3.4 Attacks

The commonly Message replay attack is one of the attacks on authentication and authenticated key establishment protocols and another commonly attack is Man-in-the-middle attack. The Other attacks are parallel session attackers, reflection attack, interleaving attack [1] attack due to type flaw, attack due to name omission etc. Interleaving Attack: Interleaving Attack uses the messages from previous protocol sessions being run concurrently to the main protocol session, in order to provide the messages in the main protocol session. The request message is easy to be modified or impersonated without a mobile station signature. The attack still exists even with the signature from the mobile station. Multiplicity Attack: A new attack called Multiplicity Attack is on the original X.509 3- way authentication protocol

3.5 Privacy and Key Management Protocol and authorization

The 802.16 standard specifies a security as a separate layer called MAC security sub layer. Two protocols are used in this MAC security sub layer an encapsulation protocol for encrypting packet data, and Privacy and Key Management Protocol as shown in fig 8 distribute the key and provide secure communication between base station and a mobile station. The Privacy and Key Management Protocol uses X.509 digital certificates, RSA public-key algorithm, and strong encryption algorithm to perform key. A two-tier key system is used in IEEE 802.16 system Authentication Key and Encryption Keys. The Authentication Key is used for authenticating mobile station to base station and the Authentication Key is used to secure the exchange of Transport Encryption Keys as shown in fig 8 and also mobile station also needs to authenticate a base station to keep away from malicious ones. The Privacy and Key Management authorization consists of a three-message exchange between a mobile station and a base station. The mobile station initiates the protocol by sending the first two messages and the base station responds to the third message. The mobile station uses Message 1 to push its Manufacturer X.509 certificate [23] to the base station so that the base station decide the mobile station as a trusted node, sometimes the security policy of the base station ignore this message as it is not a trusted node.

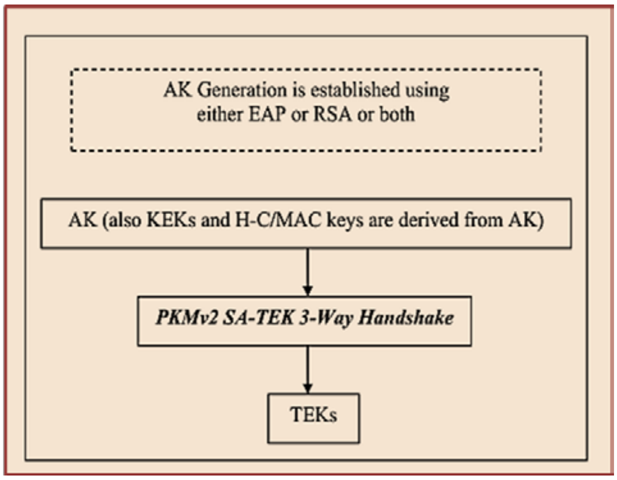
AK Generation is established using
either EAP or RSA or both
AK (also KEKs and H-C/MAC keys are derived from AK)
PKMv2 SA-TEK 3-Way Handshake
TEKs

Fig 8: Privacy and Key Management version 2 Protocol

Then the mobile station immediately sends Message 2 to the base station consists of its X.509 certificate and its identity SAID. Then the base station verifies the mobile station X.509 certificate [1] and authorizes the mobile station by sending Message 2 consists of authorization Security association between the two stations which is an authorization to access the WMAN channel. The Privacy and Key Management Protocol [25] consists of a two/three message exchange between the mobile station and a base station. The base station sends the first message which is an optional one unless it wants to rekey a data Security association or create a new Security association. The mobile station initiates the protocol by sending the second message by request Security association parameters and the base station responds with the third message as shown in fig 8. The mobile station must take Security association identifier from the authorization protocol Security association identifier [21] List or from a Message 1 as shown in fig 10 with valid Hash function-based message authentication code. If Hash function-based message authentication code is valid and Security association identifier identifies one of mobile station Security association, base station configures the Security association using Message 3.

4 Conclusions and Future Perspective

The first IEEE 802.16 standard was approved in 2001 and published in 2002 includes air interface standard for wireless broadband. The IEEE 802.16j standard approved in 2009 provides multi-hop relay operation. The relay architecture in IEEE 802.16j standard provides coverage extension and capacity increase with reduced cost. The IEEE 802.16j standard defines two layers physical and MAC layers. The current technologies of physical and MAC layers are SOFDMA, Mobile WiMAX channel encoding process, Relay station grouping and Messages, Ideal mode operation, Paging and Location management, Privacy Key Management protocol, WiMAX physical layer security [1] , comparison of WIMAX OFDM , OFDMA and SOFDMA, Uplink Sub Frame: down link Sub Frame, IEEE 802.16 Protocol Stack, Privacy and Key Management Protocol and authorization.

5 Acknowledgments

This work was supported by Department of Computer Science and Engineering, Coimbatore Institute of Engineering and Technology, Coimbatore, INDIA. We thank the management for providing facility to do research in networks laboratory.

References:

[1] "IEEE Standard for Local and Metropolitan Area Networks: Part 16: Air Interface for Broadband Wireless Access Systems, IEEE Std 802.16-2009", May 2009, 2094 pp.

[2] C. So-In, R. Jain, and A. Al-Tamimi, "Scheduling in IEEE 802.16e WiMAX Networks: Key issues and a survey," *IEEE J. Select. Areas Commun.*, Vol. 27, no. 2, pp. 156–171, Feb. 2009.

[3] D. Satishkumar, N. Nagarajan, "A Survey on Technical Issues in IEEE 802.16j Mobile Multi-hop Relay Networks," *The Smart computing Review*, vol. 1 No 1, pp. 12–33, Oct. 2011.

[4] D. Satishkumar, N. Nagarajan, "Technical Issues in IEEE 802.16j Mobile Multi-hop Relay Networks," *European Journal of Scientific research,* Vol.65 No.4 (2011), pp. 507-53

[5] D. Satishkumar, N. Nagarajan, "A new Adaptive Model for Throughput Enhancement and Optimal Relay selection in IEEE 802.16j Networks" *Wseas Transactions on Communication,* Issue 2, Volume 11, February 2012

[6] D. Satishkumar, N. Nagarajan, "Relay technologies and technical issues in IEEE 802.16j Mobile Multi-hop Relay (MMR) networks". J. Network and Computer Applications 36 (1): 91-102 (2013).

[7] D. Satishkumar, N. Nagarajan, "Simulation of Hard Hand over (HHO) Mechanism in IEEE 802.16 j Transparent Mode networks" International Journal of Computer Applications 14 (2), 35-39,2010.

[8] D. Satishkumar, N. Nagarajan, "An Improved Network Topology Acquisition process in IEEE 802. 16 j non-transparent mode relay networks" Journal of Discrete Mathematical Sciences & Cryptography 15 (1), 57-71, 2012.

[9] D. Satishkumar, N. Nagarajan "Analysis of Transparent and non-Transparent relay modes in IEEE 802. 16 j Mobile Multi-Hop relay networks" Journal of Discrete Mathematical Sciences & Cryptography 15 (1), 73-87, 2012.

[10] D. Satishkumar, N. Nagarajan "Problems faced in Communicate set up of Coordinator with GUI and Dispatcher in NCTUns network simulator", Computer Engineering and Intelligent Systems 2 (6), 61-71,2011.

[11] D. Satishkumar, N. Nagarajan "NCTUns Simulation model for IEEE 802.16 j Mobile multi hop Relay (MMR) WIMAX networks", Innovative Systems Design and Engineering 2 (5), 74-81,2011.

[12] D. Satishkumar, N. Nagarajan "Relay Technologies in IEEE 802.16 j Mobile Multi-hop Relay (MMR) Networks" Computer Engineering and Intelligent Systems 2 (3), 105-113, 2011.

[13] D. Satishkumar, N. Nagarajan "Simulation of Relay modes in IEEE 802.16 j Mobile Multi-hop Relay (MMR) WIMAX Networks", Innovative Systems Design and Engineering 2 (4), 75-84, 2011.

[14] D. Satishkumar, N. Nagarajan "A Survey of IEEE 802.16j Multi Hop Relay Based Wimax Networks, Journal of High Performance", Communication Systems and Networking: An International Journal, Volume .3 No.1, 2011, 9-14

[15] C. So-In, R. Jain, and A. Al-Tamimi, "Capacity evaluation for IEEE 802.16e MobileWiMAX," *J. Comput. Syst., Networks, and Commun.,*Vol. 2010, Apr. 2010.

[16] K. Wongthavarawat and A. Gains, "IEEE 802.16 based last mile broadband wireless military networks with quality of service support," in *Proc. Military Communications Conf.*, 2003, vol. 2, pp. 779–784.

[17] A. Sayenko, O. Alanen, and T. Hamalainen, "Scheduling solution for the IEEE 802.16 base station," *Int. J. Comp. and Telecommun. Netw.*,vol. 52, pp. 96–115, Jan. 2008.

[18] R. Jain, C. So-In, and A. Al-Tamimi, "System level modeling of IEEE 802.16e Mobile WiMAX networks: Key issues," *IEEE Wireless Comm.Mag.*, vol. 15, no. 5, pp. 73–79, Oct. 2008.

[19] A. Ghosh *et al.*, “Broadband Wireless Access with WiMAX /802.16: Current Performance Benchmarks and Future Potential,” *IEEE Commun. Mag.*, vol. 43, Feb. 2005, pp. 129–36.

[20] IEEE 802.16-2004, “Local and Metropolitan Networks — Part 16: Air Interface for Fixed Broadband Wireless Access Systems,” 2004.

[21] IEEE 802.16e-2005, “Local and Metropolitan Networks — Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum1,” 2006.

[22] Q. Liu, X. Wang and G. B. Giannakis, “A Cross-Layer Scheduling Algorithm with QoS Support in Wireless Networks,” *IEEE Trans. Vehic. Tech.*, vol. 55, no. 3, May2006, pp. 839–46.

[23] J. He, K. Guild, K. Yang, and H. Chen, “Modeling contention based bandwidth request scheme for IEEE 802.16 networks,” *IEEE Commun. Lett.*, vol. 11, no. 8, pp. 698–700, Aug. 2007.

[24] H. L. Vu, S. Chan, and L. L. H. Andrew, “Performance analysis of best-effort service in saturated IEEE 802.16 networks,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 460–472, Jan. 2010.

[25] Y. P. Fallah, F. Agharebparast, M. R. Minhas, H. M. Alnuweiri, and C. M. Leung, “Analytical modeling of contention-based bandwidth request mechanism in IEEE 802.16 wireless networks,” *IEEE Trans. Veh.Technol.*, vol. 57, no. 5, pp. 3094–3107, Sep. 2008.

[26] C. Cicconetti, A. Erta, L. Lenzini, and E. Mingozzi, “Performance evaluation of the IEEE 802.16MAC for QoS support,” *IEEE Trans. Mobile Comput.*, vol. 6, no. 1, pp. 26–38, Jan. 2007.

[27] Q. Ni *et al.*, “Investigation of bandwidth request mechanisms under point-to-multipoint mode of WiMAX networks,” *IEEE Commun.Mag.*, vol. 45, no. 5, pp. 132–138, May 2007.

[28] C. Mohanram, S. Bhashyam, “Joint subcarrier and power allocation in channel-aware queue-aware scheduling for multiuser ofdm”, IEEE Transactions on Wireless Communications 6 (9) (2007) 3208– 3213.

[29] G. Kulkarni, S. Adlakha, M. Srivastava, “Subcarrier allocation and bit loading algorithms for OFDMA based wireless networks”, IEEE Transactions on Mobile Computing 4 (6) (2005) 652–662.