Pre-authentication and Selection of suitable target Base Station during Handover procedure in Mobile WiMAX Network

Ejaz Ahmed, Bob Askwith, Madjid Merabti
School of Computing and Mathematical Sciences, Liverpool John Moores University
Byrom Street, Liverpool L3 3AF, UK

Abstract— WiMAX (Worldwide Interoperability for Microwave Access) is an emerging technology that can provide wireless broadband access at the data rates of 70 Mbps over 50 kilometres to both home and business customers. WiMAX is cost effective and offers higher data rates than other wireless networks. It supports both fixed and mobile applications. WiMAX is easier to deploy as compared to other networks and has flexible network architectures. One of the major challenges concerning the performance of Mobile WiMAX is seamless handover. IEEE 802.16e standard for Mobile WiMAX defines two kind of soft handovers (MDHO and FBSS) and hard handover. But only hard handover mandatory in the standard and Mobile Station cannot transmit or receive data packets during this hard handover. Therefore this long interruption due to hard handover is awful for real-time applications. Re-authentication of Mobile Station and selection of suitable target Base Station are two time-consuming processes within handover procedure. We proposed Pre-authentication scheme in which standard EAP authentication is skipped if Mobile Station handovers from one Base Station to another within he same network so handover latency will be reduced significantly. The modified MOB_NBR-ADV message contains useful information e.g. list of neighbouring Base Stations and number of real-time connections each of these Base Stations have etc. which can be helpful to calculate suitability index for selection of target Base Station. In the end we evaluate our proposed scheme by simulation using NS-2. The results show that our proposed scheme is more efficient than traditional handover scheme.

Keywords- Mobile WiMAX, Re-authentication, Handover, EAP

I. INTRODUCTION

WiMAX (Worldwide Interoperability for Microwave Access) is a flexible, efficient, cost effective and offers high data rates and larger coverage than other wireless broadband technologies. It supports both fixed and mobile applications. WiMAX is easy to deploy than other networks and has flexible network architectures. It supports interoperability with other networks. It also provides the possibilities for higher integrated QoS (Quality of Service). So it will be helpful in bridging the digital divide [13]. WiMAX can operate in both licensed and non-licensed frequencies so in this way it provides regulated environment as well as offering opportunity for those wireless carriers who cannot economically afford licensed frequencies. Many experts believe that WiMAX is the technology of future [4, 14, 17, 18, 19].

WiMAX can be used in a wireless metropolitan area network (MAN) technology to connect different Wi-Fi hot spots to the Internet and can also be used as a wireless extension to cable and DSL for last-mile (last-kilometre) broadband access [14]. It provides the users NLoS connectivity over the 50 km linear range and up to 70 Mbps data rate, which is enough for providing broadband internet access to more than one thousands home users. IEEE 802.16 was first designed to provide the last mile for Wireless Metropolitan Area Network (WMAN) with line-of-sight (LOS) working at 10-66GHz bands. The later version, IEEE standard 802.16a, which enhances previous standards, also supports non-line-of-sight (NLOS) within 2-11GHz bands and mesh nodes. And the Mobile WiMAX or IEEE 802.16e is designed to provide mobility in Broadband Wireless Access [17, 18, 19].

Handover is an essential function for networks which support mobile subscribers i.e. Mobile WiMAX. User receiving mobile services expect handover completed very fast so they do not experience any service degrading. In Mobile WiMAX networks optimization of handover mechanism is one of the most important research areas. During the handover procedure data packets may be delayed and connections may be dropped. The main drawbacks of Mobile WiMAX handover mechanism includes wastage of channel resources, handover latencies and loss of data packets [4, 14, 16, 19].In IEEE 802.16e standard for Mobile WiMAX, three types of handover are supported Hard Handover (HHO), Fast BS Switching (FBSS), and Macro Diversity Handover (MDHO). In IEEE 802.16e standard for Mobile WiMAX only hard handover is mandatory so Mobile WiMAX cannot transmit or receive packets during handover. Handover latency should be not more than 50 ms in VoIP and should be not more than 100 ms in streaming media. Thus real-time packets can be dropped and it may result that service providers cannot guarantee quality of service during handover procedure. The long interruption of hard handover is horrible for real-time applications like IPTV, VoIP and Sat TV. In our proposed scheme we tried to solve this latency problem during handover.
The remainder of this paper is organized as follows. Section II provides technical background of overview of Handover Operation in Mobile WiMAX / IEEE 802.16e networks. In section III an overview of previous work on Handover Operation in Mobile WiMAX / IEEE 802.16e networks is presented. We have described our proposed improvements in handover procedure scheme in section IV. In section V, we present simulation results. Conclusion and future work are given in section VI.

II. BACKGROUND

A. Handover in Mobile WiMAX

Handover [2, 5] is an important function in Mobile WiMAX. In WiMAX Network Mobile Station (MS) has the ability to perform handover function to support its mobility. In Handover a Mobile Station (MS) switches from air-interface of one Base Station (BS) to air-interface of another Base Station (BS) without losing its current sessions and data. It is also important that when Mobile Station (MS) moves from one Base Station (BS) to another Base Station (BS) then there should be minimum delay in communication. Mobile Station (MS) performs handover due to different situations which include the following:

1. In case the strength of signal weakens because of movement of Mobile Station (MS) or level of interference then the Mobile Station (MS) performs handover to other Base Station (BS) which can provide better signal quality.
2. In case Mobile Station (MS) can get better quality of Service (QoS) at another Base Station (BS).

Hard Handover (HHO) is mandatory in IEEE 802.16e but other two techniques i.e. Micro Diversity handover (MDHO) and Fast BS Switching (FBSS) are optional. The last two are called Soft Handover techniques and these are able to provide more seamless and faster Handover (HO). The description of these handover types is given below [2, 5]. Handover Procedure in Mobile WiMAX is described in Fig. 2 [15]. In WiMAX the handover procedure is mainly comprised of two processes. The first one is Network Topology Acquisition and the second one is Handover (HO) operation.

1) Network Topology Acquisition

Mobile Station (MS) gathers information of its neighbouring Base Station’s including channel description and physical quality of channel by the Network Topology Acquisition. This process is performed before the Handover (HO).

Two processes are performed to gather information for acquisition of network topology and these are called Network Topology Advertisement process and the Scanning process. Other than these two processes a Mobile Station (MS) can also perform an Association Process. An Association process is an optional process and it is performed during Scanning Process. It is an initial ranging process to help Mobile Station (MS) to get information for selecting target Base Station (BS).

2) Basic Handover Operation

Handover operation is essential to support mobility in WiMAX and in this process an MS switches from air-interface of one BS to air-interface provided by another BS. The various stages during the Handover procedure are following.

i) Cell Reselection

The purpose of cell reselection is to find suitable target BS for Handover. In this process an MS performs scanning and/or Association with one or more BS to determine which of these is suitable for Handover as a target BS. The MS can use information in neighbour advertisement message (MOB_NBR_ADV) which is sent periodically by the BS to perform Cell Reselection. In this process the connection with serving BS is not broken.

The figure below describes the Cell Reselection and procedures performed during it operation.

![Cell Reselection Process](image)

Figure 1: Cell Selection with Ranging [2]

ii) Handover Decision and Initiation

The actual Handover begins with a decision for an MS to switch from serving BS to target BS. This decision can be made at the MS, the BS, or on the network. In MS initiated HO, MS transmits MOB_MSHO-REQ message. BS responds to the MOB_MSHO-REQ with the acknowledgement message MOB_BSHO-RSP. On the
other hand BS can also initiate handover by sending an unsolicited message MOB_BSHO-REQ. MS may suggest one or more possible target BS when it sends MOB_MSHO-REQ message. BS may suggest one or more possible target BS when it sends MOB_BSHO-REQ message.

The serving BS sends a handover indication message which contains information about MS to potential target BS(s) over the backbone network when serving BS receives the MOB_MSHO-REQ message, to notify that Mobile Station intends to handover. MS may predict potential target BS(s) through previously performed scanning and Association activity. Serving BS may predict potential target BS(s) by criteria based on several factors including expected MS performance at potential target BS and QoS requirement of Mobile Station. The serving BS sends MOB_BSHO-RSP in case of MS-initiated HO to inform the MS about selected target BS but in case of BS-initiated HO it sends MOB_BSHO-REQ for this purpose.

MS makes the final HO decision after receiving MOB_BSHO-RSP or MOB_BSHO-REQ message and sends MOB_HO-IND message to BS to notify its final decision. If BS receives MOB_HO-IND message with an option of serving BS release then BS sets a resource retain timer. MS is disconnected from its serving BS upon the expiry of resource retain timer.

iii) Handover Cancellation
MS may cancel handover at any time, regardless it was initiated by MS using message MOB_MSHO-REQ or BS by using message MOB_BSHO-REQ. MS cancels HO by transmitting MOB_HO-IND message with the HO cancel option. MS and serving BS will resume the normal communication if serving BS receives MOB_HO-IND message with the HO cancel option and resource retain timer is not yet expired.

iv) Use of Scanning and Association Results
Mobile Station may scan the neighbouring target Base Stations and optionally try association. If the serving BS has already sent HO notification to target BS then the target BS may place a fast ranging element Fast_Ranging_IE in UL-MAP to allocate non-contention-based Initial Ranging opportunity. Mobile Station may scan target Base Station for UP_MAP either a contention-based or non-contention-based MS Initial Ranging opportunity.

v) Termination with the Serving BS
The MS has to break its connection with serving BS if it decides to HO after receiving MOB_BSHO-RSP or MOB_BSHO-REQ. This process is completed by sending termination message MOB_HO-IND with option of serving BS release. When the serving BS receives this message it starts resource retain timer. This timer defines how much time the serving BS should retain all context of MS including MS connections and MAC state machine etc. On the expiry of resource retain timer the MS is disconnected from serving BS and all information serving BS have about MS will be released. But if target BS sends message through the backbone to serving BS with indication that MS is attached to it then serving BS removes MAC context and MAC data related to the MS irrespective of resource retain timer.

vi) Synchronization to Target Downlink
After HO is initiated, MS synchronizes with UP and DL transmission parameters of target BS. This procedure can be shortened if target BS has already sent MOB_NBR-ADV with the information about target BSID, physical frequency, DCD and UCD.

vii) Ranging
The MS starts ranging after synchronization with UP and DL parameters of target BS. The WiMAX uses two types of ranging, initial ranging and HO ranging. The purpose of ranging is time aligning before actual communications starts and to communicate properties of transmission link between MS and target BS. The target BS dedicates a common time interval to MS for initial ranging transmission. The MS gets information about this interval through MOB_BSHO-REQ or MOB_BS-RSP message. MS may receive Fast_Ranging_IE in the UL_MAP of target BS for non-contention-based initial ranging opportunity.

viii) Drops during Handover
This is a situation when MS has ceased communication with its serving BS before the completion of normal handover procedure. MS may detect this situation by its failure to demodulate the downlink, or by exceeding the limit of consecutive RNG-REQ retries. The BS may detect drop when the number of retries of inviting Ranging Request is exceeded the allowed limit. When the MS detects a drop while trying to establish connection with the target BS, it may attempt network re-entry with its preferred target BS through Cell Reselection procedure and it may try to resume communication by sending handover cancellation message.

ix) Network Entry/Re-entry
After the successful ranging process the MS starts network entry procedure with new BS. The procedure of network re-entry is similar to the network entry when MS initially switched on. If the Mobile Station has already sent RNG-REQ that includes serving BSID during the ranging process, then target BS may acquire information about from serving BS over the backbone to accelerate the network entry process. Now target BS may decide depending on the amount of the information to skip one or more phases among the following network entry procedures negotiation of basic capabilities, privacy key management, authentication phase, registration and traffic encryption key establishment phase.

III. RELATED WORK
Significant volume of research activities have been going on worldwide on Handover of IEEE 802.16e broadband wireless network for years and several schemes for pre-authentication and Selection of suitable
target Base Station had been proposed. In [8] new handover scheme was proposed that reduces scanning and ranging latency. It also eliminates the network re-entry latency through cross-layer in mobile WiMAX. This scheme uses layer 3 to transmit MAC control messages between Mobile Station and Base Station during handover to speed up layer 2 HO. Although this scheme reduces scanning and ranging latency; and eliminates of the network re-entry latency by using the cross-layer approach however it introduces synchronization latency. In [9], authors proposed an enhanced link-layer HO scheme called Passport Handover with a new Transport CID mapping strategy for real-time applications. With the help of this CID assignment strategy confliction of CIDs of handing over services with that of ongoing services in the target Base Station can be avoided. But this scheme can be complex when deployed.

In [10], the authors proposed two efficient schemes to enhance the performance of authentication during handover in Mobile WiMAX. The proposed schemes help to avoid the device re-authentication. In the first scheme, whenever Mobile Station first enters the network it is authenticated by AAA through EAP authentication. After that whenever Mobile Station needs to be authenticated by AAA server then instead of standard EAP method used in handover authentication, an efficient shared key-based EAP method is used. In the second scheme, the standard EAP method is skipped and the device authentication is done by SA-TEK three-way handshake in PKMv2 process. This scheme is not suitable for implementation because it avoids the standard procedures. In [11], the authors proposed a secure pre-authentication that follows the least privilege principle to solve the domino effect and handover protocol guarantees the backward and forward secrecy. But this pre-authentication scheme is not efficient and secure.

In this paper we propose some improvements for handover procedure in Mobile WiMAX. Our proposed solution will reduce the latency so handover will be seamless and user will experience no or minimum interruption in service. As compared to above mentioned schemes ours is more practical as it require only few changes in the standard.

IV. PROPOSED IMPROVEMENTS IN HANDOVER

A. Handover Management Module

We propose Handover Management Module which performs many functions to expedite handover procedure in Mobile WiMAX. It will reside on backhaul network and not on Mobile Station so reducing computational load from Mobile Station. Handover Module continuously monitors and communicates with all neighbouring Base Stations. Handover Management Module will calculate and store the following information about each of neighbouring Base Stations.

1. Free Bandwidth of each BS
2. Types of connections of each BS
3. Number of real-time connections a BS has.

Handover Management Module sends this information to serving Base Station which uses it to construct MOB_NBR-ADV message. This modified MOB_NBR-ADV will be helpful to select most suitable target Base Station and efficient handover procedure. The working of Handover Management Module is described in figure 2.

![Figure 2: Handover Management Module](image)

B. Pre-authentication Scheme

Whenever a Mobile Station enters in WiMAX network mutual authentication is performed between Mobile Station and network. Also if Mobile Station handovers from one Base Station to another then mutual authentication is required to be performed again. This mutual authentication is very time consuming process and results in delay in handover procedure. We propose an efficient re-authentication scheme which skips standard EAP methods so during the handover authentication will be very fast. When Mobile Station enters in the network for the first time the standard EAP authentication is performed as shown in figure 3.

After the EAP authentication both Authentication server and Mobile Station share the AK. Now whenever Mobile Station needs to handover to a different Base Station then Authentication Server and Mobile Station can calculate the new AK using equation given below.

\[
AK_{i+1} = \text{hash} (AK_i || nonce || \text{timestamp})
\]
Where hash(.) is a cryptographic one way hash function such as SHA-2 or MD5. Re-authentication is performed as shown in figure 4.

C. Calculation of most suitable BS

Now the question is how an MS can use the additional information efficiently. According to its requirement at the time of handover every MS checks the last MOB_NBR-ADV message and computes the suitability index. Suitability index can be computed as:

If MS needs a real time connection with target BS then:

Suitability index = (Available Bandwidth / (4 * Number of Real Time connections + Number of Non Real time connections))

In this case we set priority of real time connections four time higher then priority of non real time connections. The reason to set 4 time higher priority is to minimize the risk of selecting a target BS with higher number of Real Time connections.

If MS needs non real time connection with target BS then:

Suitability index = (Available Bandwidth / (2 * Number of Real Time connections + Number of Non Real time connections))

In case of non real time connections we keep the priority of real time connections two times higher then that of non real time. The reason of choosing two time higher priority is because user is not so much worry about of quality of service and user can compromise on a little delay. Therefore numbers of real time connections are not of so much importance for that user.

Now at the end suitability index of all the BSs is compared and the one with higher suitability index is selected as the next BS.

In this simulation scenario we created 20 Mobile Stations which are travelling through the coverage area of 6 Base Stations. The inter Base Station distance is 700 meters and neighbouring Base Stations have some overlap area. All six Base Stations are connected to same ASN-GW through wired connection and this ASN-GW connected to server. The assumed traffic was constant bit rate with data rate of 2 Mbit/s. Movement, direction and started position of Mobile Stations was set random. Time for simulation was 300 seconds and speed of different Mobile Stations varied from 1 to 100 km / h in order to consider both pedestrian and vehicular movements of Mobile Stations. The results of the simulations are shown in the figure 5.
The results show that although our proposed handover scheme does not offer much improvement to reduce handover latency as compared to traditional handover scheme if the number of handovers is less. But as the number of handovers increases, our proposed scheme reduces handover latency significantly as compared to traditional handover procedure.

VI. CONCLUSION AND FUTURE WORK

Issues related to handover are among the most important challenges faced by WiMAX technology. Mobile WiMAX has defined three types of handover; first one is called Hand Hardover (HO) and it is mandatory in standard. The other two Micro Diversity Handover (MDHO) and Fast Base Station Switching (FBSS) are soft handover and are optional in standard. The focus of our research is hard handover because only that is mandatory in the standard.

In this paper, we have proposed some improvements to optimize handover procedure in Mobile WiMAX which make this procedure more efficient. We proposed Handover Management Module which will reside in backhaul network so the load from Mobile Station will be reduced and handover procedure will be efficient. In our proposed approach minimum number of neighbouring Base Stations will be scanned. Mobile Station will only scan those Base Stations which can fulfill its bandwidth requirements. So handover latency will be reduced greatly. Priority should be given to real time flows in handover. Base Station broadcasts MOB_NBR-ADV management messages periodically in order to distribute information about its neighbouring Base Stations so Mobile Station does not have to gather information about each of neighbouring Base Stations. MOB_NBR-ADV should contain list of Base Stations and their quality level. Target Base Station which has largest remaining bandwidth and minimal use of real time flows will be classified first. Also our proposed scheme avoids frequent handovers so wastage of resources can be prevented.

Handover mechanism in Mobile WiMAX is a very challenging research area. There are many issues that should be investigated for designing universally accepted WiMAX handover management framework. Implementation and performance of our proposed Handover Management Module on actual WiMAX network is worth further study. In our research we were mostly restricted to Hard Handover and extending this work to other two handovers i.e. Micro Diversity Handover and Fast Base Station Switching can be worthy of investigation.

REFERENCES