**

I. Introduction

The advancement of wireless local area network (WLAN) technology has provided network designers with more flexible options of network topologies. It opens up more applications and the possibility of different types of service which might otherwise not be possible. One of the important wireless network topologies is the adhoc WLAN as it provides flexibility for network designers and broadens WLAN applications. In adhoc WLANs, communication between nodes is achieved without using an access point (AP) as an arbiter to police and manage the traffic. This results in lower overheads and higher system throughput. Wireless nodes can join the communication group at anytime provided they are within communication range and follow the set protocols. Wireless nodes can access the Internet or nodes outside the boundary of the adhoc WLAN as long as there is one node in the network that is connected to the wired network.

Although the development of adhoc WLAN has been slow in the past compared to infrastructured WLAN, it is now seen as a potential technology for providing services effectively where it is difficult to implement infrastructured WLAN or wired LAN. Some of the practical areas of applications for adhoc WLAN include rescue operations in disaster areas, battlefields, hospitals and other adhoc communication environments. One of the important issues that needs to be addressed in adhoc WLANs is the control of traffic capacity in the network in order to maintain Quality of Service (QoS) for existing communicating nodes.

In an infrastructured WLAN set-up, such as the standardised IEEE 802.11b and 802.11e, admission control is managed by an AP [1][2]. The AP decides whether new nodes can be admitted to the network or if any of the communicating nodes need to be dropped. The AP gathers information regarding the channel traffic load and capacity needs of the nodes in the network to make effective decisions. In an adhoc WLAN, a centralized node which functions like an AP is not available. To the best of our knowledge, no work on admission control mechanisms has been undertaken in an adhoc WLAN without using an intermediatory device. Some of the published works on admission control in WLAN, such as in [3], [4] and [5], use an AP as an intermediatory device.

In this paper, we design an admission control scheme for adhoc WLAN based on a self-restraint mechanism that works by monitoring the channel collision rate. We implement this mechanism in each of the wireless nodes. Using the NS2 [6] simulator, we show that the self-restraining mechanism works effectively in sustaining traffic in adhoc WLAN and providing QoS to real-time traffic in multimedia applications. It has two important abilities to keep the traffic congestion to a level where the required throughput of all traffic sources is sustained. First, it equips each node with the capability to restraint itself from joining the network if the collision rate is too high. Second, if after joining the network the channel becomes congested, the admission control mechanism in the node will drop that node from the network and will wait for a period of time before attempting to join the network again.

We study and analyse the behavior of the collision rate and contention window in each node within the adhoc WLAN environment. We increase the congestion level in the network gradually by introducing additional nodes, and show through both analysis and simulation that the collision rate in the carrier sense multiple access collision avoidance (CSMA/CA) mode reflects the congestion level of the WLAN. The collision rate is therefore a suitable metric for designing a self-restraining mechanism.

II. Self-restraint Node Admission Control

In an adhoc WLAN, when the network operates above its congestion threshold, the network performance becomes unstable, throughput of all nodes goes down, unacceptable delays and jitters to real-time traffic occur and the network may fail. The fundamental concept of the proposed self-restraint admission control is to provide a mechanism for the network to operate within acceptable congestion bounds. This

978-1-4244-2603-4/08/$25.00 © 2008 IEEE

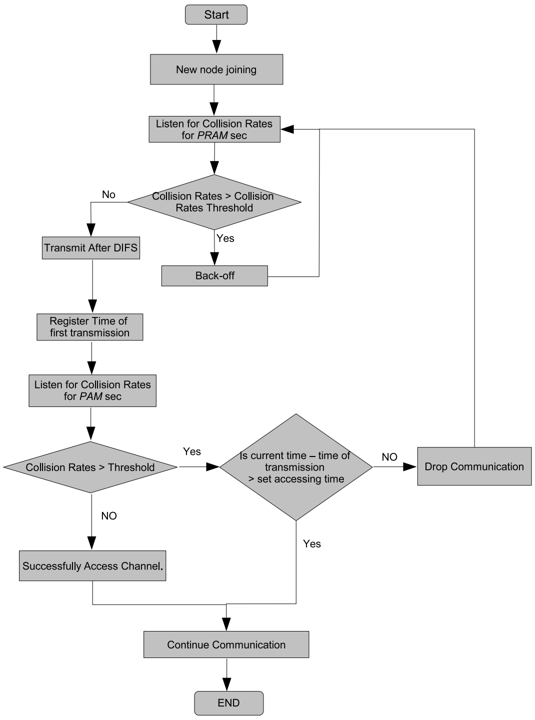
Start
New node joining
Listen for Collision Rates for PRAM sec
No
Collision Rates > Collision Rates Threshold
Yes
Transmit After DIFS
Back-off
Register Time of first transmission
Listen for Collision Rates for PAM sec
Collision Rates > Threshold
Yes
Is current time – time of transmission > set accessing time
NO
Drop Communication
NO
Yes
Successfully Access Channel.
Continue Communication
END

Fig. 1. Flow chart of the self-restraint admission control algorithm

is achieved by managing the association of new nodes into the network, and if necessary, by dropping associated nodes. In our proposed mechanism, new nodes can only join the network if they sense that the network is not congested. If the network is sensed to be congested, the node will backoff and wait until the congestion level goes down to an acceptable level. If the congestion level increases above the *collision threshold level (CTL)* as soon as a new node joins the network, that node will automatically restrain itself from continuing the communication. Nodes that have been communicating in the network for more than a set period of time will continue to receive service and are protected from being dropped. This time period, which we call the *post admission monitoring time (PAM)*, functions as a time period for the recently joined node to monitor the traffic congestion level and decide if it needs to drop off or continue its communication.

The self restraint mechanism is implemented in each of the wireless nodes at the medium access control (MAC) layer. As shown in the algorithm flow chart of Figure 1, when a new node wants to join the network, it monitors the collision rate of the channel for a few seconds which is called the *pre admission monitoring time (PRAM)*. If the collision rate is above the *CTL* during the *PRAM*, the node resets its monitoring period to zero and starts listening again. If the collision rate is below the *CTL*, the node transmits after a DCF interframe space (DIFS) and joins the network. The node will then monitor the network congestion level for a *PAM* period. If the congestion level is not above the *CTL*, due to the new node joining the network, the node considers that it has successfully joined the network and is protected from being dropped by the self-restraint mechanism. If the congestion level goes above the *CTL* before the *PAM* time elapses, the self-restraint mechanism will restrain the node from joining the network and drop the communication. The node then has to go through the admission process again.

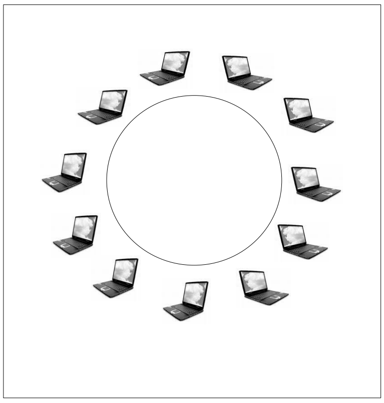

Fig. 2. Simulation scenario

TABLE I
IEEE 802.11 PARAMETERS USED IN SIMULATIONS

Bit Rates	
Data Packets Bit Rate	11 Mbps
RTS/CTS/ACK	1 Mbps
PLCP Data Rate	1 Mbps
Backoff and Inteframe time	
Backoff Slot Time	20 μs
SIFS	10 μs
DIFS	50 μs
Phy header	
Preamble Length	144 bits
PLCP Header Length	48 bits
MAC header	
MAC Header Length	224 bits
RTS, CTS and ACK	
RTS	160 bits + Phy header
CTS, ACK	112 bits + Phy header
Radio	
Radio Propagation	Two Ray Ground

In this paper we study two important parameters that can be used to optimize the effectiveness of the self-restraint mechanism, the *PAM* and the *CTL*. These two parameters determine the effectiveness of the self-restraint mechanism to block or admit nodes at above and below congestion levels respectively. It is therefore important to properly tune these parameters in order to provide effective node admission blocking. The *PAM* provides time for the node to monitor the collision rates. A long duration of *PAM* will increase the probability of node admission being restrained by the self-restraint mechanism. This will provide effective node admission blocking, but it will also increase the probability of the node being blocked when the channel is below the congestion threshold. A short duration for *PAM* will decrease the probability of node blocking, which serves well for new nodes, but is not ideal for dealing with a congested channel. Similarly, the *CTL* affects the probability of node blocking or admission in the network.

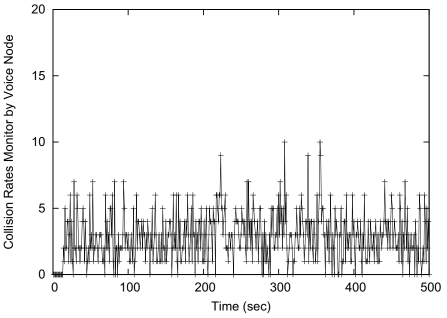

Fig. 3. Rate of collision monitored by a node carrying voice traffic with the channel above the congestion level

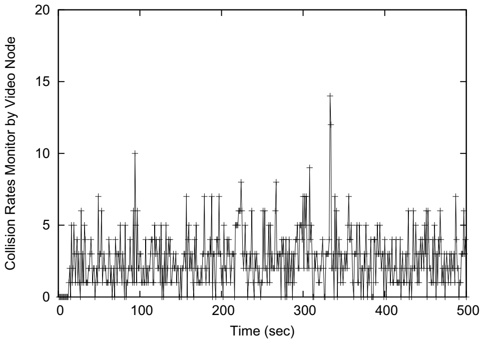

Fig. 4. Rate of collision monitored by a node carrying video traffic with the channel above the congestion level

III. Analysis of Post Monitoring Time *(PAM)* and Collision Threshold Level *(CTL)*

We set up an adhoc WLAN scenario as shown in Figure 2 with no AP acting as an arbitrator. Each node carries voice, video or best-effort traffic. We adopt the same parameters as in the 802.11 standard which is shown in Table I. We run the simulation with all nodes simultaneously trying to access the channel based on the CSMA/CA as in the 802.11b MAC protocol. We create two traffic channel scenarios, one with the channel at above the congestion threshold level and the other at below congestion threshold level. For the former, we create an estimation scenario of traffic slightly above 100% network channel capacity, while for the latter, it is about 90% network channel capacity. The collision rates monitored by

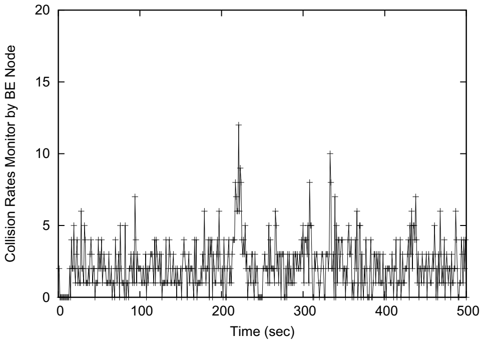

Fig. 5. Rate of collision monitored by a node carrying best-effort (BE) traffic with the channel above the congestion level

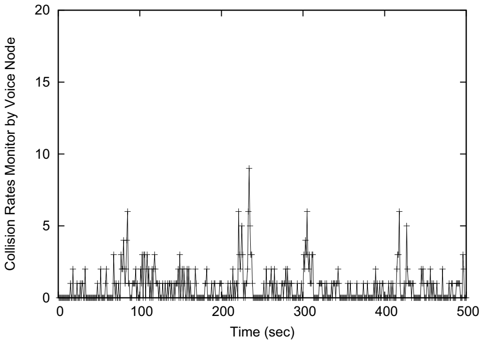

Fig. 6. Rate of collision monitored by a node carrying voice traffic with the channel below the congestion threshold

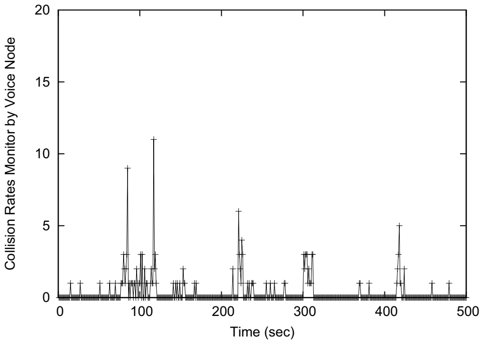

Fig. 7. Rate of collision monitored by a node carrying video traffic with the channel below the congestion level

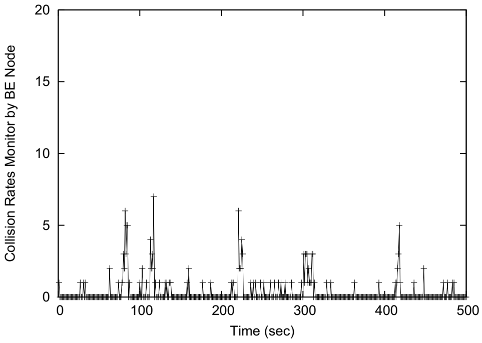

Fig. 8. Rate of collision monitored by a node carrying best-effort (BE) traffic with the channel below the congestion level

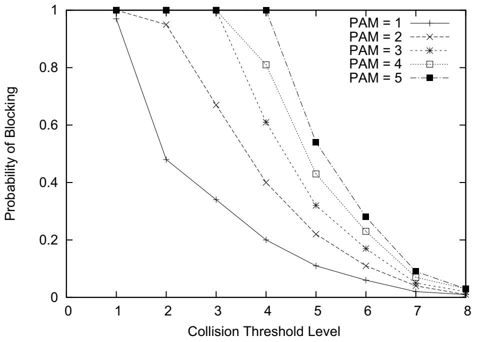

Fig. 9. Probability of blocking of a node carrying voice traffic with the channel above the congestion threshold

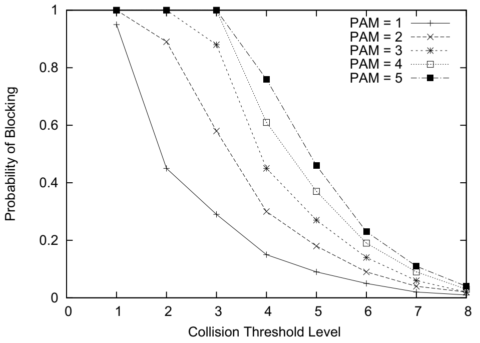

Fig. 10. Probability of blocking for a node carrying video traffic with the channel above the congestion threshold

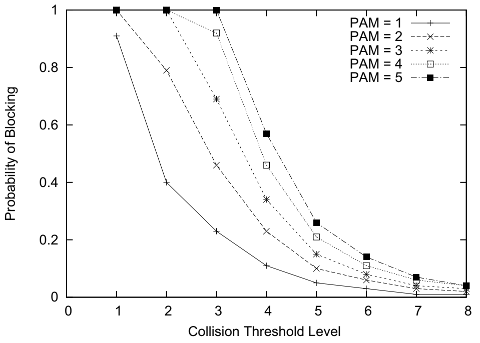

Fig. 11. Probability of blocking for a node carrying best-effort (BE) traffic with the channel below the congestion level

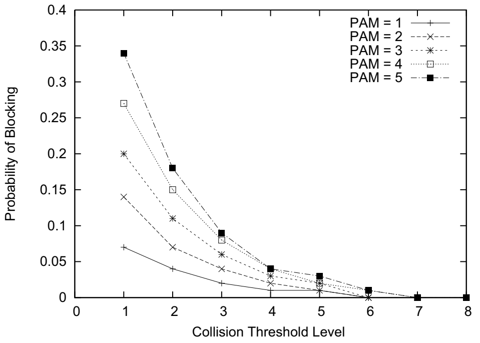

Fig. 12. Probability of blocking of a node carrying voice traffic with the channel below the congestion threshold

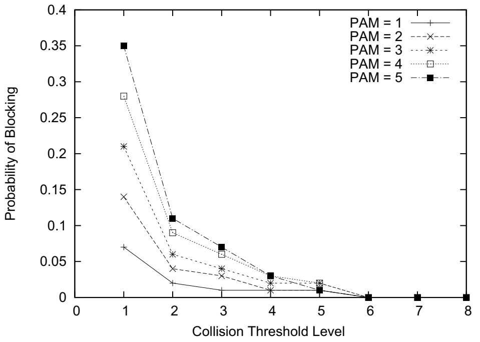

Fig. 13. Probability of blocking for a node carrying video traffic with the channel below the congestion level

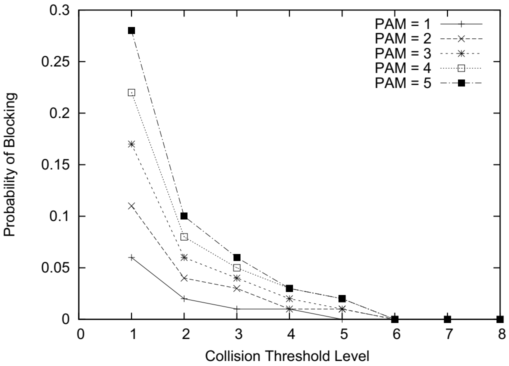

Fig. 14. Probability of blocking of a node carrying best-effort (BE) traffic with the channel below the congestion threshold

each node carrying voice, video or best-effort (BE) traffic in the channel, with the traffic above the congestion level, are shown in Figures 3, 4 and 5, while equivalent data for the traffic below the congestion level are shown in Figures 6, 7 and 8.

From these results, we derive the optimized value of the *PAM* and the *CTL*. We set the value of *PAM* from 1 to 5 and *CTL* from 1 to 8. The probability of admission for each node with the channel at above the congestion level is shown in Figures 9, 10 and 11, the same for the channel below the congestion level is shown in Figures 12, 13 and 14. When the *PAM* and the *CTL* increase, the probability of a node being dropped increases and decreases, respectively.

To provide effective admission control for the self-restraint mechanism, the optimum value is chosen so that with the traffic at above the congestion level the probability of a drop is maximised, while with the traffic at below the congestion level the probability of drop is minimised. For the *PAM* equal to 3 and above and the *CTL* equal to 3 and below, the probability of a drop for a node carrying voice traffic is 1.0, with the channel above the congestion level (Figure 9). In contrast for traffic at below the congestion level, with both the *PAM* and the *CTL* equal to 3, the probability of admission drop is 0.07 (Figure 12). For video traffic at above and below the congestion level respectively, the probability of admission drop is about 0.9 (Figure 10) and about 0.05 respectively for both the *PAM* and the *CTL* equal to 3 (Figure 13). For best-effort traffic, with both the *PAM* and the *CTL* equal to 3, the probability of admission drop when the channel is above and below the congestion level is about 0.95 and 0.04 respectively.

In our admission control technique, the pre admission monitoring time, *PRAM*, is not as critical as the post admission monitoring time, *PAM*. This is because the channel congestion level, before the new node accesses the channel, has been sustained by the admission control mechanism and the probability of admission being rejected is low. The accurate congestion level will only be measured when the new node has accessed the channel as a surge in the rate of collision can take place after the access. This is a critical time when the new node decides whether to apply self-restrain or access

TABLE II

Times That Nodes are Introduced to the Network

Time (sec)	Traffic
1	Voice
30	Video
60	Best-effort
90	Voice
120	Video
150	Voice
180	Video
220	Voice

TABLE III

Parameters of Traffic Types Used in Simulations

Traffic Type	Transport Protocol/Applications	Bit rate
Voice	UDP/CBR	64 Kbps
Video	UDP/CBR	960 Kbps
Best-effort (CBR)	UDP/CBR	320 Kbps
Best-effort (VBR)	TCP	-

the channel according to the rules laid down by the algorithm. We recommend a *PRAM* duration of 1-3 seconds since a long *PRAM* will delay the admission of a new node.

IV. Simulation Results

We set up an adhoc WLAN scenario as shown in Figure 2 with no AP acting as an arbiter. All nodes are within the communication range of each other so as to eliminate the "hidden-nodes" and multi-hopping problems. These two issues need to be addressed differently and are outside the scope of this research. Each node carries voice, video or best-effort traffic. We increase the traffic load at regular intervals by introducing a new node every 30 seconds into the network. Table II shows the times and types of of nodes being introduced into the network. For performance comparisons, we use the IEEE 802.11 Distributed Control Function (DCF) MAC protocol [1] with parameters as shown in Table I. The parameters for voice, video and best-effort traffic are shown in Table III. We then implement the self-restraint admission control mechanism in each node. The throughput for the three traffic types in the simulation with and without admission control mechanism are shown in Figures 16 and 15 respectively.

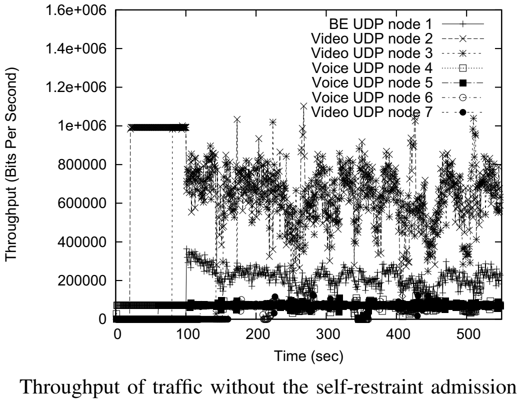

Fig. 15. Throughput of traffic without the self-restraint admission control

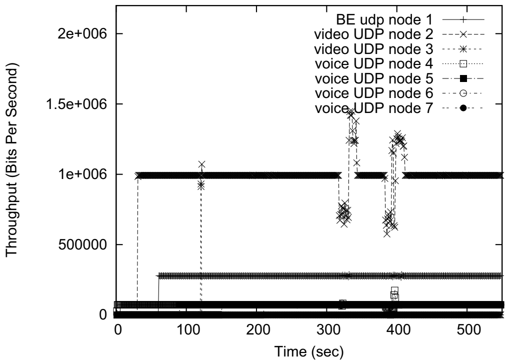

Fig. 16. Throughput of traffic with self-restraint admission control

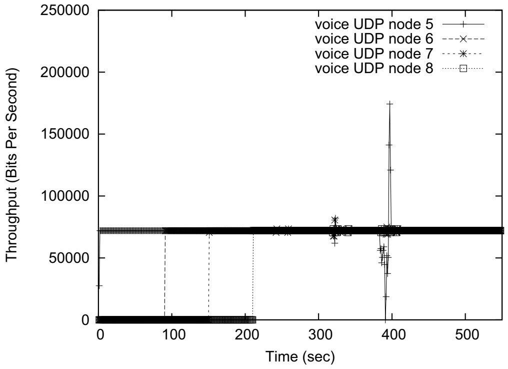

Fig. 17. Throughput of voice traffic with admission control extracted from Figure 16

The results show that the self-restraint admission control successfully maintains throughput for all traffic to a sustained level and supporting QoS by blocking new connection admissions when the channel traffic reaches congestion. To provide a clear picture, we separate the performance results for voice, video and BE (Figures 17 and 18). In these latter figure, a new node (video UDP node 3) tries to access the channel at 120 seconds. The self-restraint mechanism in the node drops the connection when it detects that the congestion level is high. A node (video UDP node 2), that has been accessing the channel, is protected from being dropped because it has been

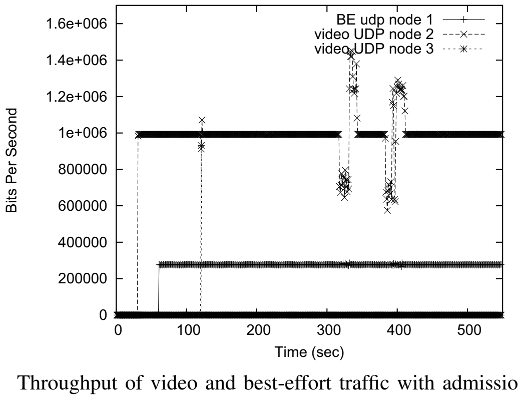

Fig. 18. Throughput of video and best-effort traffic with admission control extracted from Figure 16

communicating for more than a set *PAM* time which is set to 3. Nodes carrying voice traffic (voice UDP node 7 and node 8) are allowed to access the channel as the congestion level is still sustained below the threshold even after these nodes are admitted (Figure 17). By maintaining traffic below the congestion level, the self-restraining mechanism successfully maintains collision below *CTL*. This protects all traffic in the network and prevents the network from becoming unstable. Figures 17 and 18 also demonstrate that a short burst in the throughput of video and voice traffic occurs before it stabilizes and is sustained. This occurrence is the result of the contention mechanism adjusting to the queuing build-up in each node and its effect is only momentary.

V. Conclusion

In this paper we have presented an effective admission control mechanism for adhoc WLANs based on a self-restraining technique. We have shown that the rate of collisions in the WLAN network reflects the network traffic congestion level and provides a good metric to be used in the self-restraining mechanism. We have determined the optimum range of the collision threshold value and have shown that with these values, the probability of blocking of nodes that wish to join the network, is high when the network traffic is above the congestion threshold and low when the network traffic is below the congestion threshold. Another important parameter that has been highlighted in this paper is the post monitoring time. Long post monitoring time increases the probability of connection blocking while short post monitoring time will decrease the probability of connection blocking. We implemented the self-restraint admission control mechanism in each of the node and showed that admission control is successfully achieved in the simulated adhoc WLAN.

Our proposed connection admission control technique offers other advantages such as ease of implementation and interoperability with any type of wireless MAC protocol that uses carrier sense multiple access as in the legacy IEEE 802.11b or IEEE 802.11e [2]. Our technique can also provide prioritized admission control to priority traffic by tuning the collision rate threshold levels according to the traffic priority. The proposed admission control mechanism has not been tested in an environment where hidden nodes exist and where multi-hopping is needed. Our future work will include investigation of the effectiveness of the designed mechanism in these environments. The same overall principles will also be used to design a load balancing mechanism in WLAN.

References

[1] IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", 1999.

[2] IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications, Amendmend 8: Medium Access Control (MAC) Quality of Service Enhancements", 11 November 2005.

[3] Ping Wang, Hai Jiang and Weihua Zhuang, "Capacity Improvement and Analysis for Voice/Data Traffic over WLAN", IEEE Transactions on wireless communications, Vol 6, pp. 1530-1541, No 4, April 2007.

[4] Jiang Liu and Zhisheng Niu, "A Dynamic Admission Control Scheme for QoS Supporting in IEEE 802.11e EDCA", Wireless Communications and Networking Conference 2007 (WCN07). IEEE. pp. 3697-3702, March 2007.

[5] Taekyu Kim, Seungbeom Lee and Sin-Chong Park, "Call Admission Control Based on Adaptive Physical Rate for EDCA in IEEE 802.11e WLAN System", 5th IEEE Consumer Communication and Networking Conference, 2008 (CCNC 2008). pp. 59-61, Jan. 2008.

[6] K.Fall and K. Varadhan, "The ns manual", 2005.

[7] Hongqiang Zhai, Xiang Chen and Yuguang Fang, "A call admission and rate control scheme for multimedia support over IEEE 802.11 wireless LANs", Wireless Networks (2006), Kluger Academic Publishing, USA.

[8] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function", IEEE Journal on Selected Areas in Communications, vol. 18, pp. 535-547, 2000.

[9] P. Chatzimisios, A.C. Boucouvalas, and V. Vitsas, "Performance analysis of the IEEE 802.11 MAC protocol for wireless LANs", Int. J. Commun. Syst, Vol 18, pp. 545-569, 2005.

[10] Aura Ganz, Zvi Ganv and Kitti Wongthavarawat, "Multimedia Wireless Networks - Technologies, Standards and QoS", Prentice Hall PTR, Upper Saddle River, NJ, 2004.

[11] Behrouz A. Forouzan, "Local Area Networks", McGraw-Hill Higher Education, 2003.

[12] Jiang Zhu and Abraham O. Fapojuwa, "A new Call Admission Control Method for Providing Desired Throughput and Delay Performance in 802.11e Wireless LANs", IEEE Trans. on Wireless Communications, Vol. 6 No 2, February 2007.

[13] Telecommunication Standardization Sector of ITU "Series G: Transmission System and Media, Digital System and Networks", International Telecommunication Union (ITU-T), Recommendation G.114, Mei 2003.

[14] Todor Cooklev, "Wireless Communication Standards - A study of IEEE 802.11^{TM}, 802.15^{TM}, and 802.16^{TM}", IEEE Standards Wireless Networks Series, 2004 NY.