World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:4, 2015

# Survey on Handover Security Issues in WiMAX Networks

R. Chithra, B. Kalaavathi, K. S. Aruna Shivani



***Abstract*—**Worldwide Interoperability for Microwave Access, is a broadband technology, which can effectively transmit a data across a group of users using Multicast and Broadcast Service. WiMAX belongs to a family of (IEEE 802.16) standards and is evolving as a fourth generation technology. WiMAX is the next generation technology that offers wireless access over long distances. MBS zone, which is a group of base stations that are broadcasting the same multicast packets which defines Multicast and Broadcast services. Handover is a process of transferring an ongoing call or data session from one channel connected to the core network to another channel. The handover causes authentication, delay, packet loss, jitter that mainly affects the communication. In this paper, we present a survey on handover security issues in WiMAX.

***Keywords*—**WiMAX, Handover, Multicast and Broadcast Security.

## I. Introduction

WiMAX is termed (World Wide Interoperability for Microwave Access) of fixed and mobile broadband wireless standards. The main objective of the WiMAX network is to support number of users enable broadband connection with each other [13]. WiMAX provides two wireless services such as non-line-of-sight and line-of-sight. The WiMAX networks enable the interoperability between the different products for fixed WiMAX, it provides a Broadband Wireless Access (BWA) with a network coverage of up to 50km and 5-15km [1] for mobile stations. In mobile WiMAX, it is crucial to change the Base Station (BS), then it has to set up new connection every time. Fixed WiMAX does not support handover, whereas in IEEE 802.16e it allows portability, simple mobility which is meant for specified separate handover mechanism [4], [28]. In IEEE 802.16e, the changes had been made in BS to MSS every time when the users move out of the transmission range. In fixed WiMAX there is no movement or replacement has been made to the subscriber, it is always a fixed one [33]. There are several improvements and advancement in the IEEE 802.16e standard and they are formally termed as Mobile WiMAX [7], [34]. As it is infrastructure less it has been used in military, civil deployment areas because it gives assurance not only to the deployed nodes, which are in communication, but also to the nodes which are not able to receive the GPS signal. To enhance the capacity, the WiMAX is feasible to replace the candidate for cellular phone technologies such as GSM and CDMA [14], [35].

The wireless communication protocols are prone to number of attacks due to radio transmission [16], [32] that mainly cause various damages to the networks. WiMAX has several security challenges they are confidentiality, integrity, authentication, encryption and availability. Confidentiality is an important factor in the WiMAX network, the information exchanging between the subscriber stations in view of the fact that has an adversary having the appropriate equipment may eavesdrop on the communication in which the third party are not easily retrieve the information. In insecure networks the there is a danger in exchanging the information that can be easily altered that results in integrity, since the lack of integrity would result in many problems. Integrity controls are used as a safe tool to keep the information without any altered manner in any unexpected way [15]. The authentication in the general case provides the principles in 802.16 networks that has to be certified with X.509, while using the X.509 certificates, an attacker to parody the identity of legitimate subscribers and survive the ample protection against the theft of service. In WiMAX authentication mechanism, Privacy Key Management (PKM) protocol that lack behind the base station (BS) or service provider authentication. This makes the WiMAX networks vulnerable to man-in-middle attacks, exposing subscribers to various confidentiality and availability attacks. Encryption in WiMAX supports the advanced encryption standard (AES) cipher; it's given that strong support for confidentiality of data traffic. The availability which deals with the deployments in the WiMAX networks, an attacker to use readily obtainable tools to jam the spectrum and it is logically simple.

There are numerous prospective attacks in WiMAX security; they are rouge base stations, DOS attacks and man-in-middle attacks [2]. At some point of time Denial of Service (DOS) occurs in the base station during the Privacy Key Management (PKMv2) authentication mechanism due to heavy public key computational load [16], [17]. Man-In-the-Middle attacks are possible during the SS for their basic capability negotiation [16], [18].

WiMAX network, which generally has an uplink and downlink signal. The uplink signal is, when a user sends a data from a subscriber device to a base station the base station broadcast the wireless signal into a channel which is called uplink and the base station transmit the same or another user is called downlink [13]. For wireless medium security support is

R. Chithra, Assistant Professor, is with the Department of Information Technology, K. S. Rangasamy College of Technology, Tamil Nadu, India; e-mail: chithra@ksrct.ac.in).

Dr. B. Kalaavathi, Professor, is with the Department of Computer Science and Engineering, K. S. R Institute For Engineering and Technology, Tamil Nadu, India.

K. S. Aruna Shivani, PG Scholar, is with the Department of Information Technology, Tamil Nadu, India (e-mail: arunasadhasshivam@gmail.com).

mandatory to communicate with the other networks [12]. WiMAX basically designed with the help of the IP core network, which deploy and amalgamate easily with the existing networks. The feature that supported by WiMAX networks are scalability, security, mobility, quality of service.

The WiMAX network, has three major components Mobile Station (MS), Access Service Network (ASN), Connectivity, Service Network (CSN) [5]. Mobile Station is mainly used as a source of network connection for end users [2]. ASN is composed of two or three base stations; it also contains an ASN gateway while CSN is responsible for providing an IP function.

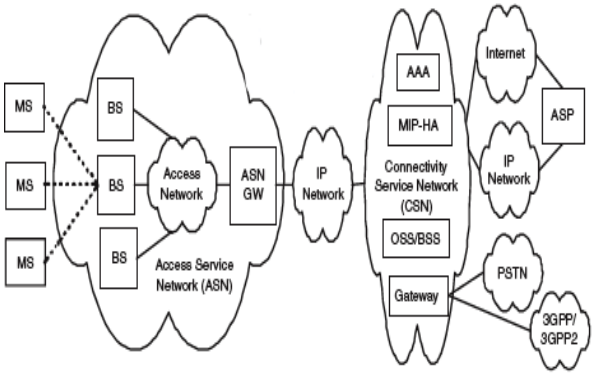


Fig. 1 Network Architecture [2]

A WiMAX architecture uses Internet Protocol (IP) which is enclosed/bounded in the ASN gateway that is connected to Service Network (SN) or CSN. ASN handles both micro and macro base stations, which afford access to the end users where CSN which provide authentication to the user devices (Mobile nodes, PC). It is also responsible for user security and Quality of Service (QOS). The IP address management is handled by CSN.IP core which is in the middle of CSN & ASN.CSN provides the connectivity to the internet and telecommunications while ASN communicates to the BS and the MS.

Handover management is one of the challenges in the mobile WiMAX, it deals with the transfer of a piece of user application's perspective from one base station to another base station [14], [37]. Handover causes delay and packet losses that affect the real time communication performance. The WiMAX supports handover, it allows MS to find the BS from the similar or dissimilar ASN and establish a connection in the absence of the network range. During the handover scheme, the MS transferred from the serving BS to target BS, and the time consumed for this method is referred as handover delay. To overcome the handover issues the multicast, broadcast service zone can be used. Broadcast services are described as all users within the broadcasting area can receive the information. The multicast services involve only the users that have subscribed to the service can receive the information [22], [36].

Fig. 2 has a mobile station, base station, gateway with authentication, authorization, and accounting server [22], [2]. The multicast, broadcast service controller (MBSC) which maintains several base stations that is adjacent to each other which help to construct the MBS zone. As the size of the zone increases, it reduces the handover delay [23].

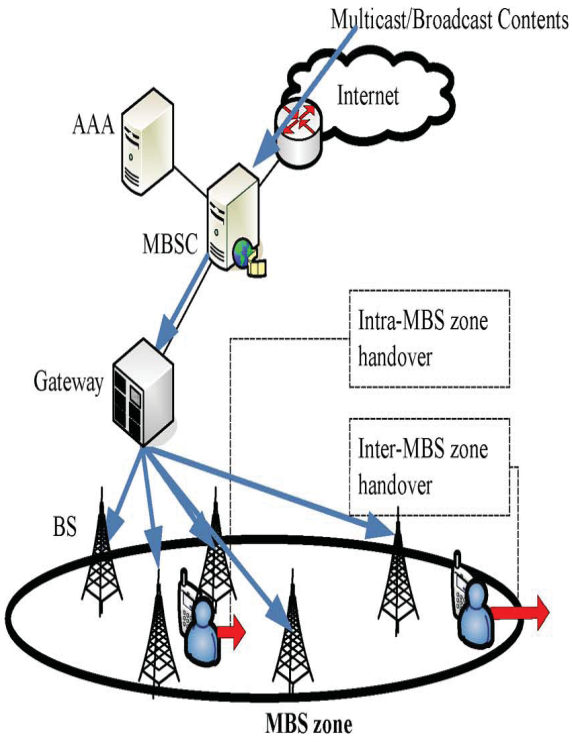


Fig. 2 Mobile WiMAX MBS zone [22]

## II. Handovers in WiMAX

In general, when a MS move from one BS to another BS it should employ a continuous connection. Handover classified either in the form of homogeneous or heterogeneous. Heterogeneous handover includes either movement between different types of access technology or movement across different administrative domains [20].

Mobile subscriber station moves from one coverage area to another base station in that case the handover is required to take place an action to transfer the bond between the current base station to another base station before the mobile subscriber station moves out of the range of the described base station, to avoid call termination. The packets in the base station are not delivered to the mobile station during the handover process is stated as service disruption [19].

In order to accommodate number of users to achieve the traffic handling capacity results in pooping the base station. Since the base station handover has to handle the transfer of the ongoing or upcoming calls to the adjacent base station with overlapping coverage area. In order to avoid interference in the case of handover of non-CDMA environment the different mobile subscriber station from different base station uses the same channel, but in different cells then the call is transferred to another channel in the same cell or other cell [1], [29].

The handover has been classified into two types, namely [3] Hard Handover and Soft Handover.

*A. Hard Handover*

In WiMAX, hard handover is mandatory. Hard handover follows the Break-Before-Make procedure. At a time, MS communicates only with one BS if it wants to communicate with one more BS, the old connection should be wrecked before the new connection recognized. The time required in hard handover is very small so that it is not perceptible to take place in a desired period, it can be achieved only with low speed. Hard handover has a high bandwidth efficient, fast, smooth and nearly glitch-free. For handling the voice centric applications with high-speed mobility, user's hard handover is not that much effective [21].

The hard handover in WiMAX network is classified into two types, namely Network Topology Acquisition Phase (NTAP) and Actual Handover Phase (AHOP) [21], [30].

In network topology acquisition phase, before the actual handover process takes place in action, the network topology acquisition phase follows the procedure that the mobile station and the serving base station, simultaneously collects the information with the help of the backhaul network about the underlying network topology. It has a mobile station, serving base station, target base station 1 and target base station 2. The various chores involved in this phase are listed in the network topology advertisement, scanning time slot allocation, downlink synchronization and association with potential target base station1, Downlink synchronization and association with potential target base station2.

In the network topology advertisement, the serving base station (SBS) collects the information about the neighboring base station (NBS) using the mobile neighbor advertisement message. In the scanning time slot allocation, a time frame allocation helps in scanning interval allocation request and response messages that have been sent by the mobile station and the serving base station after the response received from the serving base station sends a negotiates along with the potential target base stations.

In downlink synchronization and association with potential target base station, first the target base station sends the physical channel information to the mobile station. In this phase the ranging request and ranging response are exchanged between the TBS.

In downlink synchronization and Association with potential target base station 2 first the target base station2 sends the physical channel information to the mobile station. The mobile station sends a contention resolution and ranging request to the target base station 2. The target base station2 receives all the information and replies ranging response message to the mobile station.

In actual handover processes the mobile station changes its location from serving base station to the selected target base station. It has a several procedures such as handover decision and initialization, Target Base Station synchronization and ranging, network entry and reentry phase, network entry process optimization, authorization and registration [21], [31].

The process involved in handover decision and initialization are as follows, first the mobile station forwards the handover initialization request to the serving base station; after receiving the request from mobile station the SBS sends a pre-handover notification to the target base station 1 and target base station2 sends a response notification to the serving base station immediately.

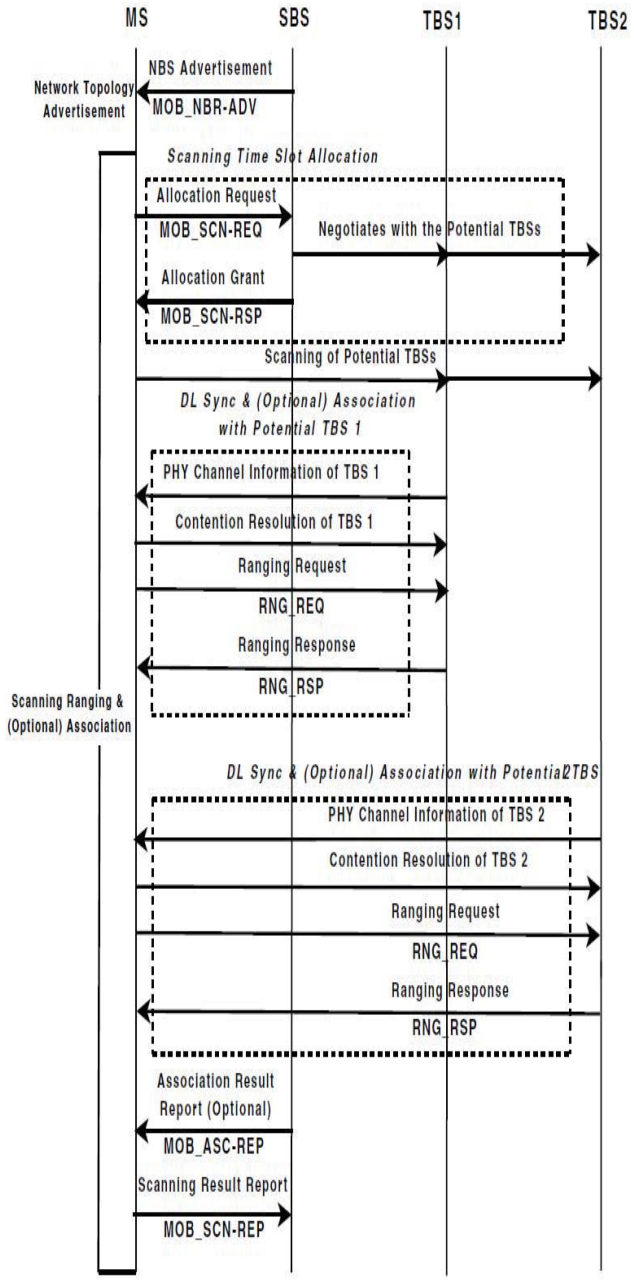


Fig. 3 NTAP message sequence charts [21]

The SBS quickly responds the serving base station initiation request to the mobile station. The mobile station forwards the indication message to the SBS, SBS confirms its message to the target base station. Once the initialization completed the connection terminated.

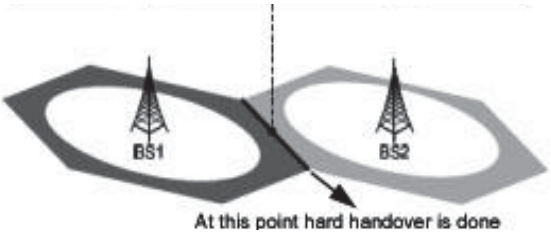


Fig. 4 Hard Handover [1]

In synchronization with the target base station the uplink and downlink parameters are used. The mobile station sends a contention resolution and ranging request to the target base station 1, after receiving the request the target base station 1 sends a ranging response to the mobile station.

In network entry and reentry phase, the TBS 1 would be serving base station (SBS) and target base station (TBS 2) acts as a backbone network in which it sends a request to the mobile station and gets a response from the backbone network.

The network optimization has several functionalities such as basic capabilities negotiation, MS authorization and authentication, context (TEX) exchanges, registration. In the authorization and registration phase, the mobile station marks the network re-entry optimization after then it gets functional aspects with the new serving base station [21].

Hard handover comprises of intracellular handover and intracellular handover. When the MSS moves from one BS to another BS, using the similar network it belongs to Intracellular handover. When the MSS moves from one BS to another BS, using the dissimilar network it belongs to Intercellular handover.

To reduce the handover delay in the multicast, broadcast service region the WiMAX network introduces an MBS zone in which the mobile station does not require to produce a new connection during handovers between the Base stations in the same MBS zone.

To achieve the best quality of service MBS Zone size has to be increased based upon the mobility level, every BS in the same MBS zone broadcasts the same MBS packets, in spite of being there, of a user in its coverage moreover, requesting a new MBS session can be blocked due to lack of available bandwidth [22].

The MBS handovers are of two types, namely they are intra-MBS-zone handovers and inter-MBS-zone handovers. Inter MBS-zone handover and inter MBS-zone handover has a several procedures to be followed that has been shown in Figs. 7 and 8.

Step 1: MAC layer performance should do first.

Step 2: When a MS migrates from one MBS zone to another it is necessary to have a new connection, and hence MBS joins request message should be transmitted.

Step 3: MBS authorization request sends and it is needed to get a response.

Step 4: Resource reservation should be done here.

Step 5: Secure Key Exchange.

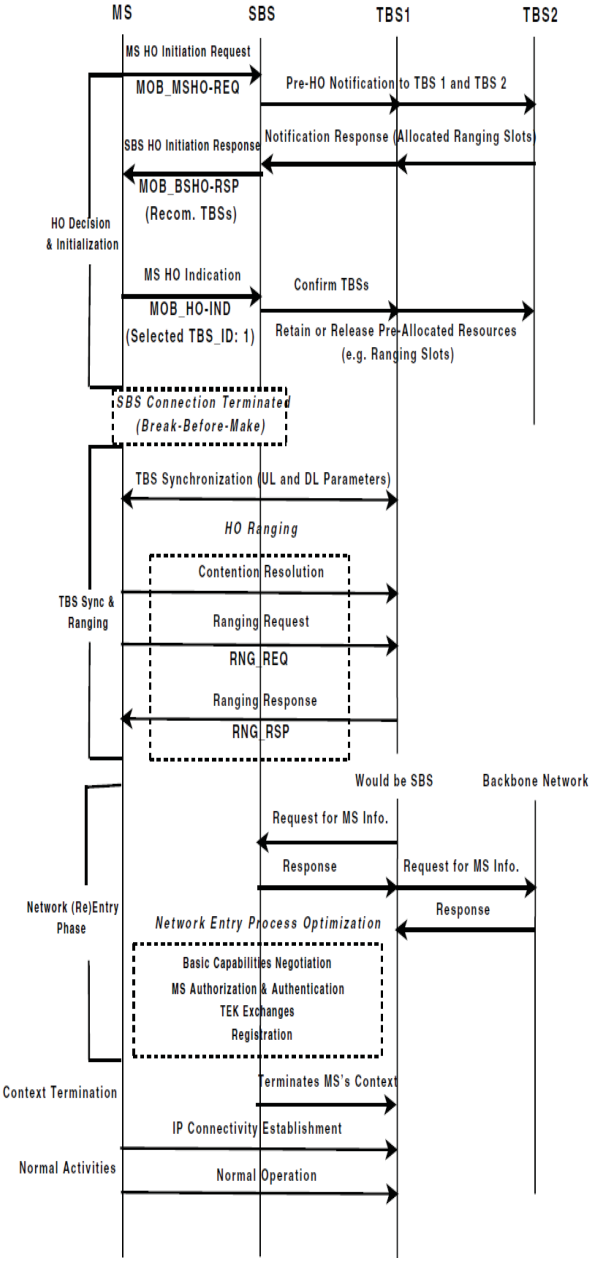


Fig. 5 AHOP message sequence chart [21]

Step 6: For inter MBS zone handover it is not necessary to have a multicast distribution tree update procedure because the target MBS zone, which contain the same user as that of the MBS session.

The same procedure has been followed by the intra MBS zone hand over the variation persist only if the mobile station navigates from one base to another station that is surrounded by the MBS zone without supplementary processing.

Usually the MBS zones are active and inactive. The zone, which contains the current users of the MBS session, is in active MBS zone; whereas those which do not have the current users are in inactive MBS Zone [22].

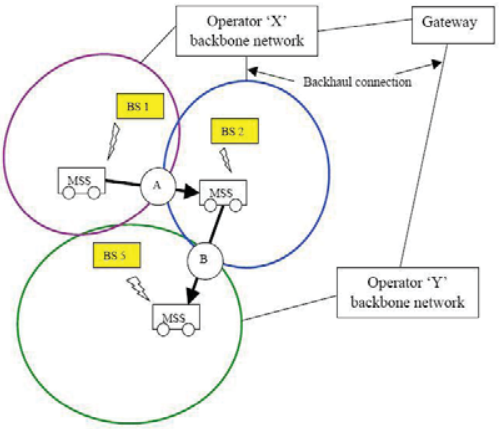


Fig. 6 Intracellular and Intercellular Handover [1]

*B. Soft Handover*

In soft handover the MS is able to communicate with more than one BS. Soft handover is used to avoid or reduce the "near-far" effect on Code Division Multiplexing networks.

The time required in soft handover is very large so that it perceptible to take place in a desired period, it can be achieved with high speed, mobility single mobile subscriber station uses several channels for the single call. Hence the overall capacity of the network is decreased as single node to involve in more than one channel which in turn cannot be made available for other MS's for new call the call rates are costlier as more than one channel is occupied for single call [1]. It generally comprises of Macro Diversity Handover (MDHO) and Fast Base Station Switching (FBSS).

The diverse set plays a major role in MDHO [3] which requires a file/register of BS's which are involved in the handover procedure, it also defines each MS's in the network. The active base station holds the all information about the mobile subscriber station including the MAC context. The serving base station is the base station where the mobile station has recently been handed over or registered with it.

The neighboring base station is not a part of diversity set and there is no traffic exchanged between the base station and the signal strength measurement with the base station only evaluated by the mobile station [1]. The main motivation of the MDHO is to reduce the handover delay and save resources. It provides a better performance with deference to multi-access interference, flexibility and coverage [21]. There exist an uplink and downlink MDHO.

When MS transmission is acknowledged by multiple BS's where selection diversity of the acknowledged information is performed it belongs to an uplink MDHO correspondingly when multiple BS's transmit data to MS, the diversity combining can be performed at the MS as it says about the downlink MDHO.

FBSS: The diverse set of all BS's which sends signals to the MS, among all these BS's, MSS selects only one BS for swapping /switch over uplink or downlink data. This is known as anchor BS.

In WiMAX network the shared nature of the medium resulting in the absence of the physical protection that makes the data transmission vulnerable to eavesdropping attacks [3].

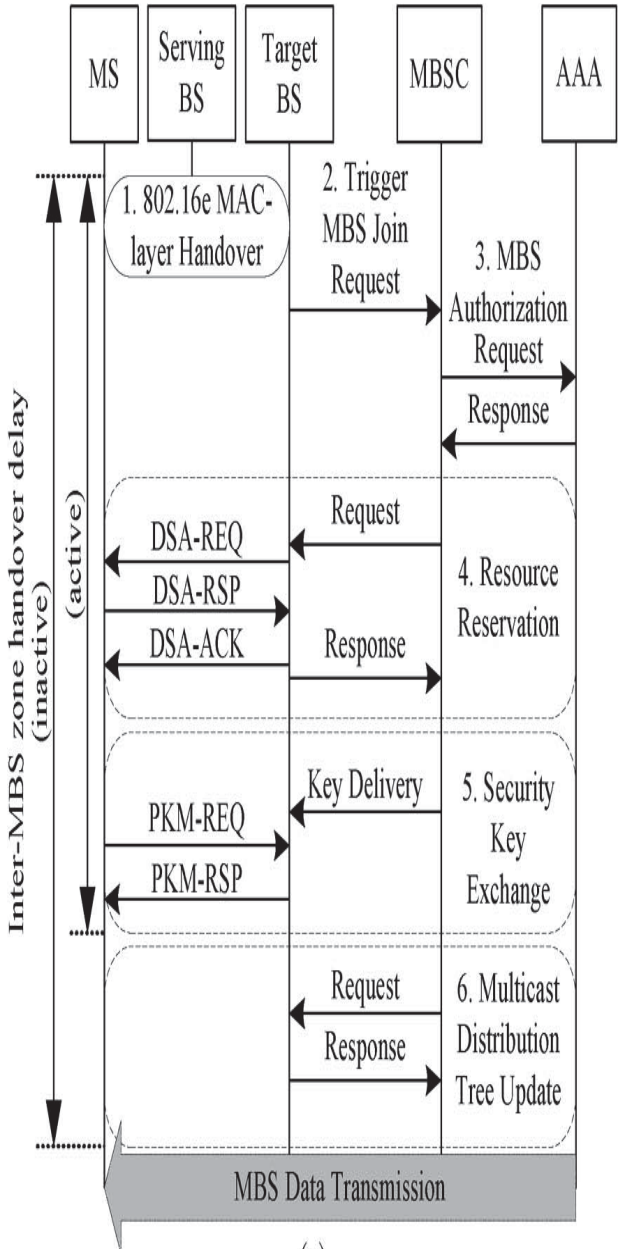


Fig. 7 Inter-MBS-zone handover [22]

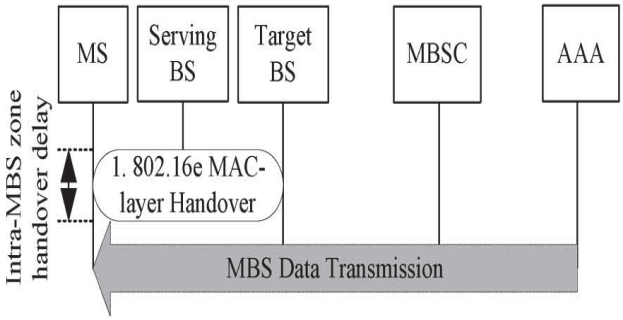


Fig. 8 Intra-MBS-zone handover [22]

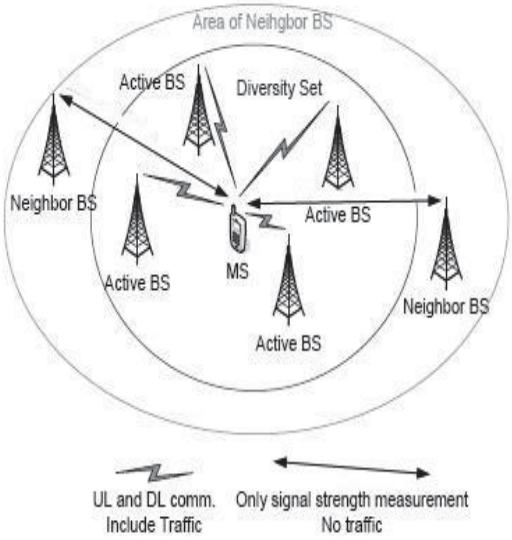


Fig. 9 MDHO [1]

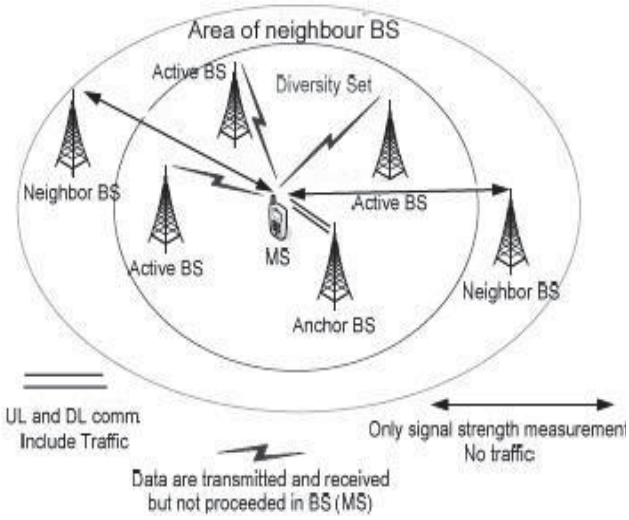


Fig. 10 FBSS [1]

The essential information during the handover authentication process can be compromised by the malicious nodes. The security issues under various handover scenarios are discussed in the following section.

## III. Necessities of Handover Mechanism

The handover mechanisms are of two types they are dynamic and non-dynamic.

The dynamic requirements are received signal strength (RSS), velocity, throughput, user preferences, handover latency, and network load balancing. The non-dynamic requirements are network cost, power consumption, network security and bandwidth.

- Bandwidth: The quality of service (QOS) in the wireless environment is achieved without any faultless handover technique it should have a bandwidth. Link capacity in the network is determined as bandwidth [25].

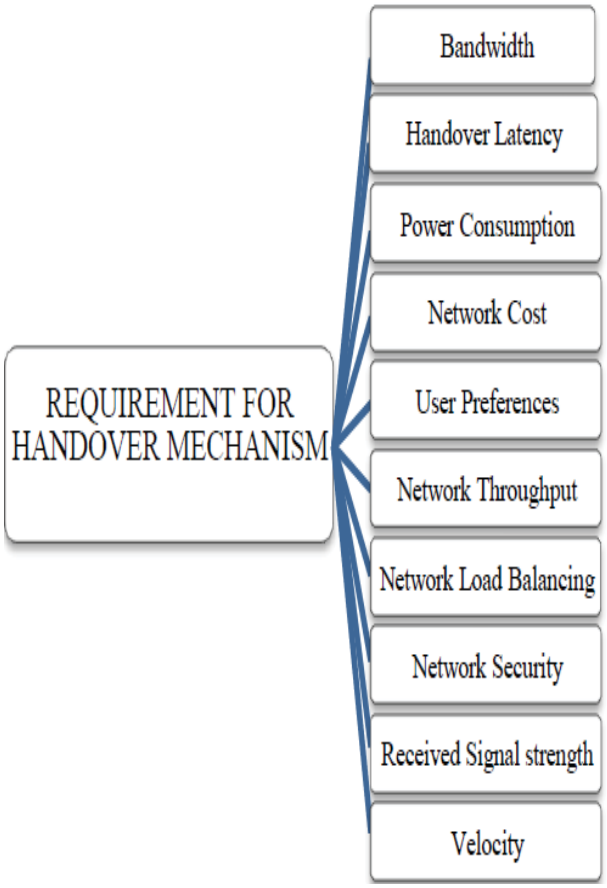


Fig. 11 Necessities of a handover mechanism [25]

- Handoff latency: The time takes place between the two base stations during the process of handover is known as handover latency.
- Power consumption: The power consumption takes place during the mobile station that switches from one station to another.
- Network cost: It determines the call arrival rate and handover call arrival rates by using the cost function.
- User preferences: It deals about the preferred networks, user application requirement, service types etc. [25].
- Network throughput: It describes about the average data rate of a specific communication link. It is measured in the form of bits per second (bps).
- Network load balancing: To avoid the worsening in the quality of service, network load balancing is used.
- Network security: It helps in monitoring the unauthorized access, abuse, modification and network accessible resources and prevents from them.
- Received signal strength: The wireless network depends on the signal strength and helps in defining the total amount of network bandwidth obtained from the connection [25].
- Velocity: In which it says during the handover process it is necessary to check the velocity of the host [25].

## IV. Security Issues in WiMAX

The security flaws in the mobile WiMAX networks are due to the management messages in WiMAX which are not secured, easily vulnerable to security problems. It becomes more difficult to use a common key to protect the message from the forged third party. There exist a several unauthenticated messages they are

Traffic Indication message (MOB_TRF-IND): The main motivation of these messages is used by the base station to alert the sleeping mobile station that there is traffic persists. When a mobile station receives a message, it first checks with every mobile station in the group, whether it addressed with the traffic indication bitmap [24]. Once the bitmap is set, the MS wakes up and receives the traffic, and the remaining mobile stations are in the sleep state.

Neighbor advertisement message (MOB_NBR-ADV): In this session the neighbor base station gets the characteristics of the serving base station message and the mobile station looking for handover possibilities. When a third party forges the messages the adversary has a capability to keep back all the individual base stations by omitting the information. In this way wrong data about neighbor base stations are distributed [24].

Fast power control message (FPC): This message is mainly used to send a message from the base station to n number of mobile stations to fiddle with their transmitting power. From this message, it is easy to abuse the transmitting power that is within the reachable mobile stations to a minimum count, so we cannot recognize the base station. The message with the maximum transmitting power is forwarded to all mobile stations that lead to the stress the batteries [24].

- Multicast assignment request message (MSC-REQ): In this method once a message is sent to the base station, it removes the mobile station from the multicast polling group. A primary connection establishment is available between the base station and mobile station that determines itself when a mobile station receives a delete message [24], the MS itself removes from the polling group and sends an acknowledgement to the base station. Polling group defines that it receives a bandwidth from the base station via polling mechanism.
- Downlink burst profile change request message (DBPC-REQ): To make a mobile station more robust and effective, a base station sends this (DBPC-REQ) message. The objective in abuse of this message is to temporarily break the connection between the mobile station and a base station by altering the mobile station's burst profile it is not probable for the mobile station to demodulate the data received from the base station. One more flaw residing in it is power control mode, the change response (PMC_RSP) message is sent from the base station. From this technique an adversary can easily adjust the transmission power and change the power control mode of the mobile station which is in communication [24].
- Association result report (ASC-REP): In this method, it has criteria that the base station does not need to answer to the ranging request. It can send the ongoing response to the serving base station of the requested mobile station. The association report message is prepared by collecting the ranging responses from the neighboring base stations [24].
- Ranging request (RAN-REQ): It is being of a digest message when an authentication key (AK) is available. In many cases authentication key (AK) persist and protects the initial network entry (INE) basically INE does not have an authentication key [24].

*Unencrypted Management Communication*

The message exchange in the network entry process is unencrypted [24]. Here the initial network entry management message is encrypted. An adversary team creates a detailed profile about the mobile station, including the capabilities of devices, security settings, and associations with base stations [24].

*Shared Keys in Multicast and Broadcast Service*

In this scheme secured encryption of data transfer to the mobile station is difficult. It has a group traffic-encryption key (GTEK) updates command message that is used to encrypt the public key [24].

*Initial Network Entry Vulnerabilities*

In this state it performs several processes they are initial ranging process, the subscriber station basic capability (SBC) negotiation process, PKM authentication process and registration.

- Initial network entry: To establish a connection to the mobile WiMAX networks, many parameters are transmitted between the subscriber station (SS) and the base station [10].
- SBC negotiation process: In this phase the PKM security contexts do not have the ability to keep the information confidential.
- PKM authentication process: It is mainly not to control message during the initial network entry, the security implies only to the normal data traffic after initial network entry.

*Access Network Vulnerabilities*

In which it has a subscriber station (SS), base station, Access service network/gateway (ASN/GW), Authentication-Authorization- Accounting (AAA) [10].

- SS: Subscriber station might be the mobile devices that has an idea to join with the mobile WIMAX network.
- ASN: In which it's a set of network function devices, it mainly consists of at least one base station and one ASN gateway [10].
- AAA: It's mainly to make the data secured without any abuse in the exchange of information.

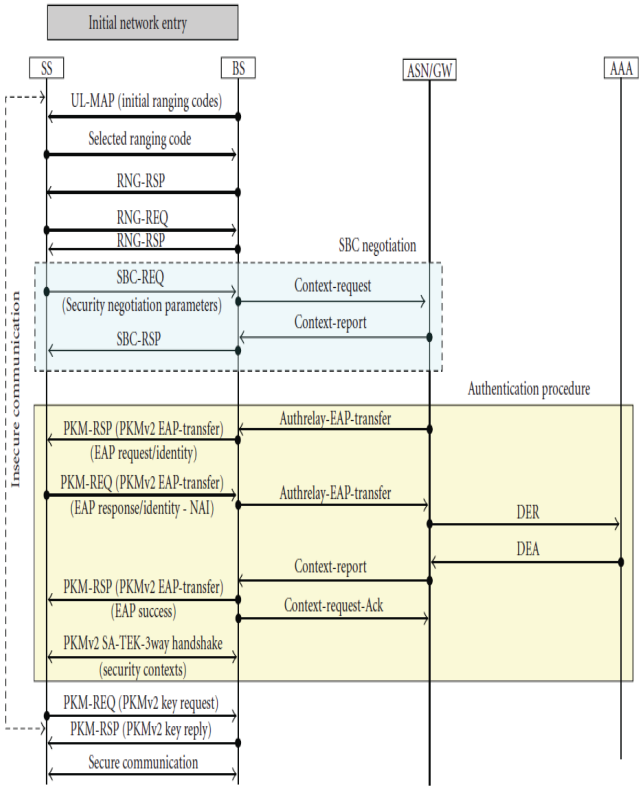


Fig. 12 Initial network entry vulnerabilities [10]

## V. Security Issues in Horizontal Handover

Horizontal handovers are homogeneous intra-network inter-cellular [14]. Hand over that occurs between the two base stations in the same system are known as horizontal handover. To maintain the service continuity horizontal handover involves a terminal device to change the cells within the same type of network [26], [25]. Horizontal handover is broadly classified into two types they are link-layer handover and intra-system handover. The Link-layer handover is flanked by two base stations beneath the same foreign agent (FA) is recognized as a link-layer handover. In intra-system handover of mobile station from one foreign agent to another controlled by different base station [25].

Handover results in service disruption as the mobile moves from serving BS to target BS. The authentication of mobile nodes in target BS is susceptible to denial of service attack and replay attack.

Denial of Service Attack in Handover: The lack of freshness indication and a proof, the NBL (neighbor list) message sent by the HSN (home Access Service Network) to a MS generally offers a security hole for DOS attack. It is antagonistic to forge its own NBL message [6]. To restart the pre-authentication process and create a PREAUTH_REQ message is sent to the hASN (Home Access Service Network).

By validating the certificates in the CA, before the MS interpret with fake NBL.

The forged NBL messages which drains the resource and energy without working for justifiable applications. There exist a number of fake ASNs incorporated in NBL will cause serious effects on MS normal activities [6].

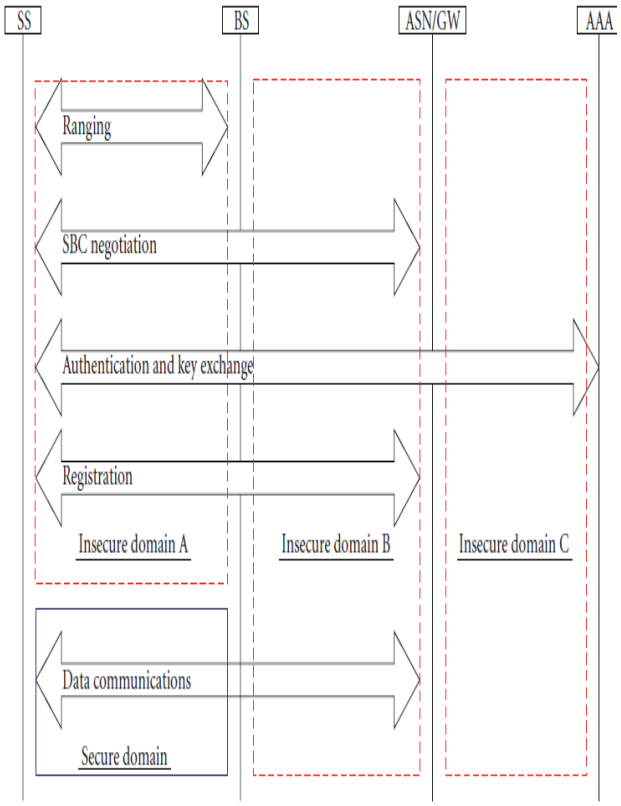


Fig. 13 Access network security [10]

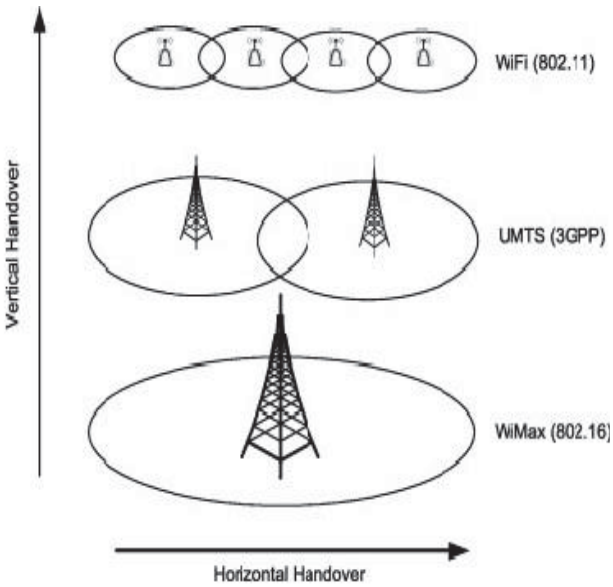


Fig. 14 Horizontal and Vertical handover [25]

The pre authentication process consuming resources not only for MS but also for hBS, hASN and nASNs is progress frequently.

Replay Attacks: When pre-authentication based handover is used in WiMAX network, the PREAUTH_REQ messages can be eavesdropped by malicious users. Since this message does

not have a freshness indicator, these messages can replay later to the home access service network [6]. Thus the normal functionality of ASN is affected. Similarly, in PREAUTH_RSP message send by the ASN can be eavesdropped by the malicious user for later usage.

TABLE I
PERFORMANCE ANALYSIS OF HANDOVER AUTHENTICATION SCHEME

| | | IEEE 802.16e Hard Handover | IEEE 80.16 e Soft Handover | Secured Hard Handover [9] | Secured Soft Handover [9] | Hur's Approach [11] | ROSMEX [10] |
|---|---|---|---|---|---|---|---|
| Communication cost | Preauthentication | 0 | m (MSK distribution), m (PMK distribution) | m (PMK distribution) | m (TEK distribution) m (3-way handshake) | High (depends on EAP protocols) | Low 1time encryption/ decryption |
| | Reauthentication | EAP authentication, 3-way handshake | 0 | 3-way handshake | 0 | | |
| Computation cost | MS | PMK,AK | PMK,AK | m×PMK, m×AK | m×PMK, m×AK | High (depends on the number of Handover) | None |
| | BS | PMK,AK | PMK,AK | AK | AK | | |
| | AS | - | - | m×PMK | m×PMK | | |
| Forward/Backward Secrecy | | YES | NO | YES | NO | NO | YES |

## VI. SECURITY ISSUES IN VERTICAL HANDOVER

Vertical handovers are heterogeneous inter-network inter-cellular [14]. The heterogeneous network has an execution and decision process.

Decision processes will decide when the handover process has to take place between the mobile nodes and the networks. After the decision process, the execution process is carried out.

Vertical handover is defined as an involuntary fall over from one technology to another in order to maintain the communication [26].

The vertical handover is mainly composed of three phases they are system discovery phase, vertical handover decision phase, vertical handover execution phase.

### *System Discovery Phase*

In this phase the decision is made by the mobile terminal that determines which network has to be used. The network supports data rates and quality of service (QOS) parameters [26].

### *Vertical Handover Decision Phase*

In this phase the mobile terminal needs to determine whether the correlation should continue using the current network or switched to another network. This network has a parameter like minimum bandwidth, delay [26].

### *Vertical Handover Execution Phase*

In this method the correlation in the mobile terminal is re-routed from the access network to the new network in a faultless manner. This method has an authentication, authorization, and exchange of the user context [27].

The authentication of mobile nodes in target BS is susceptible to denial of forward and backward secrecy, Man in Middle attack and replay attack.

Forward and Backward Secrecy: A fresh Key (kn) must be shared by MS and AP/BS for communicating in a session. The fresh key is not possible to decrypt the information [8], by BS and (n+1) mobile station are termed as forward secrecy. If the decryption is done before allocation of BS (n-1) is termed as backward secrecy.

Man in the Middle Attack: During the handover, intruder act as a middle man between the MS and BS/AP. The mutual authentication between user equipment and network is mandatory [14] where it can insert or modify the message between parties such as BS, ASN, and MS. The proposed handover protocol does not possess the right Temporary CK (TCK) and Cipher based message Authentication Key (CK) or Pairwise Transient Key (PTK) [8].

The TCK and CK/PTK is responsible for the intruder to make a masquerade by MS or BS/AP.

Replay Attack: During the handover, the message flow is recorded by the attacker and it broadcast the old access request to trick BS/AP for phony substantiation [8]. Each message in Handover (HO) authentication messages are new and unpredictable as it contains a random number. In which all the messages are protected by a calculated Cipher based Message Authentication Code (CMAC) or Message Integrity Code (MIC) value [8]

## VII. CONCLUSION

Seamless handover management is an important requirement for communication technologies. The purpose of the IEEE 802.16e handover procedures has several handover flaws. In this survey hand over the security issue in WiMAX is analyzed. These issues can be considered to provide a secure handover in WiMAX networks.

## REFERENCES

[1] Chandan Gupta, "Comparative Study of Various Handover Scenarios in WiMAX Network," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 1, Issue 2, August 2012.
[2] http://www.WiMAXForum.org/
[3] Zdenek Becvar, Jan Zelenka, "Handovers in the Mobile WiMAX"
[4] Daan Pareit, Bart Lannoo, Ingrid Moerman, "The History of WiMAX: A Complete Survey of the Evolution in Certification and Standardization

for IEEE 802.16 and WiMAX," *IEEE Communications Surveys and Tutorials*, Vol.14, No.4,2012.

[5] Bo Li, Hong Kong, "Survey On Mobile WiMAX," *IEEE Communication Magazine*, December 2012.

[6] Thuy Ngoc Nguyen and Maode Ma, "Enhanced EAP-Based Pre-Authentication for Fast and Secure Inter-ASN Handovers in Mobile WiMAX Networks," *IEEE Transactions On Wireless Communications*, Vol. 11, No. 6, June 2012.

[7] Ali Al Shidhani, "Fast and Secure Reauthentications for 3GPP Subscribers during WiMAX-WLAN Handovers," *IEEE Transactions On Dependable and Secure Computing,* Vol. 8, No. 5, September/ October 2011.

[8] Anmin Fu, Gongxuan Zhang, Zhenchao Zhu, Yuqing Zhang, "Fast and Secure Handover Authentication Scheme Based on Ticket for WiMAX and WiFi Heterogeneous Networks," *Springer*, July 2014.

[9] Junbeom Hur, Hyeongseop Shim, Pyung Kim, Hyunsoo Yoon, Nah-Oak Song, "Security Considerations for Handover Schemes in Mobile WiMAX Networks," *IEEE Communications Society*,2008.

[10] Taeshik Shon, Bonhyun Koo, Jong Hyuk Park, and Hangbae Chang, "Novel Approaches to Enhance Mobile WiMAX Security, "*Research article in proceedings of EURASIP Journal on Wireless Communications and Networking*, Volume 2010.

[11] J. Hur, H. Shim, P. Kim, H. Yoon, and N.-O. Song, "Security considerations for handover schemes in mobile WiMAX networks," *in Proceedings of IEEE Wireless Communications and Networking Conference (WCNC '08)*, pp. 2531–2536, Las Vegas, Nev, USA, March-April 2008.

[12] Bhaskar Ashoka, David Eyers and Zhiyi Huang, "Handover Delay in Mobile WiMAX: A Simulation Study," *International Conference on Parallel and Distributed Computing, Applications and Technologies IEEE,* 2011.

[13] Shabbir Ahmed, "Performance Analysis of Mobile WiMAX Technology," *International Conference on Computing for Sustainable Global Development*, 2014.

[14] Sandeep Singh Sengar, Neeraj Tyagi, and Akhilendra Pratap Singh, "A Survey on WiMAX-3G Interworking," *IEEE* 2011.

[15] Kejie Lu, Yi Qian and Hsiao-Hwa Chen, "A Secure and Service-Oriented Network Control Framework for WiMAX Networks," *IEEE Communication Magazine*, May 2007.

[16] Jeremy Brown, Xiaojiang Du, "Towards Efficient and Secure Rekeying for IEEE 802.16e WiMAX Networks," *IEEE Communications Society*, 2009.

[17] L. Maccari, M. Paoli, and R. Fantacci, "Security analysis of IEEE 802.16," *IEEE International Conference on*, 2007, pp.1160 – 1165.

[18] T. Han, N. Zhang, K. Liu, B. Tang, and Y. Liu, "Analysis of mobile WiMAX security: Vulnerabilities and solutions," *IEEE International Conference on*, 2008, pp.828 – 833.

[19] Ji Hoon Lee, Taekyoung Kwon, and Yanghee Choi, "Location Management Area (LMA)-based MBS Handover in Mobile WiMAX Systems"

[20] Ashutosh Dutta, David Famolari and Subir Das, "Media-Independent Pre-Authentication Supporting Secure Interdomain Handover Optimization," *IEEE Wireless Communication*, April 2008.

[21] Sayan Kumar Ray, Krzysztof Pawlikowski and Harsha Sirisena, "Handover in Mobile WiMAX Networks: The State of Art and Research Issues," *IEEE communications surveys and tutorials*, Vol. 12, No. 3, 2010.

[22] Ji Hoon Lee, Sangheon Pack and Taekyoung Kwon, "Reducing Handover Delay by Location Management in Mobile WiMAX Multicast and Broadcast Services," *IEEE Transactions on vehicular technology,* Vol. 60, No. 2, 2011

[23] A. Dutta, J. Chennikara, W. Chen, O. Altintas, and H. Schulzrinne, "Multicasting streaming media to mobile users," *IEEE communication magazine*, Vol. 41, No. 10, pp. 81–89, 2003.

[24] Frank, A Ibikunle, "Security Issues in Mobile WiMAX (IEEE 802.16e)," *IEEE Mobile WiMAX Symposium*, 2009.

[25] Ravichandra M, Kiran Gowda H N, Udaya Kumar C A, "A Survey on Handovers Literature for Next Generation Wireless Networks," *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, Issue 12, December 2013.

[26] Abdoul-Aziz Issaka Hassane, Li Renfa, and Zeng Fanzi, "Handover Decision Based on User Preferences in Heterogeneous Wireless Networks," *College of Information Science and Engineering, Hunan University*, China 2012.

[27] B. R. Chandavarkar, G. Ram Mohan Reddy, "Survey Paper:Mobility Management in Heterogeneous Wireless Networks," *Department of Information Technology National Institute of Technology*, Karnataka, Surathkal, Mangalore, 2011.

[28] A. Bacioccola, C. Cicconetti, C. Eklund, L. Lenzini, Z. Li, and E. Mingozzi, "IEEE 802.16: History, status and future trends," *Computer Communications*, Vol. 33, No. 2, pp. 113–123, 2010.

[29] Jamshed Hasan, "Security Issues of IEEE 802.16 (WiMAX)" *Proceedings of 4th Australian Information Security Management Conference*, Edith Cowan University, Perth, Western Australia, 5th December, 2006.

[30] R. Q. Hu et al, "On the Evolution of Handoff Management and Network Architecture in WiMAX," *In Proc. IEEE Mobile WiMAX Symposium*, No. 144-149, March 2007.

[31] S. Cho et al, "Hard Handoff Scheme Exploiting Uplink and Downlink Signals in IEEE 802.16e Systems," *In Proc. IEEE Vehicular Technology Conference (VTC)*, Vol. 3, pp. 1236-1240, Spring 2006.

[32] B. Li, Y. Qin, C. P. Low, and C. L. Gwee, "A Survey on Mobile WiMAX," *in IEEE Communication Magazine*, Vol. 45, No. 12, pp. 70–75, Dec. 2007.

[33] Ioannis Papapanagiotou, Dimitris Toumpakaris, Jungwon Lee, "A Survey on Next Generation Mobile WiMAX Networks: Objectives, Features and Technical Challenges," *IEEE Communications Surveys & Tutorials*, Vol. 11, No. 4, Fourth Quarter 2009.

[34] B. Li, Y. Qin, C. P. Low, and C. L. Gwee, "A Survey on Mobile WiMAX," *in IEEE Communication Magazine*, Vol. 45, No. 12, pp. 70–75, Dec. 2007.

[35] K. Etemad, "Overview of Mobile WiMAX Technology and Evolution," *in IEEE Communication Magazine*, Vol. 46, No. 10, pp. 31–40, Oct. 2008.

[36] A. Dutta, J. Chennikara, W. Chen, O. Altintas, and H. Schulzrinne, "Multicasting streaming media to mobile users*," IEEE Communication Magazine*, Vol. 41, No. 10, pp. 81–89, Oct. 2003.

[37] A. M. Taha, A. T. Abdel-Hamid, and S. Tahar, "Formal analysis of the handover schemes in mobile WiMAX networks," *IFIP International Conference on Wireless and Optical Communications Networks*, 2009.