2008

Node Admission Control For Multimedia Traffic In Ad-Hoc WLANs

Hushairi Zen
Edith Cowan University

Daryoush Habibi
Edith Cowan University, d.habibi@ecu.edu.au

Iftekhar Ahmad
Edith Cowan University, i.ahmad@ecu.edu.au

Alexander Rassau
Edith Cowan University, a.rassau@ecu.edu.au

10.1109/ATC.2008.4760612
This is an Author's Accepted Manuscript of: Zen, H. , Habibi, D. , Ahmad, I. , & Rassau, A. M. (2008). Node Admission Control For Multimedia Traffic In Ad-Hoc WLANs. Proceedings of International Conference on Advanced Technologies for Communications. ATC 2008. (pp. 417-420). Hanoi, Vietnam. IEEE Press. Available here

Node Admission Control for Multimedia Traffic in Adhoc WLANs

Hushairi Zen, Daryoush Habibi, *Senior Member, IEEE*, Iftekhar Ahmad and Alexander Rassau
School of Engineering and Mathematics
Edith Cowan University
Joondalup, WA 6027
Australia.
Email: hzen@student.ecu.edu.au

***Abstract*— In this paper, we design an admission control scheme for adhoc WLAN based on self-restraint mechanism. The self-restraint admission control mechanism is implemented in each of the wireless nodes instead of the access point (AP). It has two important admission control abilities: first, it can restrain itself from joining the network if the network channel is congested; second, a joining node can drop itself from the network if the channel becomes congested as a result of its admission. We simulate an adhoc WLAN and show that the self-restraining mechanism works effectively in sustaining traffic in adhoc WLAN and also protects real-time traffic.**

I. Introduction

The advancement of wireless local area network (WLAN) technology has opened up wider applications for wireless communications. One of the potential applications is the adhoc WLANs [1]. It provides ease of installation and is independent of an access point (AP). It can be used for rescue operations in disaster areas, battle-fields, adhoc meeting environments and hospitals.

However, one important issue that needs to be addressed in adhoc WLANs is control over admission of new nodes into the network. When the channel is congested, problems such as drop in throughput, delay and jitter occur. This results in unstable network as the bandwidth share of each traffic flow diminishes and fluctuates. Since real-time traffic such as voice and video require absolute throughput and delay provision from the network, management of resources becomes an important issue in adhoc WLAN. A mechanism to provide admission control is important to monitor and police the network.

In an infrastructured WLAN set-up, admission control is managed by the AP. 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 needs to listen and gather information regarding the channel traffic load and capacity needs of the nodes in the network, to make effective decisions. In the 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 have been implemented in an adhoc WLAN without using an intermediatory device. Some of the published research on admission control in WLAN, such as in [2], [3] and [4], used an AP as an intermediatory device.

TABLE I
Times Nodes are Introduced to the Network

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

In this paper, we design an admission control scheme for adhoc WLAN based on a self-restraint mechanism. We implement it in each of the wireless nodes in an adhoc WLAN topology. Using the NS2 [5] simulator, we show that the self-restraining mechanism works effectively in sustaining traffic in adhoc WLAN and protects real-time traffic in multimedia applications. The self-restraining mechanism works by monitoring the channel collision rate. It has two important abilities to keep traffic congestion to a level where throughput of all traffic is sustained. First, it has the ability to restraint itself from joining the network if the collision rate is too high. Second, if by joining the network, the channel becomes congested, the admission control mechanism in the node will drop itself and wait for a period of time to join the network again. To design an effective self-restraint mechanism, we study and analyse the behaviour of the collision rate and contention window size in each node.

II. Impact of Traffic Congestion Levels on Collision Rates

In a self restraint mechanism, each node monitors the collision rates in the adhoc network. The probability of collision in the network is a direct function of the traffic load in the network. This is shown in our derivation and our observations using simulation which support the work in [6] and [7].

We create a simulation scenario where wireless nodes are place within range of all other nodes as shown in Figure 1. By placing nodes within communication range of each other, we assume there are no "hidden-nodes" and multi-hopping problems as these two issues need to be addressed

978-1-4244-2681-2/08/$25.00 ©2008 IEEE

Fig. 1. Simulation scenario

TABLE II
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	-

differently and are outside the scope of this research. Each node carries voice, video or best-effort traffic. We increase the load at regular intervals by introducing a new node every 30 seconds into the network until the traffic in the network reaches congestion (Table I). We adopt the legacy IEEE 802.11b protocol parameters [8] in the simulation and the parameters for voice, video and best-effort traffic are shown in Table II.

The simulations provide an important relationship between traffic load and collision rate. Figure 2 shows the throughput of voice, video and best-effort traffic in the adhoc WLAN without the self-restraint admission control. We extract voice, video and best-effort traffic separately as shown in Figure 3, 4 and 5 respectively to provide a clearer picture of the throughput. The collision rates of voice and video are shown in Figure 12 and Figure 13 respectively. It is observed that nodes in the network basically hear the same pattern of collision rate and this pattern relates with congestion level of the network. This relationship is used to implement a self-restraint admission control mechanism for adhoc WLAN. Our simulation analysis shows that when the network reaches congestion, the collision rate monitors by the wireless nodes goes beyond 5 collisions per second. This rate of collision is used to tune the self-

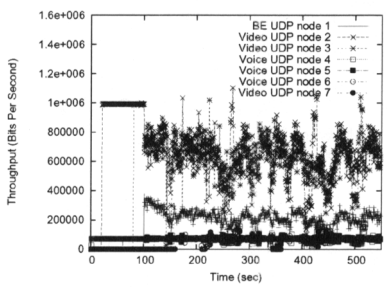

Fig. 2. Throughput of wireless nodes in adhoc WLAN without the self-restraint admission control

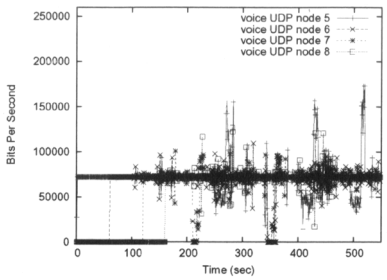

Fig. 3. Throughput of voice traffic without the self-restraint admission control extracted from Figure 2

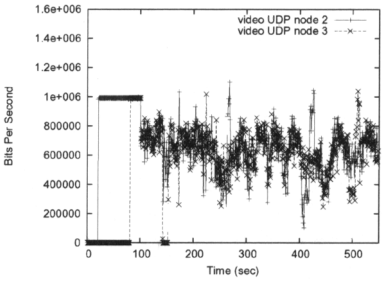

Fig. 4. Throughput of video traffic without the self-restraint admission control extracted from Figure 2

restraint mechanism in each node and to provide the most effective admission control.

III. PROPOSED NODE ADMISSION CONTROL WITH SELF-RESTRAINT MECHANISM

The fundamental concept of the proposed self-restraint admission control is to provide a mechanism for the network to operate at below congested or busyness levels. This is achieved by managing the association of new nodes into the network and dropping nodes that result in the network becoming over congested. With this mechanism, new nodes can only join the network if they sense 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 accepted level. If the congestion level increases above the *collision threshold level (CTL)*, when a new node joins the network, it will automatically restraint itself from continuing the communication. Nodes that have been communicating in

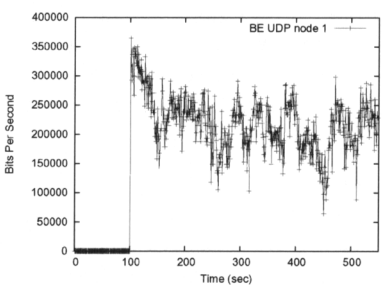

Fig. 5. Throughput of best-effort traffic without the self-restraint admission control extracted from Figure 2

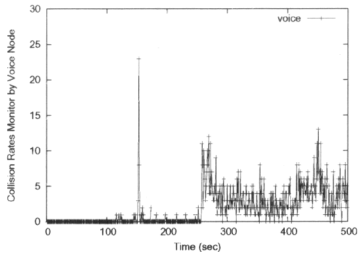

Fig. 6. Collision rate monitored by voice traffic without the self-restraint admission control

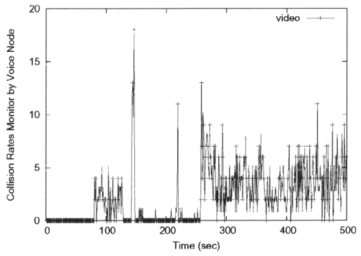

Fig. 7. Collision rate monitored by video traffic without the self-restraint admission control

the network for more than a set period of time, will continue in the service and are protected from being dropped. This time period, which we call *post admission monitoring (PAM)* time, functions as a period to monitor the traffic congestion level after the node joins the network. This time can be set by the network management, and in our simulations, this period is set at 5 seconds.

The self restraint mechanism is implemented in each of the wireless nodes at the MAC layer. As shown in the flow chart in Figure 8, when the new node wants to join the network, it listens to the collision rate in the channel for a few seconds. If the collision rate is above the *CTL* value, the node backoff and starts listening again. If it is below *CTL*, it transmits after a DCF interframe space (DIFS) and joins the network. During this time it will be in the *PAM* time and monitors the network congestion level. If congestion level is not above the *CTL* due to the new node joining the network within the *PAM* time, it has successfully access the channel and are 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 has to listen again.

We studied two parameters that can potentially be used to determine the level of busyness in the adhoc network, the rate of packet collisions and the node's contention window size. However, it was observed in our study that using the collision rate as a parameter to determine the congestion level is much simpler to achieve and more effective to implement.

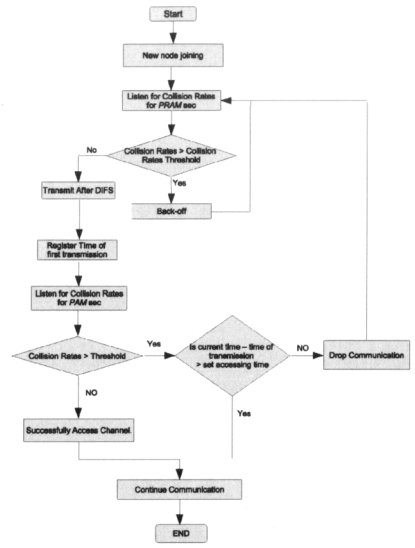

Fig. 8. Flow chart of the self-restraint admission control algorithm

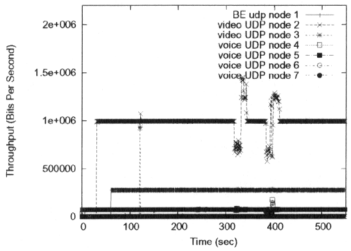

Fig. 9. Throughput of voice, video and best-effort traffic with the self-restraint admission control

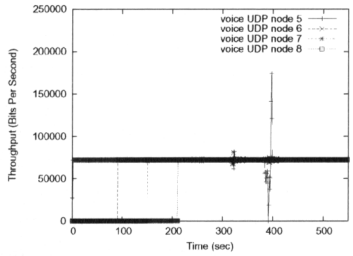

Fig. 10. Throughput of voice traffic with the self-restraint admission control extracted from Figure 9

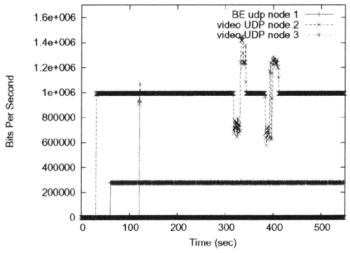

Fig. 11. Throughput of video and best-effort traffic with the self-restraint admission control extracted from Figure 9

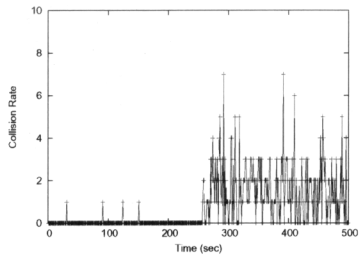

Fig. 12. Collision rate monitored by the node carrying voice traffic implementing the self-restraint admission control

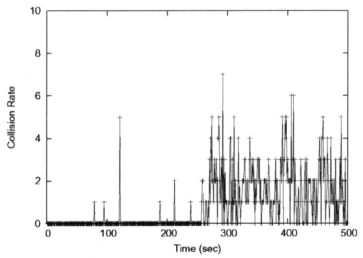

Fig. 13. Collision rate monitored by the node carrying video traffic implementing the self-restraint admission control

IV. Self-restraint Admission Control Simulation Results

We set up an adhoc WLAN scenario as shown in Figure 1 with no AP acting as an arbiter. Similar to the analysed scenario in section II, we create nodes carrying voice, video or best-effort traffic and retain the same parameters. We implement the self-restraint admission control in each of the nodes and set the *CTL* to 5. The throughput of traffic in the simulation is shown in Figure 9. The results show that the self-restraint admission control successfully maintains throughput for all traffic to a sustained level and supporting QoS. This is achieved by blocking new admissions when the congestion level is high and dropping a new node in the network if its admission has caused a congestion level higher than *CTL*. To provide a clear picture, we show the information for the three traffic typesin Figures 10 and 11. As can be seen in these figures, a new node (video UDP node 3) carrying video traffic 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. An existing node that has been accessing the channel (video UDP node 2) is protected from being dropped because it has been communicating for more than a set *PAM* time. Nodes carrying voice traffic (voice UDP node 7 and node 8) are allowed to access the channel as congestion level is still sustained below the *CTL* even after these nodes are admitted. By maintaining traffic below the congestion level, the self-restraining mechanism successfully achieves a collision rate of less than 5 as shown in Figures 12 and Figure 13. This protects all traffic in the network and avoids network instability. It is also observed in these figures that a short burst in the throughput of video and voice traffic occurs before they settle down and are sustained. This phenomemon is the result of the contention mechanism adjusting to the queuing build-up in each node and its duration is only momentary.

Comparing these results to the case without admission control, as shown in Figure 2, it can be deduced that the self-restraint admission control mechanism manages to sustain consistent throughput. Without the self-restraint admission control, the throughput fluctuates heavily when the channel is congested, as shown in Figure 2. When the network traffic is below the congestion level, the throughput of all traffic is consistent and steady. Once the congestion threshold is exceeded, introducing further traffic will cause throughput in all nodes to fluctuate and the network to fail. The rate of collisions increases drastically above the system congestion level and throughput of every node decreases rapidly.

V. Conclusion

This paper has highlighted an important admission control mechanism for adhoc WLANs. We have shown that admission control can be successfully implemented by the self-restraint mechanism in each node which uses collision monitoring techniques. Information about the congestion level in a network enables the self-restraint mechanism to work effectively in each of the wireless nodes. This admission control technique offers network designers more flexible network topologies as an AP is not necessary for implementing admission control functions.

Other advantages offered by this technique are the 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. The proposed admission control mechanism has not been tested in an environment where "hidden nodes" exist and multi-hopping is needed. Our future research includes investigation into the effectiveness of the designed mechanism for "hidden nodes" and in multi-hopping environments. The same general principles may also be used to design a load balancing mechanism in WLAN.

References

[1] Benny Bing, "Wireless Local Area Networks - The New Wireless Revolution", Wiley Interscience, 2002 New York.

[2] Ping Wang, Hai Jiang 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.

[3] Jiang Liu and Zhisheng Niu, "A Dynamic Admission Control Scheme for QoS Supporting in IEEE 802.11e EDCA", Wireless Communications and Networking Conference 2007 (WCNC07), IEEE, pp 3697-3702, March 2007.

[4] 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.

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

[6] 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.

[7] 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.

[8] IEEE, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications", ANSI/IEEE STD 802.11, 20 August 1999