Improving QoS by Reducing Authorization Request Messages from Unauthorized Devices in a WiMAX Network

Saeed Ullah, Choong Seon Hong

Department of Computer Engineering, College of Electronics and Information,
Kyung Hee University, South Korea
Email: saeed@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract

For WiMAX service providers, efficient resource allocation has a key role for providing better QoS. In a WiMAX network users put request to get network resources. The contention time is a short time period in which users send different requests to the base station. The subscribed users are barred to put request if unsubscribed users putt request in the contention time period repeatedly. One of such situation arises in authentication request from unsubscribed users to the base station. In this paper we provide a simple but very effective mechanism to restrict repeated authentication requests of unsubscribed users to the base station.

1. Introduction

Efficient resource allocation to the subscribers is the most important factor for providing better Quality of Service (QoS) in a WiMAX network [1]. To get the bandwidth and other resources from the network the device sends request to the Base Station (BS). Upon the request the BS allocates resources to the device according to its budget. In IEEE 802.16 standard [2] whenever a new Subscriber Station (SS) enters in WiMAX cell or an old SS is powered ON, it scans for the DL (Down Link) channel. After finding the suitable DL frequencies, SS communicates its basic capabilities with the BS. After it, SS sends an Authorization Request (Au-REQ) message to BS. BS validates the identity and authorization of SS. If BS finds the SS as authorized, it sends acknowledgement to SS otherwise it rejects the request. When authorization of an SS is rejected by the BS due to any reason (low balance or the SS has crossed its data limit), the SS continuously sends authorization request messages to BS; all these requests are sent in the contention period. The contention period is a very short period in which a very limited number of requests can be sent to the BS. Authorized SSs uses this contention time for different type of services requests like bandwidth requests etc.

In situations when the number of unauthorized SS is significant then legitimate users are unable to put resource request in the contention time due to continuous authorization request by these unauthorized users in the contention time period. This causes poor QoS by WiMAX network to its users. In this paper we propose a minor modification in the device authentication mechanism which reduces requests of these unauthorized SS. Our proposed modification shows significant improvement for providing QoS to the legitimate devices.

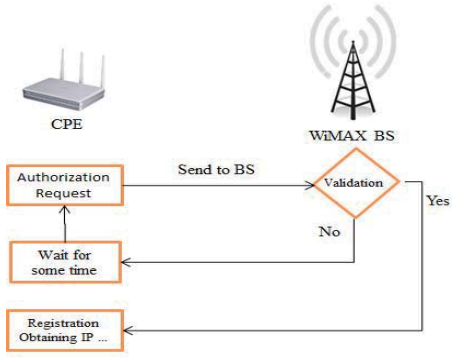

Figure 1: Au-REQ sending mechanism in existing WiMAX network.

2. Problem Formulation and Proposed Solution

Whenever a new SS enters in WiMAX cell or an existing SS is powered ON, it scans for the DL channel. After finding the suitable DL frequencies, SS synchronize with DL frame preambles. After it SS performs initial ranging to adjust its power level and timings. Then, SS sends a SBC-REQ message to inform the BS about its basic capabilities. As a response BS sends a SBC-RSP message to SS which indicates about the bandwidth allocation and PHY parameters for upcoming transmission [3]. After passing from all these steps, SS initiates the authentication process by sending an Au-REQ to BS. This message contains the manufacturer certificate X.509 of SS. After successfully completion the authentication process, SS sends an Au-REQ message to BS immediately [3], [4]. BS, upon receiving the Au-REQ message, validates the identity and authorization of SS. If BS finds the SS as authorized, it activates an AK (Authorization Key) for SS and sends it to SS after encrypting it with public key of SS. But if BS finds the

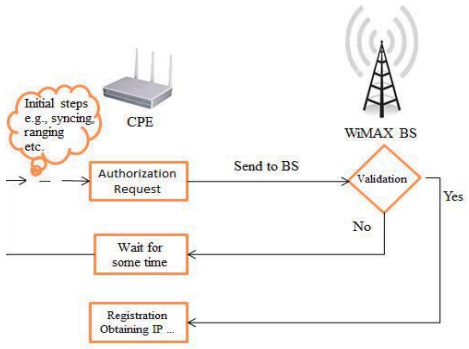

Figure 2: The proposed Au-REQ message sending mechanism.

SS as unauthorized then it rejects the request. Problem arises when an unauthorized SS is rejected by the BS; it continuously sends authorization request messages to BS; as shown in Figure 1. BS is likely to serve all these messages from both authorized and unauthorized users. Since a WiMAX BS can serve a limited number of users, thus it is more likely that the requests of legitimate SSs is to be rejected due to the unauthorized SSs in the cell. So the "Goodput" of the network becomes decrease.

Our proposed solution is to restrict the Au-REQ messages at CPE by the unauthorized users. It is done by sending a specific rejection code to the unauthorized CPE with the "Authorization Request" rejection. Upon receiving this code, CPE will go into restricted state where it is unable to send Au-REQ messages to BS. CPE will remain in this state until it reboots. In this way, unauthorized CPE will send no more Au-REQ messages to BS; this process is shown in Figure 2. A major advantage to stop the Au-REQ at CPE level is that the BS involvement will be reduced significantly.

After rebooting the CPE, it will take a start from the DL channel scan. Upon reaching at Au-REQ step, it will be allowed to send Au-REQ messages to BS. But after receiving the rejection code once, it will again go into restricted state. Thus in our proposed methodology, there will be very few Au-REQ messages from unauthorized SSs. Most of the times BS will deal messages from legitimate SS; hence it will increase the network "Goodput" significantly in case of larger number of unauthorized users. A CPE, which declared as unauthorized due to insufficient balance, will go in "restricted state" after receiving the specific rejection code. Meanwhile, if the user wants to recharge his/her account then, he/she must be needed to restart the device to enable it to communicate with the BS.

3. Performance Analysis

In the existing WiMAX network the probability of unauthorized SS success to access the channel is a typical example of binomial distribution which can be fine out using the formula given in equation 1. In Equation 1, n is the total number of nodes (authorized and unauthorized) contending to put request to the BS in the contention time period and k as

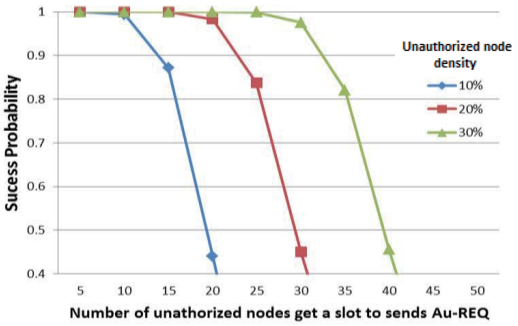

Figure 3: Unauthorized node density and it probability of network access

the number of unauthorized nodes. We have taken n = 100 and solved the equation for 3 different values of k with the

$$P_S k = \binom{n}{k} p^k (1-p)^{n-k} \qquad (1)$$

assumption that every node always has data to send to the BS. The results are shown in Figure 3.

Let suppose a BS can handle messages from 100 SSs in the contention time period then in the assumed scenario as much unauthorized SS get access to the network that much authorized SS are barred to get their message to the BS. In Figure 3 we see that as the unauthorized node density increases the blocking probability of the authorized nodes also increases.

4. Conclusion and Future Directions

In this paper we presented a mechanism for reducing Au-REQ messages from unauthorized SSs to the BS which helps in providing better quality of service. Extending analysis of the proposed mechanism and doing some simulation are very good future directions for research in this field.

Acknowledgement

This research was supported by the MKE(Th e Ministry of Knowledge Economy), Korea, under the ITRC(Information Tech. Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)" (NIPA-2012-(H0301-12-1004). Dr. CS Hong is corresponding author.

References

[1] K. Basu, S. Zeadally, and F. Siddiqui, "Quality of Service (QoS) in WiMAX", ISR journal of Technologies and Protocols for the Future of Internet Design, 2012.

[2] IEEE Std. 802.16-2009,"Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems",

[3] Matthias Hollick, Parag S. Mogre," Slow and Steady: Modelling and Performance Analysis of the Network Entry Process in IEEE 802.16", Fifteenth IEEE International Workshop on Quality of Service, 2007.

[4] Sasan Adibi, Bin Lin,"Authentication Authorization and Accounting (AAA) Schemes in WiMAX", IEEE International Conference of Electro/information Technology, 2006.