International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Volume 7 Issue 3, March-2018, Impact Factor: 3.578

# Analysis of Security and Threats in Video Data Transmission over WIMAX Networks

Mangal Sain[1], Dr. Pawan Kumar[2]

[1]Research Scholar, Mewar University, Chittorgarh, Raj.
[2]Principal, Ganga Technical Campus, Bahadurgarh

**ABSTRACT**

**This paper studies the topic strong security in wireless network which is essential for real time services of any wireless system. WIMAX standout amongst the latest wireless broadband access networks which supports mobility and high data rate and is very useful as WIMAX data LANs are used for government, military and business applications. In any case, free-space transmission exhibits new chances for tuning in on wireless data exchanges. What makes it worse is that the sender and the arranged authority do not have information whether the data transmission has been intercepted or not, so the leakage of data in every practical sense is undetectable. Number of papers has been studied and result is that the main and very important issue in the design plan of WIMAX is security development. The centre point of this paper is to examine secure information transmission for real time environment conditions while using WIMAX.**

**Keywords: WIMAX, network, video, data, transmission.**

## INTRODUCTION

The WIMAX (Worldwide Interoperability for Microwave Access) is based on IEEE 802.16 wireless Metropolitan Area Network standard which focuses on solving the problems associated with point-to-multipoint broadband outdoor wireless network. WIMAX system prove to be a more effective technique in NLOS (non-line-of-sight) situations contrasted with fixed connection DSL or cable technique which are more costly to introduce. The 802.16 standard includes various creative highlights empowering high traffic rates, scalable architecture and limited delays which make it attractive for different broadband wireless applications. It is the innovation targeted to give broadband wireless data access over long gaps. It depends on IEEE 802.16 and the standard characterizes only physical (PHY) layer and MAC layer functionalities. The innovation gives fundamental Internet Protocol (IP) link and connection oriented wireless communications to the clients. To expand the mobile user requirements and coverage area, the IEEE standard innovated the 802.16e and 802.16j forms.

At present, the IEEE 802.16m standard is attempting to help the IMT Advanced necessities. The current security issues in mobile WIMAX systems and QOS upgrades are considered in IEEE 802.16m and it has full backward interoperability and compatibility with legacy networks. The PHY layer is used for particular to transmit and receive purposes and wireless channel purposes. The MAC layer has three sub layers, MAC convergence sub layer, MAC common part sub layer and security sub layer. The first one is used for data planning such as processing of packets. The second one is used for control functions and the last one is used for the purpose of security for both system and clients.

The security sub layer underpins are to:

(i) Authenticate the user when the user enters into the network.

(ii) Authorize the user, if the user has provisioned by the network service provider.

(iii) Give the necessary encryption support for the key transfer and data traffic.

An overview of security functions is defined in the standards. Even that the IEEE 802.16 give well defined security structure, some security issues still exist because of the unauthenticated/unencrypted MAC control messages. Numerous current research efforts give answers for every security threats in light of public key management (PKM) protocol and some of ISPs have attempted IPSec practically for implementation. The default security system provide by

layer-3 Virtual Private Networks (VPNs) is IPSec. While giving solid security to an access system with IPSec, the current QOS support ought not to be influenced. Comparative examinations have been led just in re-enactments. Real investigations and estimations are essential for experts and analysts for better examination.

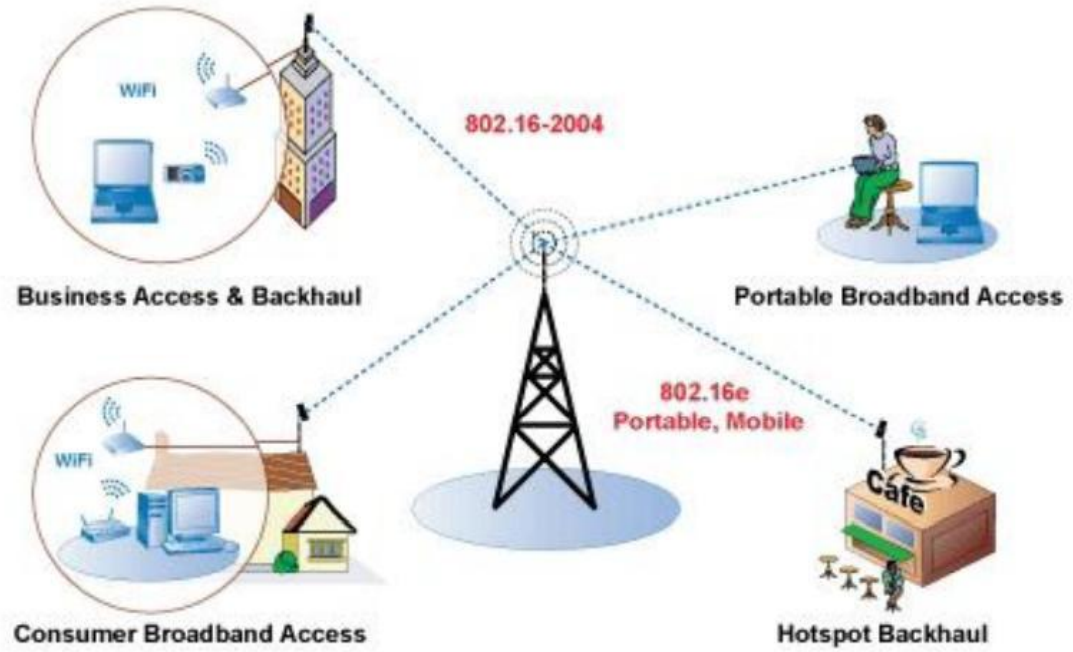


**Fig. 1: WIMAX Network**

WIMAX have generated interest among the researchers these years because of their potential usage in wide variety of the applications [4]. WIMAX supports different types of the modulation and the coding plans and enables the plan to change on a burst-by-burst basis per interface, according to channel conditions [6]. The data transmission rate and range of WIMAX make it reasonable for the following applications:

1. Giving mobile portable broadband availability crosswise over urban areas and countries through different types of gadgets

2. Giving a wireless alternate to cable system and digital subscriber line (DSL) for "last mile" broadband access

3. Giving telecommunications (VoIP), data and IPTV administrations (triple play)

4. Giving internet as a major aspect of a business design

5. Metering and smart grids

## COMPARISON BETWEEN WIMAX AND Wi-Fi

The most constructive approach is that WIMAX and WiFi are strongest when working collaboratively. Therefore multi-mode cards (for multi-mode devices) will revolutionize the roaming hotspot client's experience. Furthermore, the innovations will exist together innovatively. The advancement of WIMAX and WiFi is a complementary pattern. In the current circumstances they have existed together with each other, and facilitated well with 3G innovation. WiFi, WIMAX and 3G joint system make utilization of a brought together administration stage to share client's data. So the output of the current network can be improved. WIMAX has been sent in three stages. The main stage is utilizing an indoor antenna to implement IEEE802.16d standard WIMAX. The objective client is the known endorser in a settled area. The second stage use substantial indoor antennas. WIMAX innovation will expand the interest to administrators who try to disentangle the client purpose of establishment. The third stage is the place the IEEE802.16e standard is propelled.

WIMAX certified hardware in this standard will be utilized in portable solution for those clients who need to roam in service zone, supporting like the present WiFi capacities, yet with more stable connections. Gumaidah, B. F., Soliman, H. H., and Obayya, M. (2012) talks about the execution of WIMAX with voice communication. The outcomes demonstrate that the higher the base frequency, higher the Signal to Noise Ratio that give less delay in end to end

packet transmission and give high throughput. WIMAX are relied upon to deliver broadband access service to enterprise and residential clients at low cost. Leaving aside cellular systems, a practical method of having WIMAX and WiFi joint system is to utilize WIMAX to connect with WiFi hotspots. It can give E1/T1 and IP double channel wireless transmission for WLAN AP and accomplish a more extensive scope of high speed wireless access. Along these lines, WiFi can expand its access region and give better data services to user.

**Difference between WIMAX and Wi-Fi are visit in light of the fact that both are identified with wireless availability and Internet.**

1. WIMAX is a long range network, covering numerous kilometres that utilize authorized or unlicensed range to deliver connection to network, much of the time the Internet.

2. Wi-Fi utilizes unlicensed range to give access to the local network.

3. Wi-Fi is better known in end client devices.

4. Wi-Fi keeps running on the Media Access Control's CSMA/CA protocol, which is contention based and connectionless while WIMAX runs the connection oriented MAC.

5. Wi-Fi and WIMAX have different QOS mechanism.

6. WIMAX utilizes a QOS mechanism in view of connections between base station and the client gadget. Each connection depends upon specific scheduling algorithms.

7. Wi-Fi utilizes conflict across all subscriber stations that desire to pass data through a wireless access point (AP) are in state of competition for AP's consideration on random interrupt basis. So subscriber stations those who are at a distance from AP to be interrupted again and again by nearer stations, so reducing their throughput.

8. 802.11 (which incorporate Wi-Fi) and 802.16 (which incorporate WIMAX) both define Peer-to-Peer and ad hoc systems, where an end client communicates to clients or servers on another Local Area Network (LAN) using its AP or base station. 802.11 supports direct ad hoc or peer to peer networking between end client gadgets without an AP while 802.16 end client gadgets must be in range of base station.

## VIDEO STREAMING NETWORK TOPOLOGY

Video content refers to the audio and visual data available from the video service providers hosting IPTV and VoD services. The content starts from an extensive variety of sitcoms, reports, movies in real time, stored video formats (VoD) and sporting events. It is made as a sequence of video frames or pictures that are transmitted (streamed) to the subscriber and showed to him at a consistent frame rate [6]. The video part is coupled with a multi-channel audio part that is made as a sequence of audio frames to collectively contain the video content. Video content streaming is inherently loss tolerant yet delay-touchy [10], which infers that video playback on subscriber end may tolerate some level of frame loss. Variations or delays interframe reception quickly degrade the general video playback experience. While spilling continuous video and VoD have distinctive transmission and buffering necessities from the system and the customer station video player or set best box (STB), video content might be described by number of parameters including video format, coding plan, frame interarrival rate and pixel colour depth. Video resolutions are explained as maximum horizontal by vertical pixel geometry that have range from 128 x 96 pixels to 1920 x 1080 pixels for HDTV. Normal video resolutions for Internet-based YouTube, Google Video and Skype video streaming are 320 x 240 pixels (QVGA).

Also, combined with video resolution, colour depth, ranging up to 8 bits for every primary colour per pixel, can incredibly affect the video content size. Video content can be a sequence of images showed at a constant rate and each frame has spatial (inside) redundancy. So number of videos coding plans have been designed to decrease the raw video content size by the exploitation of this redundancy while adjusting quality. These plans incorporate the International Telecommunications Union (ITU) H.26x and International Standards Organization (ISO) Motion Picture Experts Group (MPEG) codecs. MPEG codecs including MPEG-1, MPEG-2 and MPEG-4 have differed compression qualities. Every MPEG bit stream has six layers: sequence layer, group of pictures (GoP) layer, silica layer, frame layer, macro block layer, and block layer. Besides, there are three distinctive frame types: predicted frames (P frames), intra frames (I frames) and bi directional frames (B frames). As Figure 2 shows, the coding order of a GoP is not quite the same as the display order of the GoP [12]. Therefore, as showed in Appendix A, past efforts needed to re-sequence the GoP into coding order for network transmission.

The sound segment of the streaming video content might be seen as a one or more sound channels encoded into a multi-channel sound (audio) stream. Channel arrangements go from a single channel to 5.1, 6.1 and 7.1 configurations

representing different combinations of left, centre, right, left surround, right surround, left back, right back and low frequency effects (LFE) channels. As one discretely encodes more source channels, in result the requirement of audio stream bandwidth increases. A potential bargain in Internet based video system down mixing multi-channel sources into conventional two channel stereo format or to just encode the two main channels. The encoding parameters of various other channels contribute to overall requirement of bandwidth.The sample size and sample rate play an important part in stream size. There can be loss or loss free the codec compression technique. The lossy compression strategies remove non-essential audio content while keeping certain frequencies intact where loss free strategies guarantee reproduction of audio source content while compressing output.

As appeared in Figure 2, protocol stack for streaming video services incorporate the Real Time Protocol (RTP) that provide a packet structure for audio and video data over the transport layer protocol. RTP indicates a 12-byte header with fields to describe the type of content being carried (MPEG-2, MPEG4, and so on), packet sequencing and time stamping. Since RTP lies over transport protocol, it is implemented in the end system. RTP does not give mechanism to ensure bandwidth or packet delays. [15].

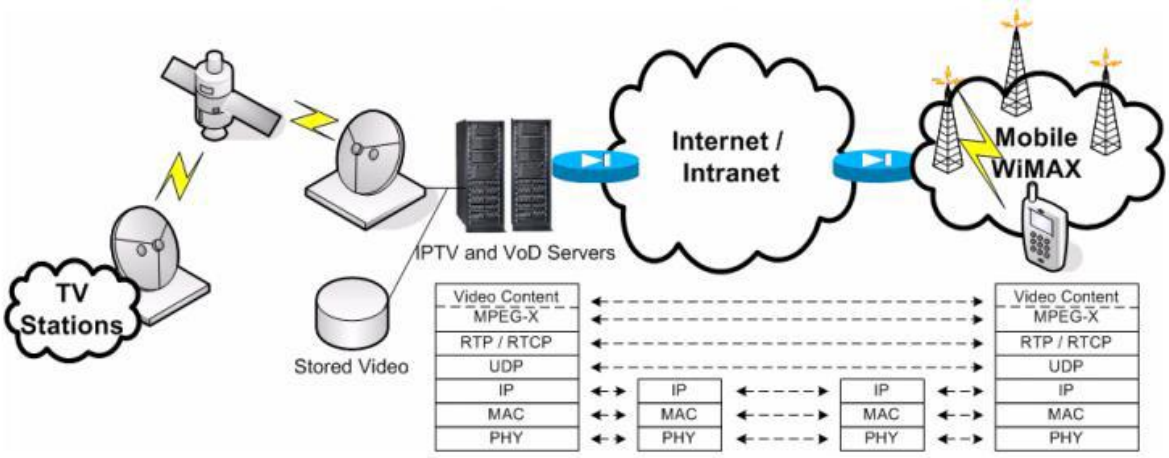


**Fig. 2: Video streaming network topology**

## SECURITY AND THREATS IN WIMAX NETWORKS

There are three security plans considered for this examination:

1) Default MAC-layer security defined by the standard.

2) IPSec security over the MAC-layer security

3) The proposed ECDH protocol at MAC layer with default security. To begin with, we clarify how the proposed ECDH protocol defeats the current security dangers in each classification for both WIMAX and LTE systems.

### Analysis of Security Threats in WIMAX Networks

1) Ranging attacks: In our proposed architecture for security, RNG_REQ and RNG_RSP messages are encrypted by public key of receiver. So intermediate rogue node has difficulty in processing the message in a short period of time. So system is free from DoS/Replay and other different types of attacks during initial stage.

2) Power saving attacks: the IEEE 802.16m standard gives an alternate for encrypting control messages in a power saving mode. For IEEE standard, network may utilize ECDH implementation to beat the power saving attacks.

3) Handover attacks: The MOB NBR-ADV attacks don't exist in the IEEE 802.16 network on the grounds that the BS can encrypt the message. For some other networks, the messages are encrypted with the use of ECDH to defeat those security dangers. During handover for latency issues, two situations are considered:

i) RS mobility (e.g., RS is implemented on the top of a train, and WIMAX clients are inside the train),

ii) MS mobility. For RS mobility in the proposed security design, re-authentication for RS isn't important, on the ground that the BS or the target RS knows list of RSs and the relating RS_ID in the network. Something else, if the target node is other BS, the serving BS can send the RS verification data including AK in a secured way, as defined in IEEE 802.16m.

4) Miscellaneous attacks: For downgrade attacks, if the security level is low in the MS basic capacity ask for the message, the BS ought to ignore the message. For bandwidth spoofing, the BS ought to allot the bandwidth on the ground of the provisioning of the MS. These downgrade attack and bandwidth spoofing can be tackled by utilizing basic intelligence in the BS.

5) Multihop security threats: It is major issues in multihop wireless network. It is the presentation of rogue node in multihop path. In the distributed security mode, once the joining node is validated by the home system (AAA server), mutual validation happens between the joining node and the access node (RS or BS). So the new node recognizes the rogue node during the mutual validation step, and other credential data is not shared. In this manner, the proposed arrangement maintains a strategic to avoid the rogue node problem. Using the ECDH public key of the receiver, the communication between the BS and access RS is encrypted. This is done for tunnel mode security support. So the system supports tunnel mode operation utilizing the ECDH tunnel.

6) Other security threats: Other security threats, for example attacks against WIMAX security, mess mode attacks and multicast/broadcast attacks don't exist in IEEE 802.16m systems. Otherwise the control messages are encrypted if the network utilises ECDH implementation. Hence, those security threats are avoided.

## CONCLUSION

In this paper, the author has studied secure video data communication for wireless transmission mobile WIMAX systems. WIMAX system studies continue to project increased subscriber growth rates and planned carrier trials around the world. With these growth rates, keeping in mind that if WIMAX is formidable player in fourth era mobile systems, it is desirable to evaluate performance utilizing video-rich emerging services to adequately load and stress the system to exploit the potential bandwidth, delay and mobility limitations.

## REFERENCES

[1] M. Purkhiabani and A. Salahi, ―Enhanced authentication and key agreement procedure of next generation evolved mobile networks,‖ in Proc. 3rd Int. Conf. Commun. Softw.Netw., 2011, pp. 557–563.
[2] H-M. Sun, Y-H. Lin, and S-M. Chen, ―Secure and fast handover scheme based on pre-authentication method for 802.16-WiMAX,‖ in Proc. IEEE Region 10 Conf., 2007, pp. 1–4.
[3] T. Shon and W. Choi, ―An analysis of mobile WiMAX security: Vulnerabilities and solutions,‖ in Lecture Notes in Computer Science, T. Enokido, L. Barolli, and M. Takizawa, Eds. Berlin, Germany: Springer-Verlag, 2007, pp. 88–97.
[4] J. Donga, R. Curtmolab, and C. N. Rotarua, ―Secure network coding for wireless mesh networks threats challenges and directions,‖ J. Comput. Commun., vol. 32, no. 17, pp. 1790–1801, Nov. 2009.
[5] L. Yi, K. Miao, and A. Liu, ―A comparative study of WiMAX and LTE as the next generation mobile enterprise network,‖ in Proc. 13th Int. Conf. Adv. Comm. Tech., 2011, pp. 654–658.
[6] A. Panayides, M.S Pattichis, C.S Pattichis, C.N.Schizas, A. Spanias, and E.C. Kyriacou, "An overview of recent end-to-end wireless medical video telemedicine systems using 3G," in Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc., Buenos Aires, Argentina, Aug.31-sep.4, 2010, pp. 1045-1048.
[7] C.S Pattichis, C.P Loizou, and M. Pantziaris, And A. Nicolaides, "An integrated system for the segmentation of atherosclerotic carotid plaque,"IEEE Trans. Inf. Technol. Biomed., vol. 11,no. 5, pp. 661-667, Nov.2007.
[8] M.G. Martini and C.T.E.R. Hewage, "Flexible macroblock ordering for context-aware ultrasound video transmission over mobile WiMAX," Int. J. Telemed. Appl., vol. 2010, p. 14, 2010.
[9] A. Alinejad, N. Philip, and R. Istepanian, "Cross layer ultrasound video streaming over mobile WiMAX and HSUPA networks," IEEE Trans. Inf. Technol. Biomed., vol. 16,no. 1, pp.31-39,Jan. 2012.
[10] O. Issa, J. Gregoire, Y. Belala, J. Wong, and M. Bage, "3G video uploading applications: performance and improvements," IEEE Computer Society 2008, vol. 15, no. 4, pp. 58-67, Dec. 2008.
[11] R. Weber, M. Guerra, S. Sawhney, L. Golovanevsky, and M. Kang, "Measurement and analysis of video streaming performance in live UMTS networks," in Proc. WPMC 2006, San Diego, CA, Sep. 2006, pp. 1-5.
[12] M. Yang and N. Bourbakis, "A prototyping tool for analysis and modeling of video transmission traces over IP networks," in Proc. IEEE Rapid Prototyping Workshop, Chania, Crete, Jun. 2006, pp. 33-39.
[13] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "Real time protocol," RFC 3550, Jul. 2003.
[14] WiMAX forum, WiMAX Technology info, www.quantum WiMAX.com.
[15] Jamil M. Hamodi and Ravindra C. Thool, "Investigate the performance evaluation of IPTV over WiMAX networks" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.1, January 2013.
[16] Kamali, B., Bennett, R.A. & Cox, D.C. (2012) 'Understanding WiMAX: An IEEE-802.16 StandardBased Wireless Technology', Potentials, IEEE, 31(5), pp. 23-27.
[17] Long H. (2006) OPNET Modeler and Computer Network Simulation. Shan Xi: University of Electronic Science and Technology.
[18] Marzuki, A., & Baba, M.D. (2011) 'Downlink Performance Evaluation of Multi-Mode Devices in WiMAX and WiFi Environment', Control and System Graduate Research Colloquium (ICSGRC), IEEE, pp.150-158.

[19] Patidar, M., Dubey, R., Jain, N.K., &Kulpariya, S. (2012) 'Performance Analysis of WiMAX 802.16e Physical Layer Model', 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN), pp.1-4.
[20] Ahmed, S. (2014) 'Performance Analysis of Mobile WiMAX Technology', 2014 International Conference on Computing for Sustainable Global Development (INDIACom), pp.959-961.
[21] Sina. (2011) Taipei free wireless network fully opened while using WiMax and WiFi. Available at: http://tech.sina.com.cn/t/2011-10-10/14346157133.shtml (Accessed: 1 August 2014).
[22] Hughes, J. (2009) Network simulation Introduction. Available at: http://www.openxtra.co.uk/articles/network- simulation (Accessed: 7 October 2014).