The authors of [26] proposed that there were various perils to certainty of WiMAX. Perils were linked to both the layers that is Physical Layer and Multiple Access Layer. Serious perils were spying of management messages, personating of Mobile Station or Base Station, jamming. Perils were enlisted and graded on the basis to the level of risk they impose. Preventive measures were needed to be followed. A spying detection system approach was suggested to check the perils.

The authors of [27] proposed that cooperation and relaying had appeared a vital topic in wireless communication. The proposed scheme authenticated Subscriber Station and Relay Station at network entry. Multihop relay network was embryonic to attain high capability services in large cell coverage area. Thus relay based WiMAX was used because it had lower infrastructure cost and high data speed. Nonetheless it was vulnerable to various kinds of attacks. If the number of devices or Hop increased, vulnerability increased. The proposed scheme used forward relays with localized authentication. New scheme maintained better security of the network. Performance evaluation showed the network security improved significantly.

The authors of [28] proposed that in order to minimize packet loss and handover delay the two tier mobility management was defined by the WiMAX Forum. But the question arises was: When to execute ASN gateway relocation? To answer this question algorithm was introduced (GRAC) which incorporated Admission Control (AC) and Wiener Process based on prediction algorithm. The algorithm improved the performance in terms of blocking probability, mean serving rate, mean signalling overhead, dropping probability.

The authors of [29] proposed a new call Admission Control algorithm. It rejected new requests scarcely and it provided good quality of service for in progress connections and new connection. CAC algorithm used momentary accept policy at the system then
performance of system was evaluated and then decision to reject or accept the request was made. The new CAC algorithm performed better with respect to other CAC algorithms. Authors simulated the algorithm with MATLAB tools.

The authors of [30] proposed that the adaptive Bandwidth issuance and Connection Admission Control (CAC) mechanism. CAC mechanism was based on game theory in WiMAX Networks. Non cooperative two person general sum game was articulated, where the participants were the Base Station and New Connection. The game articulation provided three decisions first accepting a new connection, second rejecting a new connection, third amount of Bandwidth issued to new connection. Delay and throughput outputs were examined by a queuing model contemplating Adaptive modulation and coding in Physical layer. Payoffs for Base Station and Mobile Station are optimized by using this queuing model used for Bandwidth issuance. Nash equilibrium was used to acquire candidate strategies and decision of the game was based on stance of admissible strategy duo. By using extensive simulation the Bandwidth allocation and admission control algorithm was estimated. The proposed scheme had efficiently maintained the QoS performance at the needed level.

The authors of [31] proposed that WiMAX had three classes of connections 1) connections with high priority 2) connections with medium priority 3) connections with low priority. Shadow server approximation technique was used to solve the problem of mixed priority strategy. The authors of this paper presented a single cell WiMAX network, where there was a Base Station and subscriber. The sub-channels were provided to the subscriber by the Base Station. Multiple connections at the subscriber Station share the sub-channels issued to a subscriber station. At a subscriber station two Connection Admission Control (CAC) mechanism, threshold based and queue aware CAC schemes were contemplated to ensure the quality of service. Connection level and packet level output were studied and compared with their analogues. The connection arrival was modeled by Poission process. Queue Aware method and threshold based method were contemplated. Threshold based CAC connection fixed the number of outgoing connections. The queue aware CAC mechanism contemplated the number of packets in the queue for the admission control judgment of a new connection. Since channel quality enhanced packet level performance also enhanced.
The authors of [32] proposed that among MMR Mobile Multihop Relay networks guarding security was the important goal to achieve. To make network more secure Private Key Management was proposed. Although, this protocol was not that much efficient in guarding the network and was vulnerable to replay attacks, Man In middle attacks and other Medium Access Control layer attacks. This article proposed a better version PKM protocol named as SEAKS (Self Organized Efficient Authentication and Key Management Scheme) protocol which made network more secure in end to end data transmission. SEAKS used distributed hop by hop authentication and localized key management scheme. SEAKS provided hybrid authentication scheme with localized re-authentication and key maintenance SEAKS prevented most of the vulnerabilities. SEAKS PKMv1 and PKMv2 were two modified PKM protocols which were responsible for authenticate each other. SEAKS overall in all aspects improved the levels of security and it could be applied to any MMR network.

The authors of [33] first compared the Wifi and WiMAX. After comparison WiMAX network was developed. Secondly authors did analysis of vulnerabilities related to Wifi and WiMAX. Wifi was more vulnerable as compared to WiMAX. Two important issues were discussed, first was the implementation of EAP mechanism. All EAP applications mentioned mandatory algorithms to assure security and mutual authentication. Latter issue was to ensure soft handover. According to WiMAX forum initial products had high energy consumption and high latency. The 802.16e implemented mobile VoIP, full mobility. It was a vulnerable network. Security guidelines for the network were described that formed a safe environment for the users.

The authors of [34] proposed that for long distance access WiMAX was the reliable technology. To control different traffic loads CAC was deployed. Proposed framework of 2 D CAC is to nest various features of WiMAX network. 2 D downlink and uplink were decomposed into two 1 – D CAC. An effective and equality constrained optimal revenue policy was developed to resolve the optimization problem. Expectations of both the service providers and subscribers had to be taken care of for a efficient WiMAX network. Simulation results proved that the proposed WiMAX CAC approach fulfilled the needs of both subscribers as well as service providers.
Privacy Key Management protocol is utilized to secure the connections in WiMAX Network. This protocol plays a perfect role to protect data during communication from Base station to User’s Station.

The authors of [35] used scyther tool to test the security for PKM v2. The authors also proposed a model of secured protocol (SPKM) and prevent authorization protocol from hacking virus. As per results found by the author that verified formally the key management protocol in provisions of secure session, distribution and key establishment and also maintain integrity, authenticity, confidentiality and access control.

The authors of [36] have suggested various improvements in the existing model. They made use of two way authentication between subscriber station and base station to make WiMAX more efficient and also to eradicate the Rogue base station attack. A further enhancement which has been done in the paper is the use of time stamp which will remove the DOS attack. To improve the capabilities and encryption time they had introduced some improvement in the model for security purpose. Also the comparison of ECC and RSA has been done here which reveals the goodness of ECC over RCA because of the smaller key size. At last, they have compared the proposed model with reference to the existing model performing several attacks. They carried out simulation by NS-2.

A special concentration or focus for security developments is required in IEEE 802.16 standard. The authors of [37] summarizes many of the vulnerabilities involved in infrastructure and WiMAX distribution and the security solution necessary to deal with them. This paper have an inclination on general description of many dangers associated with the infrastructure and IEEE 802.16 deployment and the security solution required to control them. To better understand the security in WiMAX, the beneficence of this research overview helps the researchers a lot. Although WiMAX technology has multiplex verification and authorization techniques, but the very well encryption techniques are still in danger from various threats or attacks. Being a new technology, we wish that in the coming time, these will become lesser and gets resolved. At last they concluded that there will be and there are no. of ways to study problems for modern technologies until this communication will be secured hundred percent.

The authors of [38] have considered various WiMAX security methods for encryption, authentication and availability. The WiMAX network must suggest or provide equivalent security in order to take part in with the existing broadband cable or DSL services.
Security is very important and must be directed for a broadband wireless standard such as WiMAX. This is to assure the wide acceptance both from the view of the end users and the service providers. We have learned from the past that Wi-Fi deployment has provided WiMAX an opportunity in allowing a safer wireless networks. The preventive measures that were taken with WiMAX were not done for wi-fi because at that time threats or attacks were mysterious, so proper preventive measures were not taken at Wi-Fi’s launch. Now that the attacks and dangers are known widely and recognized, so they have been forwarded before the WiMAX’s deployment. There are chances of the new threats being unknown and will therefore not be directed till WiMAX is launched. WiMAX do not have many possibilities. WiMAX will enable customers a fully wire independent network connection at their homes/business. WiMAX will also contribute superior services for mobile devices. These are also little contemplation for WiMAX to be used to support games. Also they have discussed the possible dangers or threats to the security of WiMAX. This paper will also examine how and why these threats play a main role in the versatility and flexibility of WiMAX.

The authors of[39] proposed an Enhanced EAP- based pre-authentication (EEP) scheme to get rid of attacks with very less requirements of communication resources and on computation. In order to solve the problem and to enhance the efficiency, we have given the EEP scheme. Also we have the MS to exchange key, material with the AS which will distribute key to the tSAN where the handover is assured. This is done to decrease the no. of cryptography functions and pre-authentication latency. HMAC has been employed in the first message. Now we have tested the security functionality of both schemes, EPA and EEP using SPIN and conducted comparison among both. It is seen that EEP scheme can’t only detect and avoid the DoS and the reply attacks. But the main advantage is that it can decrease the amount of pre-authentication delay and the power needed. The EEP scheme could reduce the handover delay which was large bottleneck of handover process given by the IEEE 802.26e. Authors concluded that their proposed scheme is both efficient and secure and is very capable to replace the current handover scheme.

Authors of [40] made an analysis of performance of WiMAX Security Algorithm which they proposed. As compared to other networking technologies wireless network is insecure, because of evolution of new technologies. Therefore, many security measures are taken to secure a wireless network. To protect the wireless network from malicious threats and unauthorized access the WiMAX groups has designed some security
mechanisms. To protect the network and its resources from unauthorized access an authentication and authorization model is used. Authors also propose threats related to MAC layer and physical layer of WiMAX and also intend few improvements to existing model which will enhance the performance of encryption algorithm. Their paper also intends some techniques to improve existing model capability and functionality. By using Qualnet4.5 simulation tool simulation is performed and in last results is provided.

For mobile WiMAX networks the authors of [41] gives an efficient group based handover authentication scheme. The main context of their scheme was that during the MS handover authentication phase, all the handover group member's security contexts are transmitted to target BS. The service BS will transmits all handover group member security content to target BS when the handover group's first Mobile Station (MS) moves from service Base Station (BS) to target BS. The Extensible Authentication Protocol (EAP) can be bypassed by rest of MSs in the same handover group and the handover latency is reduced by security content transfer phases to perform handover authentication directly. Therefore, to perform direct handover and authentication EAP authentication and SCT phases can be bypassed by the rest of MSs in same handover group. For high security performance and to minimize the handover latency the proposed scheme is very proficient as compared to existing schemes.

Authors of [42] proposes EAP-based wireless networks proxy ring signature based handover authentication method with location privacy preservation. Firstly, proxy ring signature scheme is integrated from an efficient ring signature and a proxy signature, which allows authentication of Mobile Node (MN) due to inherent anonymity of proxy ring signature without enlightening its location privacies and identity. Secondly, for low-power mobile devices in wireless network point multiplication operations on resource-constraints MN is required by our scheme. Lastly, to validate performance of proposed scheme they give an extensive simulation. The results show that in terms of communication overhead and on computation their scheme is relatively efficient.

The authors of [43] propose implementation of analysis of authentication protocols with description of threats in WiMAX. The limitations of existing architecture and security sub-layer are also described in this paper. The possible attacks in authorization and authentication are identified and dealt with passage of time. Various serious deficiencies are reported in PKM v1, while some are found in PKM v2. A number of shortcomings of
PKM v2 protocol are discussed in this paper. BWA is a developing field and mobility integration, it provide secure access to network with introduction to complexities. They give priority to network security by combining some methods to fill up the noticeable holes in authentication framework. During the work in progress to neutralize the posed security threats, it is better to infer with more issues as BWA users and its deployments increase at an expected rate. They intend that their proposed approach will improve and strengthen the network security by resynchronization of Base Station and Subscriber station.

To increase the reliability and to make WiMAX network safer from various threats the vital requirement is security. The authors of [44] surveyed the various security threats that may happen to Mobile WiMAX network and they surveyed regarding their solution also. Now a days as we know the emerging wireless internet technology is none other than IEEE 802.16 based WiMAX. There are many salient features of WiMAX which are as follows-it provides high speed internet over long distances. The layers in WiMAX are associated with some threats. The possible solutions of these threats were present in this survey paper.

The authors of [45] proposed that security of broadband wireless access becomes more complicated when wireless device were added. Threats were graded according to their level of risk they offered. This paper reflected the recent work related to IEEE and WiMAX forum. The threats were divided into five groups: 1) fabrication attack 2) modification attack 3) repudiation attack 4) interception attack 5) repudiation attack. One major threat was jamming that was used by attackers to obstruct the services. By using spreading technique this attack could be prevented. Another attack could be data modification where attackers manipulate the data. Digital signatures were provided to avoid these attacks. Then different wireless protocol and their architecture were introduced.

The authors of [46] proposed that security support was mandatory for all networks. Since WiMAX is a wireless technology and reachable to all which make hackers to access the network easily. So security solution for the WiMAX was provided. Solution was for both point-to-multipoint and mesh network. The integrated solution for point to multipoint is composed of D-H key agreement for secured initial network entry. For avoiding latency
and pre authentication issue during handoff, MIP scheme was proposed. To check encryption load issue data forwarding was employed.

In paper [47] authors first proposed the overview of security architecture of WiMAX network. They found out that the initial network procedure was not secure enough and the attacks were possible. DoS attacks were not prevented by resource saving and handover procedure. For the solution authors proposed SINEP (Secure Initial Network Entry Protocol) that was based on Diffie-Hellman (DH) key exchange protocol. These network protocols enhanced the security level. Authors modified the DH key exchange protocol to make it suitable for the mobile WiMAX networks. It was concluded that SINEP could prevent the DoS attacks toward mobile WiMAX networks and could abolish the probability of the man-in-the-middle attacks.

The authors of [48] proposed that Security was a major topic in telecommunications. Wireless systems were more vulnerable as compared to wire-line systems. The main objective was to provide security solutions for the WiMAX network. In paper [48], authors had introduced the requirements and principles of security in WiMAX networks. Then authors presented the data link security sublayer functions as defined by WiMAX forum. Finally, the Network Aspects of Security and Mobile WiMAX Network Architecture were discussed. IEEE 802.16e-2005 standard had accepted the lessons learnt and had specified a whole set of solutions.

Authors of [49] proposed that for fixed and mobile access the WiMAX IEEE 802.16e was a technology supporting broadband wireless communications. WiMAX supported handover and roaming facility, it also provided high throughput broadband connections. WiMAX had a security sub layer that maintained authentication and secure key exchange. Mobile WiMAX showed vulnerabilities while adopting improved security architecture. Several versions of 802.16 networks were developed. This paper focused on minimizing the security vulnerabilities in the protocol PKM and the initiation of traffic encryption keys (TEKs). They proposed the utilization of 1) Device certificate for key exchange process to maintain secure authentication 2) A formal evaluation of the PKM protocol (authorization phase and exchange of TEKs phase) and 3) Gave a formal evaluation of their new PKM protocol (authorization phase and exchange of TEKs phase). A specialized model checker Scyther was used for the formal evaluation which utilizes proofs of the security protocol.
The authors of [50] proposed that security was highly important in wireless networks since these networks were more prone to attacks. Thus authorization protocol was evaluated. Probable attacks were replay and suppress replay attacks. A mechanism was introduced to check these attacks. Methodology described WiMAX architecture, PKM protocol, drawbacks and necessary solutions. Attacks were prevented by timestamp and nonce together. PKMv1 and PKMv2 were compared and it was concluded that PKMv2 provided better security. Drawbacks of PKMv1 were improved in PKMv2. This version 2 of PKM protocol was secured for real time environment. By utilizing nonce and timestamp various attacks were prevented. Most probable attacks were checked but numerous more to occur when WiMAX implemented and tested in real time environment.

The authors of [51] proposed that in WiMAX network, the handover must be done quickly. They have proposed strategies to minimize the handover time. They modelled the WiMAX coverage area and proved that there were strategies which minimize the time required for handover. They proposed two new strategies to minimize the number of frequencies to check while finding a downlink from base station and provided various simulation results. MRU performed best when tested in along path or random locations. Another strategy was introduced to improve the neighbourhood messages, here MS recalls the history of handovers undergone and this data was used to choose the BS best for handover connection. This strategy had improved the performance of the WiMAX network.

The authors of [52] proposed that WiMAX was more efficient as compared to other wireless technologies. From commercial side, its feasibility depended upon revenue it generated and the quality of service it provided to the subscribers. This article explained two management mechanisms, first adaptive power allocation and call admission control. How to allocate the limited power was emphasized by APA and how to allocate a subscriber’s access bandwidth was decided by CAC. APA and CAC worked simultaneously. To efficiently deploy WiMAX system it had to meet the demands of subscribers as well as service providers. WiMAX was OFDMA TDD based network to satisfy the demand of subscribers and service providers.

The authors of [53] proposed that researchers were paying more attention to the issue of good quality of service. The paper dealt with the methods of admission control. There
were two groups of AC methods: measurement based and parameter based. The authors did the simulation of AC methods. Simulations were focused on required bandwidth. Different methods and algorithms to admission control, used to allocate Bandwidth for data flows were discussed in paper. Simulations made it clear that increase in number of samples increase the memory as well as time. It also increases the bandwidth required. MBACs, MBACf, MBACv algorithms were simulated in the paper.

The authors of [54] proposed that WiMAX was the high speed emerging technology that was useful for high data rate real time applications like banking, video screening etc. WiMAX provided last mile access. It had two layers 1) Physical Layer 2) MAC layer. WiMAX network was accessible to all this made it vulnerable to attacks. Authors analyzed the risk caused by attacks. The authors analyzed that some attacks could not be made in standard network and some could be made but could not harm the network.

Using Omnet++ Simulator the authors of [55] conducted an investigation of certificate based and identity based cryptography in WiMAX network. It is applicable for various purposes like infrastructural and end-client usage. WiMAX is said to be sufficient to handle wide range of usage scenarios because it is a large framework of networks and high end technology. Different mode addresses many security problems, modes, final security standard of WiMAX key management version2 (PKMv2) and privacy policies. Potential benefits are there in identity based cryptography by which enhancement to the overall security and security standard can be provided efficiently. WiMAX is used for acquiring services like video streaming on demand, mobile bank transactions and voice over internet protocol connections. It can also be used for data relaying purposes among access points by service providers. An enhancement was proposed which has combined identity of users with public key and hence eliminated the distribution load of public key from the network. Though IBC has few limits like requirement of a safe and secure the medium for distribution of private keys. To overcome these disadvantages, IBC is combined with certificate-based security.

The authors of [56] presented a security scheme in which a continuously moving target is represented by network security that has to be attained to ensure the required level of confidentiality, availability and services of network and integrity of system. Here definition of security plan is very imperative thing for setting up a new (WiMAX) network, after working on it point-to-point covering all the steps.
Broadband internet is implementation and access to high-speed internet which is major challenge of this century. For this, new standards for wireless access called IEEE 802.16 have been developed by IEEE. Considering the fact and assumptions, the standard does not specify a scheduling algorithm[57] and on the basis Latency-Rate (LR) server theory, the characteristics of system specified by the system standard a new scheduler with a call admission control has been presented by the authors of [57] which specifies standards of system by using the Wireless MANOFDM. The time frame (TF) is calculated by proposed scheduler so as to capitalize on the number of allocated stations in system and required delay for each user is managed meanwhile. Simulations investigated properties of this proposal in theoretically. It has been shown by the results that for a large range of network loads, it is possible to achieve an upper bound delay with optimization of bandwidth.

The growing significance of IEEE standard 802.16 is going to contend with new technologies like UMTS. Accepting this technology & its services depend on security. The authors of [58] deal with basic security features of WiMAX & WiMAX security architecture with its most important elements has summarized here. WiMAX is defenceless in two phases: key exchange phase and authentication phase which is depicted by security analysis. It also deals with some of its limits, potentials attacks counter measurements.

Mobility and Security architectures for subscribers that work along secluded wireless networks have been defined by the authors of [59]. Some key issues such as mobility management and security management are not addressed properly because of mobility of users and networks. Due to infrastructural unavailability for handling of authentications, Cellular network provides ideal solutions and services in isolated areas but the bandwidth, communication cost and availability of different services is limited by cellular networks. Due to this reason, WLAN (IEEE 802.11) in a mesh configuration with WiMAX has been integrated to offer various services. Thus a centralized system has been proposed for processing authentications and management of mobility in network that provides services to users and networks as well. For mesh and slave modes, a master node acts as a gateway here in this proposed architecture. A server called AAA acts as an authenticity barrier and accounting server for mesh nodes and slave nodes are interconnected to WLAN and WLAN is used by users as an access network. To access
the services in networks, the network is authenticated by using one time password method of EAP by the user. In this paper, mobility management in architecture has been proposed by us where along the different access networks, user ROMs, in a proper manner. Evaluation of architecture has been done by using a test bed. Also, calculations of architecture time and re-authentications during roaming have been done. At user level delay is there and mobile nodes comprise various networks.

In wired as well as wireless communication, a major concern is provided by security to restrict the communication. Security for Network Layer is more essential in current scenario and effect of misbehaving node has been analyzed and simulated by the authors of [60]. In this scheme MAC protocols are not respected by node and its packets are sent without any restriction as no protocol is followed by it. The performance comparison analysis with and without misbehaviour node was also investigated by the authors using OPNET. A packets flowing to authorize node can be destroyed by unauthorized clients present in the network. Misbehaviour Node attack (Network Layer), in that no protocol is followed by node and Constant Bit Rate (CBR) packets are transmitted continuously which alters the performance of network and also introduces noise.

In the upcoming generation wireless networks are dominant with the integration of various wireless access networks. By heterogeneous wireless network (HWN), it is possible to integrate various wireless networks to a common network. Intelligent and Complex Radio Resource management (RRM) techniques are required by HWN by which synchronization between various radio access technologies are enabled. Common RRM mechanism is a new Joint Admission Control (JAC) through which handover procedure requests in the HWN is handled. Handover signalling on the wireless backbone is reduced by vertical handoff scheme and also low handover delay to mobile nodes is provided. The important issue in this hybrid network is unlined handovers. A vertical handoff scheme between 802.11 and 802.16 is proposed and interworking architecture of wireless mesh backbone is presented by the authors of [61].

A significant role is played to Quality of Service (QoS) in wireless networks with a resource allocation function by Connection Admission Control (CAC). To admit new incoming connections, fuzzy sets and fuzzy logic theory is used by CAC mechanism for OFDMA-based WiMAX networks to achieve bandwidth efficiency with less computation
complexity and connection requirements. To decide whether a new incoming connection either to accept or reject, an algorithm is proposed by the authors of [62] that eliminates traffic load, available bandwidth and incoming connection required bandwidth. The incoming connections blocking probability is investigated using MATLAB simulated with the fuzzy logic-based CAC system. In the blocking probability for both UGS and non-UGS services as compared to Fuzzy Logic Based Admission Control Method in Wireless Networks (FLACWN), the results of simulation show improvement. And also proves that WiCACFL performs well in terms of blocking probability as number of connections increased.

An access to the Internet and other Application Service networks is provided by a CSN which contains a mobility anchor and an authentication server. Methods for CSN connected mobility for handoff across access networks and across Base Stations within an access network as well are defined by WiMAX. An alternate to CSN connected mobility using CMIP or PMIP through anchoring mobility at Correspondent Node rather than within CSN is defined by the authors of [63]. Securing connections to the Correspondent Node anchor provisions are also considered by the authors.

Authors of [64] proposed an admission control algorithm based on bandwidth. With different requirements of Quality of Services and varying bandwidth is supported by different multimedia Services in wireless communication medium as its main objective. In order to perk up the performance of network is the role of WiMAX network resource management. changing the Anchor Point (AP) of Mobile station (MS) from one GW of an ASN to another GW of different ASN which is not affected on Traffic’s Link Layer (LL) handover is included in Gateway (GW) relocation of Access Service Network (ASN). GW relocation from one ASN to other ASN to be performed is not specified as per existing standards defined by IEEE 802.16 but based on different call admission control algorithms have some information about GW relocation procedures. Focus on request size from MS instead of the number of MSs arriving in ASN is proposed by Bandwidth based call Admission Control (BAC) algorithm. The packet loss ratio is minimized and throughput over existing New Call Bounding (NCB) algorithm is also improved by IEEE 802.16e standard which defines the mobility management in WiMAX network, Call admission control using BAC algorithm in reference.
Authors of [65] presented an outline of security scheme in IEEE 802.16 based mobile WiMAX. The growing importance of IEEE 802.16 WiMAX will lead to compete with the 3G technologies. Security is the key feature on which the adoption and acceptance of any technologies depends. The possible solutions for eliminating the vulnerabilities of security founded in WiMAX are shown in this article. To encrypt the initial management communication and to reduce unauthenticated messages the Diffie-Hellman key exchange protocol is proposed which enhances the security level for the period of the initial network entry. Cryptographic sealing function is used to remove the man-in-the-middle attack which leads to modification of Diffie-Hellman protocol to make it fit into mobile WiMAX. This use of cryptographic sealing function not only eliminates the occurrence of man-in-the-middle attacks but also resist DoS attacks. As a result they establish that their proposed algorithm has 2.5 times improved performance with respect to existing systems.

Authors of [66] addressed a scheme which they call it SEAKS (self organized efficient authentication and key management scheme) for the purpose of hop by hop distribution and localized security control for multihop non-transparent relay based IEEE 802.16 networks. For both fixed as well as mobile non-transparent relays this scheme is suitable. Their security analysis of presented scheme and security goals are presented in this paper. Hybrid authentication scheme is provided by SEAKS with distributed authentication and key maintains .as we know this technique helps in reducing the overall authentication overhead on MR-BS and AAA sever but it also helps in providing competent way to counter measure the possible threats. In future they will try to implement a prototype of SEAKS. This will extend the scale of the experiments of other key management techniques which will have advance features such as extremely proficient and secure key management scheme on terms of authentication overhead, complexity and throughput.

Authors of [67] presented the general phenomenon of security standards and security issues associated with multihop WiMAX networks. There requires a hop by hop authentication for a secured communication in any multihop wireless network. Erstwhile hop by hop authentication is supported by WiMAX multihop networks only in a disseminated security mode. In addition to, the prevalent security issues must be taken into consideration of multihop standards. The new designed multihop standard IEEE 802.16m supports improved security and functionalities over the former one, and MAC is one of them. Performance of multicast broadcast service is another issue for which
simultaneous network coding is utilized for improved multicast broadcast service. Alternatively, the standard IEEE 802.16m has a break down over the security intimidation for initial ranging, multihop support and network coding. To overcome the above considered malfunctions, here a new distributed security architecture using ECDH (Elliptic Curve Diffie Hellman) key exchange protocol was proposed by them. The new designed architecture is capable of solving the network coding and multihop security related issue.

For fixed WiMAX network authors of [68] presented a comparison between security supported by standard and IPSec security. IP security has an advantage of strong data security because of tunnels; it also affects the QoS performance due to overhead in frame. Regardless of how, no article is reported the real measurement of the overhead of IPSec. All practical and theoretical experiments are performed before producing this sheet which is necessary for the analysis and evaluation. In addition to the strong security, IPSec security has a disadvantage that it does not support mobility. One of the results stated that if modified IPSec will be merged with IP (MIP), it may support mobility to some extent. But high mobility is not considered. Besides this ECDH is superior to IPSec in a manner that it eliminates all MAC layer security issue in the network and may provide better QoS performance of existing WiMAX MAC layer security. ECDH requires further consideration for real time testing and evaluation.

To enhance the QoS for end users it is very important aspect for multihop WiMAX networks to deploy packet scheduling and CAC (Call Admission Control). For multihop WiMAX networks the authors of [69] proposed two scheduling schemes and an adaptive call admission control method. Depending on requests made by the handover users most recently the deployed CAC changes the bandwidth reservation adaptively and put asides a limited bandwidth for mobile users. When there are no or few handover user exists on the network, the reserved bandwidth is given to the Low priority Best Effort user for effective bandwidth utilization with the admission of every new call (NC) or handover call (HC), the Base Station verifies the both bandwidth and multihop delay requirements to satisfy the QOS of the call. Following the above considerations the two downlink scheduling algorithms (P+E) and (P+TB) are also generated for the Base station. The scheduling algorithm (P+E) is a combination of priority and earliest due date scheduling while (P+TB) is a combination of priority and token bucket scheduling. (P+E) scheduling
algorithm works better in low or moderately loaded network for both multihop and single
users, but real time services are highly affected under high loaded condition.

Security and Mobility Services both are important features in WiMAX technology. Authors of [70] conveyed that based on WiMAX technology how security and mobility services are equipped together in vehicular scenario. IKEv2 and MIPv6 protocols are designed to support two different implementation schemes namely “MIP6d” and “OPENIKEv2”. An access control mechanism is provided by this coordination for visited networks. The basis of this mechanism is EAP protocol which supports a change in authentication method and tests their different behaviour in mobility scenario. The University of Murcia has developed the “OPENIKEv2”. For this reason all changes performed in order to interoperate with “MIP6d” have been performed in our IKEv2 implementation. The development in WiMAX infrastructure leads to open many research possibilities and acts as a platform to check both WiMAX and its protocol performance, where mobility and security are important aspects. Change in authentication provides to test their protocol performance in mobility scenario. Security is another important aspect in the WiMAX technology which is based on IPSec and IKEv2 to establish a secure connection.

Authors of [71] show the Femtocells services beyond the WiMAX macrocell. The research introduces the capabilities of Femtocells and a suitable call admission control algorithm and also suggests a resource management method that seriously reduces unnecessary handover. Classification of Femtocell in a WiMAX service has a very complicated work. In this work they examine that one of the key technical challenge in enhancing acceptance of Femtocell products is seamless handover between a WFAP and a macrocell. Unnecessary handover significantly affect the QoS. Signal to interference level, mobility and available bandwidth are inspected by their CAC in such a manner that uninterrupted services can be provided by WFAPs while MSs performs handover procedures. In their research, these parameters can be used to improve existing conventional schemes.

To refer to accumulation of standards and service offerings, we use the term WIMAX. They are borrowed from the IEEE 802.16 family of standards for the wireless network. These ideas describe physical and MAC layer elements which ensures interoperability of compatible equipment. Every idea gives two types of details i.e. 1) the details of the
packet scheduling algorithms. 2) the values of the performance. The second idea is related to configuration parameters to network operator. Fundamental characteristics are alternatively determined by parameters and algorithms. These characteristics include round-trip & abeyance credible throughput on the network. The authors of [72] show that arranged policies and parameter values affect real performance in ways which are not possible to characterize in inclusive studies of WIMAX.

For airport WiMAX security authors of [73] proposed a RF-DNA fingerprinting scheme. In a localized regional air monitor by making use of equipment specific RF-DNA fingerprints, a wireless communication security is addressed by the authors. Earlier RF-DNA work using OFDM based 802.11a peer-to-peer WiFi signals and GMSK based intra cellular GSM signals motivated the RF-DNA fingerprinting and thus enhances the security. The multi-carrier OFDM modulation of 802.11a and the cellular control structure of GSM are the technologies which are almost common with WiMAX technology and thus for WiMAX device discrimination RF DNA fingerprinting may be effective. To augment previous Wavelet Domain (WD) and Time Domain (TD) techniques authors in this paper introduces a Spectral Domain (SD) RF-DNA fingerprinting technique.

Authors of [74] defined the working strategy of WiMAX in an enterprise. They studied about how WiMAX and Wi-Fi can be use together. To support enterprise users roaming how unified seamless handover can be realized between Wi-Fi and WiMAX network is the biggest question of their research. Other queries in their mind were that for such an integrated network whether it is to possible to design a unified security model and how would the architecture of this integrated wireless network look like?

As the demand for network services increases, the authors of [75] presented an admission control mechanism to reduce the overwhelming effect of radio resources. Simulations were carried out by them with hierarchical Quality of Service (QoS) using NCTUns module. Their result shows that the proposed admission control mechanism can reduce the wastage of radio resources by 35% while the number of subscribers being served is increasing.