

A survey of Various Research issues in WiMAX

ANIL SANGWAN

UIET, MDU, Rohtak

anilsangwan1979@gmail.com

ABSTRACT : The full form of WiMax is Worldwide interoperability for Microwave Access. This is a communication technology that has a data transmission using various transmission modes from transportable and totally mobile internet access to point to multi-point links. This technology can provide up to 72 Mbit/s stellate broadband speed while there is no requirement for cables. This technology is predicated on IEEE802.16 standard. WiMAX offers broadband wireless access (BWA) up to 50 km for mounted stations, and 5 to 15km for mobile stations. In distinction, the WiFi/802.11 WLAN standard is proscribed in most cases to solely a 100 to 300 feet that is 30 to 100m. The main aim of my paper is to review the recent research work conducted on the WiMAX by various researchers.

Key words: WiMAX, Handover, Security

INTRODUCTION

The latest technology that provides broadband access with large coverage is Worldwide Interoperability for Microwave Access (WiMAX). WiMAX can guarantee user mobility in a large area. It has high speed internet access over an area of 30 miles and provides speed up to 70Mbps. As a cost-effective solution, multi hop communication is becoming more and more important to WiMAX systems. The advantages are increasing transmission rates, cost effective deployment and Quality of Service. WiMAX provide broadband access to anywhere [1]. It supports both fixed and mobile applications. It is a wireless technology with IEEE 802.16 standard based that provides broadband connections over long distance and it supports mobile internet which transfers data, voice, and video. Supporting both fixed and mobile broadband wireless access an IEEE 802.16e based base stations are used [2]. It fully supports mobility. There are two modes of IEEE 802.16. They are point-to-multipoint and mesh in the medium access control layer. In the point-to-

multipoint mode, base station has the overall control of all subscriber stations included in a base station cell [1]. Here the communication contains many paths from a single location. It is designed as one-to-many connection. A WiMAX PMP network aims at providing last-mile access to a broadband Internet service provider [3]. WiMAX offers many features like high bandwidth, extended coverage and low cost. By these features last mile broadband access technologies had lead to rapid raise in future networks. The structure of the network contains the Mobile Subscriber Stations(MS), Base Stations(BS), Access Service Network(ASN), Access Service Network Gateway(ASN GW)and Connectivity Service Network(CSN). The connectivity between the base station and the subscriber station is the mobile subscriber station. Base station is a fixed station in a network, used for communicating with the mobile subscriber stations. Connectivity service network also have network function that provide connectivity service to the subscriber through access service network[4].

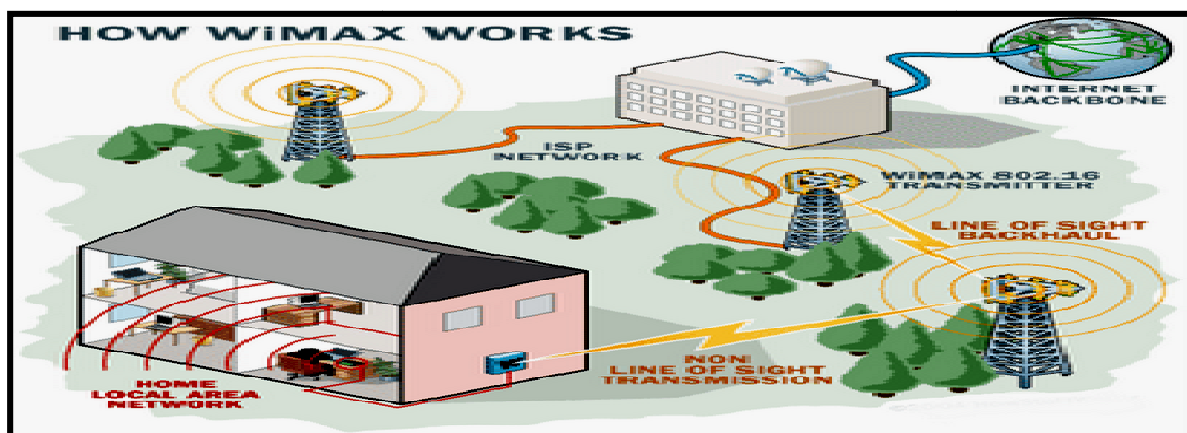


Fig1: Basic WiMAX Network [51]

Base station and Subscriber stations are organized into a cellular like structure. There are two types of channels, uplink and downlink channels. The uplink channels are from the subscriber station to base station. On the other hand the downlink channels are from base station to subscriber station. Here the subscriber stations share the channels. For WiMAX subscribers Access Service Network (ASN) will provide wireless radio access. There are two handovers in access service networks. They are inter-handover means the mobile station is within the access service network and with different access service network gateway. And in intra-handover the mobile station moves between different access service networks. A two-tier mobility management was defined by WiMAX Forum to decrease the handover delay and packet loss.

In general, handover is the important process in mobile systems. When a mobile station switches from the serving base station to another base station migrating is known as handover [5]. The main reason for handover is the mobile station gets out of the base stations transmission range[6]. Handover mechanism is divided into three phases. They are information phase, based on the decision about handover this phase have different parameters. The parameters may be distance, cost, etc. Second is the handover decision, considering this phase is one of the key factor and according to the key according to the key factor the handover decision will be taken. And the third is handover execution, in this phase the handover process is executed [7]. Before execute a handover scan for the neighboring base station for selecting the target base station by the mobile station is crucial component. When a mobile station want to join the network, then it involves scanning of desired frequency in the base station. While moving from one base station to another base station the mobile station will continuously perform scanning for maintaining the connectivity with the particular network [5]. In general, handover is divided into two types. They are soft handover and hard handover. In soft handover, before breaking the connection with serving base station registration phase will be done with the target base station. In hard handover the connection will be broken by the mobile station with the original base station before connecting with another base station [6].

The WiMAX 802.16e standards effort specifies a number of advanced security protections including: control/ management message protection, mutual device/user authentication, key management protocol, security protocol optimizations and strong traffic encryption for fast handovers when users switch between different networks. A key management protocol that enables crypto key exchange for authentication, encryption and protection of multicast and broadcast traffic to enhance security and mobility, WiMAX Forum have

been improving the standard incorporating some other capabilities [8]. Over a wireless network the data being transmitted should be protected. These are needs to confidentiality which allow only the legitimate recipients to read the information. Integrity may refer to ensure another party has not altered messages after it has been sent. And the authentication will make sure that parties sending messages or receiving messages , are who they say they are , and have the right to undertake such actions[8].

Authentication might be done by two method, they are RSA which is of mobile WiMAX standard. And the second is the Extensible Authentication Protocol, is more flexible and the ability to interact with authentication, authorizing and accounting infrastructures. And it is used for the next generation mobile WiMAX standard [group based handover]. Some of the examples security mechanism to address security are Virtual Private Networks (VPNs), Internet Protocol Security (IPSec), Intrusion Detection Systems (IDS) and Firewalls. The pre-authentication technique of mobile station and authentication server pre-compute the shared secret keys before a handover. The main advantage of the pre-authentication is that the cryptographic material will not be reused, hence it becomes more secure. The handover delay could be effectively reduced to the same amount of the time used by a 3-way handshake, resulting in the shortest authentication signaling delay [9]. In WiMAX many attacks are open to adversaries, they are Rogue base station, DoS attack, man-in-middle attack, network manipulation with spoofed management frames. Some of them are DDOS, jamming, Rogue base station attack, Reply attack, etc. Denial of service is to make the network resources of a machine unavailable to the intended users. But the target of denial of service may vary. A replay attack may be a delayed in valid data transmission in network. The rogue base station attack is a set of subscribers who try to get service which they believe to be a legitimate base station. It may lead to disturbance in service. The attacker has to capture the identity of legitimate BS. Then it builds messages using the stolen identity. The attacker must transmit while achieving a RSS (receive signal strength) higher than the one of the fake base station. Reducing the load in the system becomes an important issues in access service network gateway. Even though WiMAX is growing rapidly, still it faces a lot of security problems. In this paper a novel secure authentication scheme is proposed to provide security over the network.

LITERATURE SURVEY

Kejie Lu, Yi Qian and Hsiao-Hwa Chen have developed an effective control network framework for WIMAX. They considered both the security

requirements of the communications and the requirements of potential WiMAX applications that have not been fully addressed previously in the network layer design. The planned framework consists of two basic components: a service-aware control frame-work and a unified routing scheme. Besides the design of the framework, that they had deliberated a variety of key enabling technologies that were vital to a practical WiMAX network together with the deployment of BSs and key management, and secure routing [3].

Semin Sim and Seung-Jae Han and Seong-Choon Lee have emphasized the advantages of flat architecture for mobile WiMAX networks for data-centric wireless services. These advantages came with tough challenges, one in all that was the seamless IP-mobility mechanism. They gave a cross-layer answer for efficient handover within the flat architecture mobile WiMAX networks. A scheme was also presented to deal with the seamless mobility issue, which was one of the key challenges of the flat architecture. The proposed scheme have combined two standard IP-mobility protocols, Fast Mobile IP and Proxy Mobile IP, and customized them for IEEE 802.16e-based mobile WiMAX networks that has ability to provide interoperability with existing mobile WiMAX networks [30].

Sayan Kumar Ray, Krzysztof Pawlikowski, and Harsha Sirisena, have centered on potential handover-related research problems in the existing and future WiMAX mobility framework. A survey of those problems within the MAC, Network and Cross-Layer scenarios was presented along with the discussion of the various solutions to those challenges. A relative study of the proposed solutions, coupled with some new insights to the relevant problems, was additionally included. This paper identified the diversified MAC layer and potential network layer handover problems in MWiMAX, and additionally has highlighted those cross-layer (L2+L3) challenges that demand additional attention. Out of those, the MAC-layer HHO problems associated with the reduction and optimization of scanning activities and inter-handover CDT are still thought of to be wide open, because the MWiMAX Forum has not reached a particular conclusion regarding whether and how to modify the existing standard to include the changes recommended to date [2].

Ramanpreet Singh and Sukhwinder Singh have thought of the problem of detecting rogue base station in WiMAX/802.16 networks. A rogue base station duplicates a legitimate base station and so it is considered as attacker station. The rogue base station puzzles a collection of subscribers who attempt to get service that they believe to be a legitimate base station and it may lead to disturbance in service. The

strategy of attack depends on the kind of network. Their approach was based on the received signal strength (RSS) reports received by mobile stations and inconsistencies in sensitivity can be seen if a rogue Base Station (BS) is present in a network. These reports are assessed by the legitimate base stations, for example, when a mobile station undertakes a handover towards another BS. A new algorithm for detecting a rogue base station was described in this paper [20].

Shahid Hussain Muhammad Naeem Khan and Muhammad Ibrahim have projected a new and distinctive security model and Encryption technique on the idea of existing model to secure WiMAX from Rogue Base station Attack and reply attack. They used two way authentications between base station and therefore the subscriber station to eliminate the Rogue base station Attack. Another improvement done on this paper was the use of nonce and time stamp that eliminate reply and DOS attack. For security they projected some improvement in their model to enhance the capabilities and encryption Time. The comparison of ECC and RSA has done that shows that ECC is better than RSA due to smaller key size [25].

Zong-Hua Liu and Jyh-Cheng Chen proposed an algorithm, which incorporates traditional Admission Control (AC) and Wiener Process (WP)-based prediction algorithms to determine when to carry out ASN GW relocation. They further develop an analytical model to analyze the proposed algorithm. Simulations are also conducted to evaluate the performance of the proposed algorithm. Their results show that the proposed algorithm can improve the performance significantly in terms of blocking probability, dropping probability, average serving rate, and average signaling overhead [4].

Tonderai Muchenje, Hippolyte Muyingi provides an outline of security problems on a converged WiFi and WiMAX networks. They also seek out to provide a comparative overview of different alternative wireless convergence scenarios which might be used depending on applications requirement capabilities, suitability, and availability of coverage. They performed this research to investigate and evaluate the wireless technologies security and also to examine how the convergence of WiFi and WiMAX address confidentiality, integrity and availability (CIA) in a rural setting, Dwesa/Cwebe that was selected as the test bed for their project. Their conclusion reveal that inherent WiFi and WiMAX networks protocols could not achieve a robust and seamless converged wireless network [8].

Bo Rong, Yi Qian, Kejie Lu, Hsiao-Hwa Chen, and Mohsen Guizani, planned a framework of a 2-D CAC to accommodate variety of features of WiMAX

networks. Specifically, they decompose the 2-D uplink and downlink WiMAX CAC issue into two independent 1-D CAC issues and formulate the 1-D CAC optimization, in which the demands of service providers and subscribers are collectively taken into consideration. To solve the optimization problem, they develop a utility- and fairness-constrained optimum revenue policy, as well as its corresponding approximation algorithm [10].

Arif Ansari, Santanu Dutta and Michael Tseytlin, proposed a sub-channelization and tiling structure that permits the allocation of one subcarrier over two types of slots — two data symbols and eight data symbols with one pilot symbol in each slot. Frame synchronization strategies are proposed such that the uplink and downlink frames do not overlap, thus allowing HFDD operations over the satellite channel. These strategies use the ranging information to divide the uplink subframe into subregions and to use the appropriate one and retard or advance the uplink transmission, respectively [11].

Noudjoud Kahya, Nacira Ghoulmi, Pascal Lafourcade formally verified the key management protocol of version 2 in terms of the secure session key establishment and distribution, confidentiality, authenticity, integrity, access control. As mentioned in this paper, authentication protocol vulnerable to replay, DoS and Man-in-the middle attacks. Some solutions are introduced to solve those issues in their secure protocol (SPKM) by using nonce and timestamp together. The nonce helps the BS to identify successive requests and it enhances the BS capacity to reject those requests which was sent by the intruders or adversaries so to prevent DOS attack. The timestamp helps the BS in identifying the latest requests, which prevents reply attacks. The nonce value sent by the BS helps in preventing the man-in-the middle attack. In stapes authorization reply message, the BS sends the timestamp and nonce of SS/MS. That helps in preventing an adversary from forging a BS. Their protocol (SPKM) also provides mutual authentication. It additionally helps the SS/MS to identify the recent messages, and hence it can identify the AK used by the SS/MS as new or not. Scyther has been with success used for the analysis and design of protocols, and has also been used for theoretical research and teaching. Using this tool they prove that their solution is efficient to tackle the various security threats such as replay, man in the middle and DOS attacks [12].

Qing Wang, Chunping Hou, and Yilong Lu presented a study to understand and to demonstrate the practicability of using WiMAX signals for passive radar. The study includes WiMAX signal analysis, the design and implementation of a WiMAX-based passive radar demonstrator, the associated radar signal processing scheme, and the

field measurements. Results based on field measurements for various moving targets provide some useful references about the performance and potential capability of using WiMAX signals for passive radar applications [13].

Daan Pareit, Bart Lannoo, Ingrid Moerman, and Piet Demeester conferred a survey on all relevant activities that took place within three important organizations: the 802.16 Working Group of the IEEE (Institute of Electrical and Electronics Engineers) for technology development and standardization, the WiMAX Forum for product certification and the ITU (International Telecommunication Union) for international recognition. An elaborated and comprehensive overview of all those activities is given, which reveals the importance of the willingness to innovate and to continuously incorporate new ideas in the IEEE standardization process and the importance of the WiMAX Forum certification label granting process to ensure interoperability. They also emphasize the steps that were taken in cooperating with the ITU to improve the international esteem of the technology. Finally, a WiMAX trend analysis is made. They showed how industry interest has fluctuated over time and quantified the evolution in WiMAX product certification and deployments. It is shown that most interest went to the 2.5 GHz and 3.5GHz frequencies, that most deployments are in geographic regions with a lot of developing countries and that the highest people coverage is achieved in Asia Pacific. This elaborated description of all standardization and certification activities, from the very start up to now, will make the reader comprehend how past and future steps are taken within the development process of new WiMAX features [14].

CONCLUSION

WiMAX is one of the fast growing technologies in the world as compare to other wireless networks. The traditional management admission control (AC) algorithms cannot be used directly once the two-tiered mobility quality management is deployed in WiMAX, because some mobile stations (MSs) could also be served by two access service network gate ways (ASN GWs). If there are many Anchored MSs, new incoming users will likely be rejected due to the lack of resources. There is a possibility of security issues and threats like Distributed Denial of Service (DDOS), jamming Rogue Base station attack, Reply Attack and so on in WiMAX networks. Different WiMAX Security Models are proposed in different papers. The various models for WiMAX can either handle one or two possible attacks in the given, Dos attack, Replay attack, Rogue base station attack and Man in the middle attack, and does not able to handle all these attacks, which is the main deficiency in

these models. And also in the GW relocation, the handover latency will be too high if the handover MS needs to wait for the ASN GW relocation of one Anchored MS. The main concept behind this work is to allow new mobile stations to the access service network by an admission control(AC) algorithm which cooperates with the ASN GW relocation. When a new MS arrives and there is no resource for the newly arrived MS, the gateway relocation admission control algorithm GRAC will request an Anchored MS to perform ASN GW relocation. The proposed work provides high security and also handles DoS attack, Replay attack, Rogue base station attack, and Man in the middle attack successfully by using two way authentication mechanisms. And also this proposed scheme reduces the acceptable handover latency by using a grouping algorithm to handover a mobile station from a service base station to the target station.

REFERENCES

- [1] Bokrae Jung, JungYul Choi, Young-Tae Han, Min-Gon Kim, and Minho Kang, "Centralized Scheduling Mechanism for Enhanced End-to-End Delay and QoS Support in Integrated Architecture of EPON and WiMAX", JOURNAL OF LIGHTWAVE TECHNOLOGY, VOL. 28, NO. 16, AUGUST 15, 2010
- [2] Sayan Kumar Ray, Krzysztof Pawlikowski, and Harsha Sirisena, "Handover in Mobile WiMAX Networks: The State of Art and Research Issues", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 12, NO. 3, THIRD QUARTER 2010
- [3] Kejie Lu and Yi Qian, and Hsiao-Hwa Chen, "A Secure and Service-Oriented Network Control Framework for WiMAX Networks", IEEE Communications Magazine, May 2007
- [4] Zong-Hua Liu and Jyh-Cheng Chen, "Design and Analysis of the Gateway Relocation and Admission Control Algorithm in Mobile WiMAX Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 1, JANUARY 2012
- [5] Prashant Shinde, "Optimization of Handover Performance in Mobile WMax 802.16E", International Journal of Emerging Technology and Advanced Engineering, Volume 2, August 2012
- [6] Firas Abdullah Thweny Al-Saedi and Wafa A. Maddallah, "Evaluation of Handover Process in WIMAX Networks", IJCSET, Vol 2, Issue 1, 831-838, January 2012
- [7] Sajjan Singh, Rasveen and S. V. A. V. Prasad, "A Parametric Scheme to Perform an Efficient and Reliable Vertical Handover", International Journal of Engineering and Advanced Technology, ISSN: 2249 – 8958, Volume-2, October 2012
- [8] Tonderai Muchenje and Hippolyte Muyingi, "An Overview of Security Issues on a Converged WiFi and WiMAX Network"
- [9] 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
- [10] Anmin Fu, Shaohua Lan, Bo Huang, Zhenchao Zhu and Yuqing Zhang, "A Novel Group-Based Handover Authentication Scheme with Privacy Preservation for Mobile WiMAX Networks", IEEE COMMUNICATIONS LETTERS, VOL. 16, NO. 11, NOVEMBER 2012
- [11] Arif Ansari, Santanu Dutta and Michael Tseytlin, "S-WiMAX: Adaptation of IEEE 802.16e for Mobile Satellite Services", IEEE Communications Magazine, June 2009
- [12] Noudjoud Kahya, Nacira Ghoulmi and Pascal Lafourcade, "Secure key management protocol in wimax", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.6, November 2012
- [13] Qing Wang, Chunping Hou, and Yilong Lu, "An Experimental Study of WiMAX-Based Passive Radar", IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES, VOL. 58, NO. 12, DECEMBER 2010
- [14] Daan Pareit, Bart Lannoo, Ingrid Moerman, and Piet Demeester, "The History of WiMAX: A Complete Survey of the Evolution in Certification and Standardization for IEEE 802.16 and WiMAX" IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14, NO. 4, FOURTH QUARTER 2012
- [15] 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
- [16] S. Srikanth and P. A. Murugesu Pandian and Xavier Fernando, "Orthogonal Frequency Division Multiple Access in WiMAX and LTE: A Comparison", IEEE Communications Magazine, September 2012
- [17] Anmin Fu, Shaohua Lan, Bo Huang, Zhenchao Zhu and Yuqing Zhang, "A Novel Group-Based Handover Authentication Scheme with Privacy Preservation for Mobile WiMAX Networks", IEEE COMMUNICATIONS LETTERS, VOL. 16, NO. 11, NOVEMBER 2012
- [18] Qi Jing, Yuqing Zhang, Xuefeng Liu and Anmin Fu, "An Efficient Handover Authentication Scheme with Location Privacy Preserving for EAP-based Wireless Networks", Communications (ICC), 2012 IEEE International Conference.
- [19] Poojabhat and Bijendermehandia, "Analysis of Handover in Wimax for Ubiquitous connectivity", International Journal Of Computational Engineering Research, Issue No.4, Vol.2, July-august 2012

- [20] Ramanpreet Singh, Sukhwinder Singh, "Detection of Rogue Base Station Using MATLAB", International Journal of Soft Computing and Engineering, ISSN: 2231-2307, Volume-1, Issue-5, November 2011
- [21] B.Sridevi, Dr.S.Rajaram, "Dynamic Inter Arrival Time Based Seamless Handoff for Mobile WiMAX Ping-Pong Calls Bypassing PKMv2 EAP Authentication", I. J. Computer Network and Information Security, 2012
- [22] Abhijeet V. Shinde, A.D.Bijwe, "A Novel Handoff Technique for Heterogeneous Wireless Network", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 1, January 2012
- [23] Prashantshinde, "Algorithm for the selection of target base station during handover in mobile wimax 802.16e", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 9, September 2012
- [24] MRS. M. REKHA and DR. C. CHAND - RASEKAR, "Trust Based Authentication Technique for Security in WiMAX Networks", International Journal of Communications and Engineering, Volume 03– No.3, March 2012
- [25] Shahid Hussain, Muhammad Naeem Khan, Muhammad Ibrahim, "A Security Architecture for Wimax Networks", International Journal of Computer Applications, Volume 50 – No.9, July 2012
- [26] Himanshu Kaushik, Sumit Chaudhary, Neha Singh and Kapil Kumar Verma, "Advance Handoff Requirements Schemes in Wimax and LTE Networks in Wireless Sensor Network", International Journal of Computer Applications, Volume 59– No.19, December 2012
- [27] Paul Boone, Michel Barbeau and Evangelos Kranakis, "Strategies for Fast Scanning and Handovers in WiMax/802.16"
- [28] Bo Rong, Yi Qian, Hsiao-Hwa Chen, "Adaptive power allocation and call admission control in multiservice wimax access networks", IEEE Wireless Communications, February 2007
- [29] Deepti and Deepika Khokhar, "Detection of Rogue Base Stations in Wimax/IEEE 802.16 using Sensors", International journal of computer technology & applications, vol.3. July-August 2012.
- [30] Semin Sim Seung-Jae han and Seong-choon Lee, "Seamless IP Mobility support for Flat Architecture Mobile WiMAX Networks" IEEE Communications Magazine, June 2009.
- [31] C. Politis, K. A. Chew, N. Akhtar, *et al.*, "Hybrid multilayer mobility management with AAA context transfer capabilities for all-IP networks," IEEE Wireless Commun., vol. 11, no. 4, pp. 76–88, Aug. 2004.
- [32] C. M. Huang and J. W. Li, "A cluster-chain-based context transfer mechanism for fast basic service set transition in the centralized wireless LAN architecture," Wireless Commun. Mob. Comput., vol. 9, no. 10, pp. 1387–1401, Oct. 2009.
- [33] J. Hur, H. Shim, P. Kim, *et al.*, "Security considerations for handover schemes in mobile WiMAX networks," in Proc. 2008 WCNC, pp. 2531–2536.
- [34] A. Fu, Y. Zhang, Z. Zhu, *et al.*, "A fast handover authentication mechanism based on ticket for IEEE 802.16m," IEEE Commun. Lett., vol. 14, no. 12, pp. 1134–1136, Dec. 2010.
- [35] L. Shan, F. Liu, and K. Yang, "Performance analysis of group handover scheme for IEEE 802.16j-enabled vehicular networks," in Proc. 2009 Advances in Data and Web Management, pp. 653–658.
- [36] L. Lee, D. Kim, B. Chung, *et al.*, "Adaptive hysteresis using mobility correlation for fast handover," IEEE Commun. Lett., vol. 12, no. 2, pp. 152–154, Feb. 2008.
- [37] H. H. Choi, J. B. Lim, H. Hwang, *et al.*, "Optimal handover decision algorithm for throughput enhancement in cooperative cellular networks," in Proc. 2010 IEEE VTC – Fall, pp. 1–5.
- [38] S. J. Vaughan-Nichols, "Achieving Wireless Broadband with WiMAX," IEEE Comp., vol. 37, issue 6, June 2004, pp. 10–13.
- [39] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security," IEEE Sec. & Privacy, vol. 02, no. 3, May-June 2004, pp. 40–48.
- [40] Akyildiz and X. Wang, "A Survey on Wireless Mesh Networks," IEEE Commun. Mag., vol. 43, no. 9, pp. S23–S30, Sept. 2005.
- [41] R. Bruno, M. Conti, and E. Gregori, "Mesh Networks: Commodity Multihop Ad Hoc Networks," IEEE Commun. Mag., vol. 43, no. 3, Mar. 2005, pp. 123–31.
- [42] M. Lee *et al.*, "Emerging Standards for Wireless Mesh Technology," IEEE Wireless Commun., vol. 13, no. 2, Apr. 2006, pp. 56–63.
- [43] N. Ben Salem and J.-P. Hubaux, "Securing Wireless Mesh Networks," IEEE Wireless Commun., vol. 13, no. 2, Apr. 2006, pp. 50–55.
- [44] H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002, pp. 70–75.
- [45] Jamshed Hasan, "Security Issues of IEEE 802.16 (WiMAX)" Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, Page(s): 1-10, 2006.
- [46] Syed Shabih Hasan and Mohammed Abdul Qadeer "Security Concerns in WiMAX", IEEE First Asian Himalayas International Conference, Page(s): 1-5, November 2009.
- [47] Sanjeev Dhawan, "Analogy of Promising Wireless Technologies on Different frequencies: Bluetooth, WiFi, and WiMAX" 2007, IEEE 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Page(s): 1-9.

- [48] Lang Wei-min, Wu Run-sheng and Wang jian qiu, "A Simple Key Management Scheme Bsaed on WiMAX", IEEE Computer Science and Computational Technology, ISCSCT '08. International Symposium, Page(s): 3-6, Dec. 2008.
- [49] Jim Martin, Bo Li, Will Pressly and James Westall, "WiMAX Performance at 4.9 GHz", IEEE Aerospace Conference, Page(s): 1-8, March 2010.
- [50] Mussa Bshara and Leo Van Biesen, "Localization in WiMAX Networks Depending on The Available RSS-based Measurements", International Journal on Advances in Systems and Measurements, volume 2 no 2&3, Page(s): 214-223, 2009.
- [51] <http://www.seminarpaper.com/2012/02/worldwide-interoperability-for.html>