An End-to-End Measurement-Based Admission Control Policy for VoIP over Wireless Networks

Ala’ Khalifeh  
Department of EECS  
University of California, Irvine  
[akhalife]@uci.edu

Abstract—in this paper, we present a new policy for admitting Voice over IP (VoIP) sessions over wireless networks. Our proposed policy receives the admission information advertised by the VoIP gateway on the wired network, and uses it to decide whether a new VoIP session can be admitted or not. The proposed policy can be easily integrated with the current Call Admission Control algorithms used in wireless networks. We show that implementing the proposed policy increases the number of successful VoIP sessions admitted to the access point polling list, thus improving the wireless network utilization.

I. Introduction

The emergence of wireless networks and the evolution of 802.11e standard, have created a promising infrastructure for delivering real-time Internet applications such as Voice over IP (VoIP) over wireless networks. To provide QoS support for real-time traffic over wireless networks, various mechanisms have been proposed that lead to the current 802.11e standard. Call Admission Control (CAC) is one of these mechanisms that determines whether a new VoIP session can be admitted into the network or not. The Quality of Service Enabled Access Point (QAP) admits calls only if their QoS constraints can be met, without jeopardizing the QoS constraints of the existing calls in the network. Once the QAP admits a VoIP session, the VoIP terminal issues a call setup request to the VoIP softswitch which uses another call admission control policy to ultimately determine whether or not this VoIP call can meet its end-to-end quality of service constraints. Accordingly, the final admission decision is issued by the VoIP softswitch, and the call is either torn down or successfully conducted. The current CAC algorithms used in the QAP do not take into account whether the end-to-end QoS constraints of the admitted VoIP sessions can be met or not. The proposed policy ensures that the QAP admits the VoIP sessions only if its end-to-end QoS constraints can be achieved. As a result, implementing the proposed policy improves the utilization of the wireless networks, and increases the number of successful VoIP sessions conducted within a certain period of time. In literature, the cited call admission control algorithms suggested for wireless networks use the local wireless available resources such as: bandwidth, collisions, and the number of admitted VoIP sessions as a threshold parameters in the admission process, and do not take into account the end-to-end QoS constraints. An extensive survey of the recent call admission control algorithms for 802.11e networks can be found in [5]. A brief description of the algorithms mostly related to our work is summarized. In [10], [13] the authors proposed a Distributed Admission Control algorithm (DAC). In DAC the QAP announces a transmission budget for each Access Category (AC), the stations receive this information and send their traffic. The QAP measures the total amount of time occupied by the transmitted traffic of each AC, and subtracts it from the transmission budget of that category. If the transmission budget of that AC is vanished, the new flow will not be admitted, and the admitted flows will not be allowed to increase their transmission time either. The authors also suggested a Two Level Guarantee and Protection Mechanism, in which the first-level protects the existing voice and video traffic from the new QoS traffic, while the second level protects the QoS traffic from the best-effort traffic. A Threshold-Based Admission Control algorithm is suggested in [6]. In this algorithm, each station measures the traffic load conditions of the wireless network. If the measured traffic conditions were above certain upper level threshold, the network is considered highly loaded, so the wireless station will stop transmitting the lower priority AC traffic, so more priority is given to the higher priority AC traffic. If the traffic conditions become around medium threshold or below lower level threshold, the network is considered inefficiently utilized, and the station will resume transmitting the lower priority AC traffic. The most related work to our proposed policy can be found in [11], the authors proposed a scheme based on the Endpoint Admission Control (EAC) paradigm. According to their scheme, the caller probes the path to the VoIP server, and determines whether the originating path is good or not, if it is good, the callee will receive a call setup request from the VoIP server, so the callee will probe the path to the VoIP server, to make sure that the terminating path is in good conditions. If the path is good, the call is admitted. The proposed scheme works well if the caller and callee are within the same local area network as they assumed. While our proposed scheme works well for all cases, whether calls are issued within local area networks or within the Internet. Also according to their suggested scheme, the same procedure is repeated for different calls that target the same callee network, while in our proposed scheme, the caller will take advantage of the call admission caching functionality exits in the VoIP softswitch and the QAP, which will reduce the call setup time. In addition, our proposed scheme is more realistic and practical since it resembles the current deployed VoIP networks in which call admission control and probing is done in the VoIP softswitch and VoIP gateways, not on the end systems. Besides, the proposed scheme takes advantage of the upcoming QAP which has more advanced fea-
The Internet

Fig. 1. Network Architecture for Voice over Wireless Networks.

The PSTN Network

The Internet

VoIP Gateway

VoIP Enabled Mobile phones

User B

Softswitch

Laptops with VoIP soft phones

WLAN

Access Point

VoIP Gateway

Laptops with VoIP soft phones

Domain 2

IP Phones

PSTN PBX

PSTN phones

TRUNK Internet

PSTN Network

User A

Softswitch

Domain 1

VoIP Enabled Mobile phones

Laptops with VoIP soft phones

Access Point

VoIP Gateway

IP Phones

PSTN PBX

PSTN phones

tures than the traditional access points; such as QoS, layer 2/3 and roaming support [1][2].

The remainder of the paper is organized as follows: General description of VoIP network architecture is presented in Section II. The proposed end-to-end measurement-based admission control policy is presented in Section III. Simulation setup and results are presented in Section IV. Finally, Section V concludes the paper and suggests future work.

II. VOICE OVER IP NETWORK ARCHITECTURE

Fig. 1 depicts the network architecture for a VoIP enabled network, including both wired and wireless VoIP terminals. Here we assume that the Session Initiation Protocol (SIP) is the protocol used for signaling purposes and for call set up. For more details a bout network components and architecture, the reader is encouraged to look at [12][8]. The following scenario shows how a VoIP call over wireless network is established. Let us suppose that user A in Domain1 would like to call user B in Domain2. When user A accesses the wireless network, the QAP uses Call Admission Control algorithm to determine whether or not the wireless network can safely admit the new VoIP call. If the call is admitted, user A will send a call setup request to the VoIP softswitch (SIP INVITE message), Fig. 2. The softswitch called (Proxy server in case SIP protocol is used or Gatekeeper in case H.323 protocol is used) [8], will perform some operations; such as authorization, authentication, and accounting. After that, the softswitch will lookup the IP address of the domain of the destination VoIP gateway (Domain2). Notice that in some networks, address lookup can be done in the local Domain Name Server (DNS) of the network. So once the destination IP address is determined; the VoIP gateway checks the links status by using an appropriate Call Admission Control mechanism. End-to-End Measurement-Based Admission Control is one of the widely used admission control in VoIP gateways [3]. The VoIP gateway gauges the quality of the network path, by sending probes to the destination IP address, which is usually the IP address of the destination gateway or the destination softswitch, and measures the end-to-end delay, packet loss, and jitter delay of these probes to determine the quality of the network path [3], which will be reported to the softswitch. The softswitch uses this information to determine whether the call can be admitted or not, if the call is not admitted, the connection is rejected, and a busy signal will be sent to the VoIP terminal. The process is repeated till the call is successfully established.

INVITE SIP: USER A @ Domain1.com SIP/ 2.0 Via:SIP/2.0/UDP From: sip: USER A @ Domain1.com To: sip: USER B @ Domain2.com

III. THE PROPOSED END-TO-END MEASUREMENT-BASED ADMISSION CONTROL POLICY

In this Section, we will describe our proposed scheme, and show how it improves the network utilization and the number of successful VoIP calls conducted within specific period of time. As mentioned in Section II, probing the path is done in the VoIP gateway and the end-to-end link status is reported to the VoIP softswitch to be used in the admission process. We have proposed to report this information to the QAP too, so it can be used as a policy in the call admission process in the wireless domain, so this way and after the QAP performs the call admission algorithm, this policy is checked to see whether this call will be admitted by the VoIP gateway or not, if the information reported about the end-to-end path link of this call indicates that the destination path is congested and this call can not be admitted, the QAP rejects the call and does not register it in the Hybrid Coordination Controlled Channel Access (HCCA) polling list[9], consequently, the wireless resources will not be
wasted in admitting unsuccessful VoIP call that will be ultimately rejected by the VoIP gateway. At the beginning, neither the softswitch nor the QAP has entries in their link status table, so the QAP will admit all the calls, and the softswitch will start building the link status table for these calls, so once this table is populated, it will be sent to the QAP to be used for the new incoming calls. The link information for the destination networks is stored in a lookup table that contains the destination addresses, and its’ paths status. So once the VoIP call is received by the QAP, its destination address is checked using that table, and the call is admitted only if its end-to-end path conditions are satisfactory. Caching concept is also used in our proposed scheme, so the links status information for the destination networks is kept in cache memory for certain time-out period, the VoIP gateway keeps updating the softswitch and the QAP with the status of the destination networks attempted so far. After certain time-out period, the link status information related to certain network destination is removed from the table, if no one accesses that network. Fig. 3 depicts how our policy can be integrated with the QAP call admission algorithm. To further shows the benefits and the justifications of implementing this policy. Let us look at a scenario in which the caller is trying to establish a VoIP call to a congested network. As discussed above, after the caller terminal device establishes a connection with the access point, and registers itself as one of the admitted stations in the polling list, the caller will contact the softswitch, and go through billing, authentication, authorization, IP address look up stages, and finally checks whether the call can be admitted or not [7][3]. In this case, the call is rejected and a busy signal is sent back to the caller terminal, which will try again to establish a connection and go through the previous process, until the destination link becomes less congested, so the call can be admitted, or until the caller gives up and stops from setting up the call. As we can notice that during the failed call setup attempts, the caller terminal utilizes the wireless channel, and registers itself in the polling list for the whole period of time used in attempting to conduct the call. This time might be significant, for the following reasons:

I. Contacting the softswitch might take some time due to the fact that in real networks, the softswitch is usually hosted in the Internet Service Provider (ISP) network, not in the local wireless network. II. Some time will be wasted for doing authentication and other functions mentioned earlier, which is considered useless as far as the call will be rejected. III. The softswitch might be loaded or its links might be congested, which might increase the process and access time. IV. Usually, once the VoIP is rejected by the VoIP gateway, the caller station will still be registered in the QAP polling list, so the caller will keep trying many times to establish a call, and according to the network congestion statistics, the successive trials most likely will fail, since usually the congestion in network path lasts for a period of time [4]. While according to our policy, rejecting the call from the first time will give the opportunity for other stations to access the network, which might conduct VoIP calls with different destination networks that do not have congestion, thus improving the utilization of the wireless network, and increases the number of successful VoIP calls.

![Fig. 3. Integrating the suggested policy with the current QAP Call Admission algorithms.](image)

IV. SIMULATION SETUP AND RESULTS

To evaluate the performance of the proposed policy, we simulate the proposed policy using the network diagrams shown on Fig. 1. We supposed that both the caller and the callee have similar network infrastructure to the one depicted on Fig. 1, and the users on Domain 1 is trying to conduct a VoIP call to other wireless users on different networks. We assume that the wireless network always in a saturation level, i.e., the number of the wireless stations trying to make a VoIP call is very large, and exceeds the maximum number of VoIP calls that can be admitted. So this assumption shows the effectiveness of applying the proposed policy in terms of increasing the network utilization, and increasing the blocking/admission probability for the unsuccessful/successful VoIP calls. We define the network utilization as the ratio between the time used in conducting successful VoIP calls (the calling time) and the sum of the wireless network access time, the time spent on trying to conduct unsuccessful VoIP calls, and the the time spent on trying to conduct successful VoIP calls (the calling time). The call is considered successful if its end-to-end delay is below 150 ms at the time of establishing the call, while the call request is tear down and rejected if its end-to-end delay exceeds 150 ms. As shown in Fig. 1, when stations in Domain 1 access the wireless channel to conduct a VoIP call with one of stations on the other destination networks, the VoIP calls follow certain path in the Internet. To simulate the major Internet backbone paths, we have modeled the Internet backbone networks using six major paths Fig. 4 (a),(b),(c) and Fig. 5 (a), (b), (c) show the delay characteristics of these paths as described in [4]. So the VoIP calls eventually will go through one of these paths before reaching the final destination network. The first path is assumed to have high delay variability with random delay pattern, the delay in this pattern is considered below 150 ms most of the time, and follows a random pattern, Fig. 4 (a). The second path is assumed to have high delay variability with very high delay spikes, the delay in this pattern reaches very high values (in the range of 400 – 700 ms) every 10 – 20 ms, followed by low spikes of values below 150 ms, Fig. 4 (b). The third path is assumed to have high delay variability with blocking pattern, it consists of cluster of spikes of 250 ms that lasts for 1 second, followed by low spikes below 150 ms. The cluster is repeated every 2 – 3 seconds Fig. 4 (c). The fourth path is assumed to have very low delay variability, corresponds to very high provisioned network, the delay is below 50 ms most of the time with 80 ms spikes occurs every 10 minutes, Fig. 5
V. Conclusion

In this paper, we have proposed a policy to be used with the current QoS Call Admission Control algorithms for admitting VoIP calls. The proposed policy uses the admission information obtained from the VoIP gateway on the wired network, and provides this information to the access point to be used as a policy in the call admission process in the wireless domain. We show that implementing the proposed policy improves the network utilization, and increases the number of successful VoIP sessions admitted to the access point polling list, thus increasing the number of successful VoIP calls conducted within certain time period. As a future work, we are looking toward studying the performance of the proposed policy with different Call Admission Control algorithms, and with different traffic conditions. Also we are investigating on how the QAP communicates efficiently with the softswitch to obtain the network link status of the destination networks.
Fig. 5. Delay characteristics patterns of the major Internet backbones used in the simulation (continued) (a) Backbones with a very low delay spikes corresponds to very high provisioned links (b) Backbone links with blocking pattern (c) Backbone links with high delay spikes with a periodic pattern.

Fig. 6. Performance evaluation of the proposed policy (a) The admission probability of the successful VoIP calls (b) The blocking probability of the failed VoIP calls (c) The utilization of the wireless network with and without implementing the proposed policy.

REFERENCES