Mobile WiMAX Network Security Threats and Solutions: A Survey

Vinod Kumar Jatav
Division of Information Technology
Indian Institute of Information Technology, Allahabad
Jhalwa, Allahabad (U.P.), India
vinodj217@gmail.com

Dr. Vrijendra Singh
Division of Information Technology
Indian Institute of Information Technology, Allahabad
Jhalwa, Allahabad (U.P.), India
vrijendra.singh@gmail.com

***Abstract*—IEEE 802.16 based WiMAX is an emerging wireless Internet technology. Salient features of WiMAX such as high speed internet facility over a long distance, quality of service, scalability, security, and mobility proves it better than Wi-Fi Internet access. Security is a vital requirement to prevent WiMAX network from the various attacks and to increase the reliability. This survey paper presents the threats associated with the layers in WiMAX along with possible solutions. The paper reviews the physical layer threats i.e. scrambling and jamming, MAC layer threats i.e. user authentication and data confidentiality, routing layer threats i.e. black-hole attack and other miscellaneous attacks e.g. Man-in-the-Middle (MITM), Denial of Service (DoS) and Bandwidth Spoofing. The paper observes that jamming attack and eavesdropping of management messages are the most destructive attacks for WiMAX network.**

Keywords-Mobile WiMAX, Security Attack, Privacy Key Management, Base Station, Mobile Station

I. INTRODUCTION

Worldwide-Interoperability for Microwave-Access (WiMAX) is an emerging wireless internet technology which provides higher data transmission rate up to 70 Mbps with a broad coverage of 30 miles. Broad coverage of WiMAX makes it suitable for Wireless Last Mile Technology. WiMAX apply point-to-point (PP) and point-to-multipoint (PMP) applications to provide its services [1]. It supports two type of transmission techniques Line-of-Sight (LoS) and Non-Line-of-Sight (NLoS). WiMAX aims to deploy Broadband Wireless Metropolitan Area Network (WMAN) [2] and integrates the benefits of broadband technology and Wi-Fi access. IEEE 802.16e (Mobile WiMAX) [4] supports the wireless connection of mobile devices, such as laptops, smart phones etc. Mobile WiMAX networks are also known as the Next Generation Networks (NGN). High bandwidth, quality of services, security, deployment ease, full duplex including DSL/cable, and low cost are the major strengths behind the popularity of WiMAX applications.

WiMAX Forum, a non-profit organization encourages IEEE 802.16 compliance and the interoperability [3].The IEEE 802.16 standards have been extended to gratify the growing demands and security for broadband wireless communication [8]. Table I shows the development phases of IEEE 802.16 extensions [7][9][10] from the beginning to last release.

TABLE I. EVOLUTION OF WIMAX STANDARDS

IEEE Std.	Year	Freq. Band	Specific Features
802.16	2001	10-66 GHz	Initial version of WiMAX based on the single-carrier physical layer and the burst TDM MAC layer [26]. Uses LoS towers to fixed locations.
802.16a	2003	2-11 GHz	Operates with NLoS (Lower freq. band can easily penetrate barriers. Max Transmission rate is 75 Mbps.
802.16c	2003	10-66 GHz	Broadband Wireless Access (BWA). Interoperability specification.
802.16d	2004	2-11 GHz	Based on 802.16a standard with some improvements and supports both TDD and FDD transmissions.
802.16e	2005	2-6 GHz	Mobile WiMAX supports mobile stations (MS). Operates with NLoS transmission, Multicast and broadcast services. Mobility support to 65 mph with data transfer rate up to 15 Mbps and coverage area of 1-3 miles. Privacy Sub-Layer for N/W security and Power saving modes for MS.
802.16f	2005	2-11 GHz	Introduces the mesh networking and Management Information Base. Ability to bypass obstacles, which improves the coverage area.
802.16g 802.16h 802.16i 802.16j 802.16k 802.16m	2007-2011	2-11 GHz	Management Planes Procedure and Services, Mobility at higher layer. Improved Coexistence Mechanisms for License Exempt Operation [19]. Mobile Management Info. Base. Multi-hop Relay specifications. Advance Air Interface (WiMAX2.0). Data transfer rate of 1Gbps for fixed subscribers and 100Mbps for mobile subscribers [18].

Fig. 1 shows the architectural model for a Mobile WiMAX network. Mobile WiMAX network architecture consists of the following components [6]:

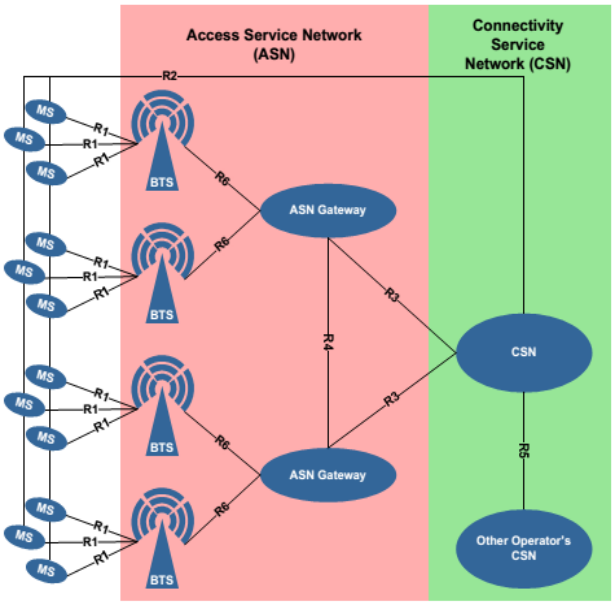

Figure 1. WiMAX architectural components.

- Mobile Subscriber Station (MS): MS is a mobile device used by the mobile subscriber to provide connectivity between subscriber equipment and base station equipment.
- Base Transceiver Station (BTS): BTS is known as BS which is an electronic device with a tower. Each BS provides large area coverage, also known as cell. Any wireless device located in the cell can access the internet. According to IEEE 802.16, the maximum radius of a cell is 30-mile [5].
- Access Service Network (ASN): ASN is a complete set of network functions that provide radio access to a subscriber. ASN includes DHCP addressing function, proxy AAA (Authentication, Authorization and Accounting) server, and other IP-based resources, including network management [6]. Radio access network is created by multiple ASNs and base stations. ASN is used in the handover process, mobility management, Quality of Service and radio resource management [7].
- Connectivity Service Network (CSN): The IP connectivity services to the subscribers are provided by CSN through the ASN [6]. The Network Service Provider (NSP) uses CSN for internet connectivity, management of IP addresses, authentication, authorization and roaming among the ASNs [7].

Rest of the paper is organized in the following manner: Section 2 presents an overview of WiMAX Layer architecture. Comprehensive survey of Mobile WiMAX network security attack/threat models and solutions have been reviewed in section 3. Section 4 contains the analysis part of the survey paper and discusses about the various kind of existing simulators for WiMAX. Finally, Section 5 concludes the survey paper followed by the references.

II. WiMAX Layer Architecture and Security

Fig. 2 shows the architecture of WiMAX protocol Layers.

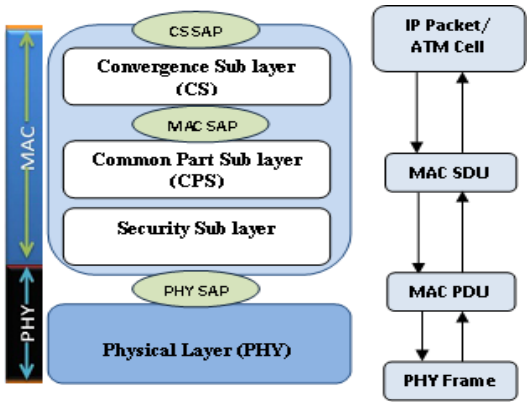

Figure 2. 802.16 Layer Architecture

A. *Physical Layer (PHY)*

Physical layer provides two-way mapping between MAC Layer PDUs and PHY layer frames [3]. Physical layer defines the transmission power and modulation-demodulation techniques.

B. *Medium Access Control Layer (MAC)*

MAC layer of WiMAX provides an edge between the network layer and the physical layer. MAC layer prepares MAC PDUs from the packets or ATM Cells received from the network layer. In addition, MAC Layer maintains the scheduling and multiple access connection [7]. Sub-Layers of MAC Layer are discussed below.

- Convergence Sub-Layer (CS): CS layer adapts data units (IP packets or ATM cells) from higher layers and prepares MAC Service Data Unit (SDU). Mapping between higher level data services to MAC layer service is also done by Service Access Points (SAP) at CS layer. [3].
- Common Part Sub-Layer (CPS): CPS defines the rules for system access, grant connection control, uplink scheduling, bandwidth request and allocation etc. CPS also handles MAC PDU construction, connection establishment and bandwidth management. MAC SAPs exchanges MAC SDUs with the CS layer. SPS is tightly incorporated with the Security Sub-Layer [3].
- Security Sub-Layer: Security Sub-Layer exchanges MAC PDUs with physical layer. This Sub-layer is responsible for the encryption/decryption of MAC SDUs and MAC PDUs including with authentication handling and secure key exchange.

Fig. 3 shows the security sub-layer of MAC for Mobile WiMAX. Security Sub-Layer of MAC [12] defines all the security specifications related to IEEE 802.16 standard.

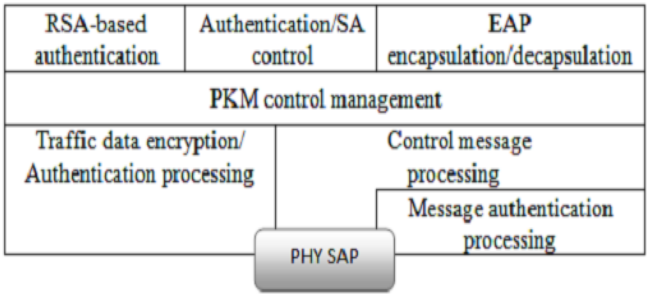

Figure 3. IEEE 802.16 MAC Security Sub-layer

Security Sub-Layer applies three steps to support WiMAX security; Subscriber Authentication (at the time of entry in to the network), Subscriber Authorization (if the subscriber is provisioned by the NSP), and then Encryption (for the secure key exchange and data traffic). Component Protocols at Security Sub-layer guarantee the authorization and confidentiality at the time of link establishment between the authorized parties (service provider and subscriber) [19].

- Encapsulation Protocol (EP): EP secures packet data across the IEEE 802.16d (fixed BWA) network. It defines a set of well defined cryptographic suites (pairs of data encryption and authentication algorithms) and protocol to apply those algorithms to MAC PDUs [20].
- Protocol for Key Management (PKM): PKM provides secure distribution of featured data from BS to SS. PKM helps SS and BS in the synchronization of featured data. PKM imposes restricted network access to the BS.

Security Sub-Layers of IEEE 802.16d [21] and IEEE 802.16e [4] states the security methods for fixed WiMAX and mobile WiMAX networks respectively. Fixed network uses protocol PKMv1 for security architecture and consist some of the security issues. Mobile WiMAX uses PKMv2 protocol which provides flexible solutions to the network security issues including with authentication for devices and subscribers between MSs and CSNs. PKMv2 authentication protocol is a 3-way hand shaking process, including with a confirmation message from MS to BS.

III. MOBILE WIMAX ATTACKS AND SOLUTIONS

WiMAX security issues and solutions have been discussed by many of the researchers in the past. Problems of 802.16d and the analysis of WiMAX security [23], Security issues and solutions for both PMP and mesh networks [24]. This section has categorized these researcher papers based on the nature of attacks and presents a comprehensive review with solutions.

A. Physical and MAC Layer Attacks

Threats associated with the physical layer and MAC layer are reviewed and ranked in [3] and are surveyed in [12]. An overview of the WiMAX security architecture has been discussed along with various kinds of threats at Physical Layer (scrambling and jamming) and MAC Layer (forgery attack) in [29][30]. Paper [2] examines the threats associated with both the layers of WiMAX and proposes some enhancements to the existing model to improve the performance of the encryption algorithms [2].

Solution: Paper [26] analyzes the security issues at physical layer in WiMAX and proposed a new method to solve the security issues using neural cryptography, which could generate a pair of secret keys through neural synchronization [26]. Research paper [28] introduced the scrambling attack at Physical layer in WiMAX networks and provided a prevention approach DCJS [27]. Table II briefs the attacks and countermeasures for WiMAX layer threats.

TABLE II. WIMAX LAYER THREATS *AND COUNTERMEASURES*

Layer	Attack	Countermeasure
Physical Layer	Jamming attack	Increase the power or bandwidth of signals
	Scrambling attack	Anomalies monitoring, DCJS [23]
	Water-Torture attack	Discarding bogus frames
	Forgery attack	Mutual authentication
	Replay attack	Mutual authentication
MAC Layer	MAC Management message in Initial Network Entry	Diffie-Hellman key agreement scheme
	Access Network Security	PKI based key exchange[46]
	MITM Attack	Diffie-Hellman key exchange protocol
	DoS Attack	Digital Signatures

B. Routing Layer Attacks in WMN

The Warm-hole attack using sinkhole attack at network layer of Relay WiMAX (IEEE 802.16j) is a severe attack [50].The performance of Black hole attack in WiMAX-WLAN interface network, with high impact with fewer efforts by intruder nodes is presented in [29][30]. Black Hole attack affects the performance of entire network like decrease the throughput and increase the packet drop or packet delay [29].

Solution: Paper [31] discusses the main solutions for routing security in Wireless Mesh Networks (WMN) and presents a model CONFIDENT comprising a novel way to characterize the effectiveness of such approaches. CONFIDANT is a secure routing protocol based on the DSR protocol in NS-2 simulator. Network Entry Process with Reliable Counter (NEPRC) scheme related threats have been presented in [32] along with an enhanced solution to detect and prevent the topological attacks including wormhole attacks and sinkhole attacks completely in WMN.

C. Security Sub-Layer and Encryption

An interdependent and open security plan has been proposed in [38], which offers a centralized management solution for the authentication, authorization and accounting part for a WiMAX network. Yang and Li has given an overview of the security issue on both the layers of WiMAX in their research paper [39]. Authentication, encryption, and availability security mechanisms along with security threats to WiMAX network have been discussed in [1]. Huang and

[16] have discussed about the security Sub-layer, Authorization Protocol, Key Management Protocol, Encryption and Security Issues in Multi-hop Communications for WiMAX.

Solution: Paper [40] compared the security mechanisms in authentication protocol (PKM). A comprehensive security frame-work for mobile WiMAX has been presented in [41] which uses public key certificates and HIBC. Implemented framework provides a complete, secure and efficient solution for stationary and mobile subscribers, compared to the proposed standard (PKMv2).

D. WiMAX Attacks based on Risk Level

Fig. 4 shows the list of WiMAX attacks based on their risk level [8] [33]:

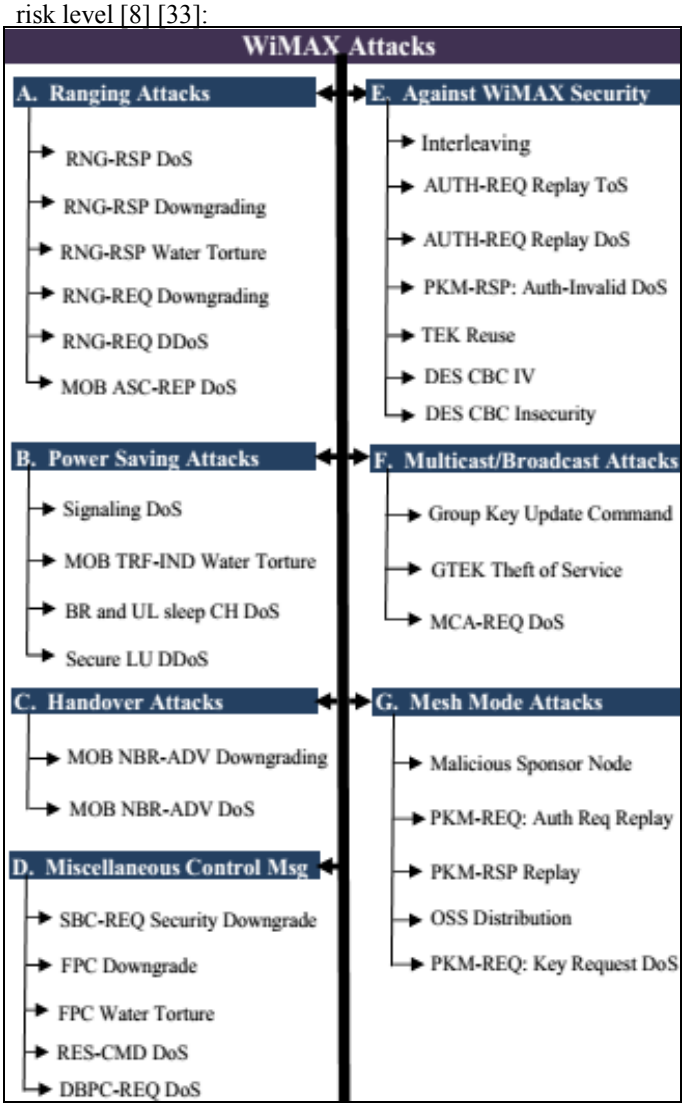

Figure 4. WiMAX Attacks

Paper [33] presents different security vulnerabilities found in IEEE 802.16e with possible solutions to eliminate them. Research paper [31] focuses on problems regarding fixed WiMAX network including with request and RNGRSP authorization.

Solution: Paper [8] provides a comprehensive taxonomy of attacks and countermeasures on 802.16 followed by a full-scale assessment study of indicative attacks that belong to broader attack classes. Each attack has been classified based on its type, occurrence, impact upon the system etc with possible countermeasures and remedies.

E. NSP Security Concerns

According to the white paper [6] presented by Motorola Incorporation, it is the responsibility of the NSPs to develop comprehensive security strategies for the design of secure network, policy, integration and operational security practices. Table III lists the major concerns related to WiMAX security for NSPs [6]:

TABLE III. WiMAX SECURITY CONCERNS FOR NSPs

Requirement	Threat	Description
Confident-iality	MITM	One-way or two-way impersonation between BS and MS.
Integrity	Privacy Compro-mise	Attacker captures real-time packets and does offline analysis to detect the management traffic information over physical links (wired or wireless).
	Theft of Service	Attacker MS (without proper authorization and online/offline auditing) accesses services with no payments.
Availability	Physical DoS	Disturbing of physical links (like jamming attack) disgraces the network services and performance.
	Protocol DoS	Injection of modified traffic control information can be used to tire out the resources and network performance.
	Replay	Repeatedly legitimate messages are inserted to drain network resources or to exclude legitimate MS.

F. MITM and DoS Attacks

Paper [22][34] presents an overview of Mobile WiMAX protocol layer and security scheme including with MITM attacks and DoS Service attacks.

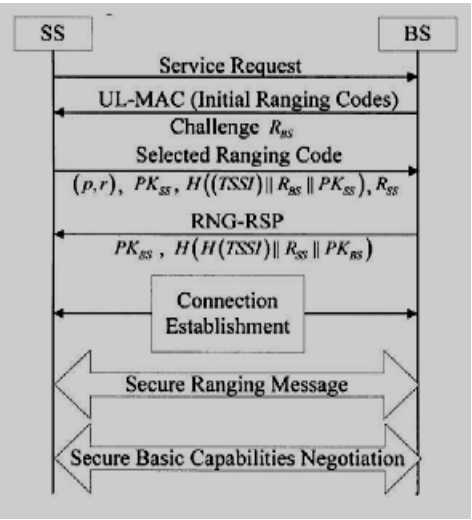

Figure 5. SINEP Model

Solution: Focusing on MITM and DoS attacks, a Diffie-Hellman key exchange protocol based model (SINEP) has been proposed in [22]. SINEP model shown in figure 5 reduces the possibilities of MITM attacks and defends against DoS attacks toward mobile WiMAX. The model used H parameter to detect DDoS attacks for the traffic generated in Mobile WiMAX Network. High amount transmission of RNG-REQ messages toward the Base Station introduces the DDoS attacks. An attacker node can misuse RNG-REQ messages to waste the resources of the network by changing some fields randomly and forwarding to the Base Station in bulk [36]. Simulation results of [36] show the statistical property variations among the normal and attack traffic patterns. Research paper [21] presents RNG-RSP message attack and concludes that it is vulnerable to DoS attack in WiMAX. A robust model ISNAP for DoS, MITM, and replay attacks has been presented in [35]. DoS attack traffic on the Wi-Bro network, logs generation and the trackbacking of the attackers has been analyzed in [37].

G. Miscellaneous Threats

A detailed literature review has been presented in [42] for WiMAX network vulnerabilities. Paper [15] proposes an algorithm for WiMAX network system to prevent fixed/mobile misbehavior node attacks. Analysis of BWA technology has been presented in paper [7]. It compares WiMAX technology with Wi-Fi and 3G internet technologies. Paper [6] discusses reference architecture for Mobile WiMAX Security. Paper [43] classified wireless attack on a system into four major classes: interception, fabrication, modification, interruption including with a fifth class of attacks repudiation. Ranking of these threats according to the level of risk is presented in [44].

IV. Analysis and Simulation Tools

Many of the security issues had already been fixed by the evolutionary development in 802.16 extensions, but still some security issues exist without any appropriate solution. Threats or vulnerabilities related to WiMAX layers have fascinated the concentration of researchers for gentle solutions. Threats like jamming, scrambling, water-torture, forgery, and replay attacks are of major consideration at WiMAX Physical layer. Critical threats at MAC layer of WiMAX are MAC management message eavesdrop, MITM and DoS attacks [5].

Some of the most well-known and widely used simulators have been taken in the consideration out of the research papers [5][36][51][52][53][54][55] viz. NS-2, NS-3, OPNET, Qualnet, Asset 3G/WiMAX, Winprop and NCTuns etc. OPNET Modeler Wireless Suite supports modeling and simulation of WiMAX Network [56]. It includes NGN architectures designing, application performance prediction, and development of scheduling schemes for BS and MS.

V. Conclusion

A wireless network system makes the use of an open and insecure radio channel with kind of security issues (traffic confidentiality, integrity) and network attacks [17]. Security plays a key role in the performance and reliability for WiMAX network. Implementation of top level security is highly required to lessen the threats in the network.

Like other wireless networks, WiMAX network is also uncovered to many of the security flaws at both the protocol layers i.e. Physical Layer and MAC Layer. This survey paper categorizes the security threats related to the WiMAX and presents them along with the proposed solutions for the ease of new researchers.

In future, the collaboration of multiple attacks/attackers may cause more severe results, if they are taken together.

References

[1] J. Qayyum, M. Lal, F. Khan, M. Imad, Survey & assessment of wimax, its security threats and their soltuions, International Journsal of Video & Image Processing and Network Security 11 (2011) 36–47.

[2] M. Habib, T. Mehmood, F. Ullah, M. Ibrahim, Performance of wimax security algorithm (the comparative study of rsa encryption algorithm with ecc encryption algorithm), International Conference on Computer Technology and Development, ICCTD'09., volume 2, IEEE, 2009, pp. 108–112.

[3] M. Barbeau, Wimax/802.16 threat analysis, in: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, ACM, 2005, pp. 8–15.

[4] I. L. S. Committee, et al., Ieee standard for local and metropolitan area 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 corrigendum 1, IEEE std 802 (2005).

[5] M. Chakraborty, D. Bhattacharyya, Overview of end-to-end wimax network architecture, WiMAX SECURITY AND QUALITY OF SERVICE (2010) 1.

[6] Paolini, Monica, and S. F. Consulting. "Building end-to-end WiMAX networks."Senza Fili Consulting (2007).

[7] M. S. Islam, M. T. Alam, Wimax: An analysis of the existing technology and compare with the cellular networks (2009).

[8] C. Kolias, G. Kambourakis, S. Gritzalis, Attacks and countermeasures on 802.16: Analysis and assessment (2013).

[9] S. S. Hasan, M. A. Qadeer, Wimax as a next generation wireless network, in: 2nd IEEE International Conference on Computer Science and Information Technology. ICCSIT., IEEE, 2009, pp. 485–489.

[10] R. K. Nichols, P. C. Lekkas, Wireless security, McGraw-Hill New York, 2002.

[11] H. Rashvand, Wimax cybercity & ngn, in: Proceedings of the International Conference on Mobile Technology, Applications, and Systems, ACM, 2008, p. 108.

[12] T. Nguyen, A survey of wimax security threats, Computer Science Department, Washington University , 2009.

[13] S. Katti, B. Krishnamurthy, D. Katabi, Collaborating against common enemies, Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement, USENIX Association, 2005, pp. 34–34.

[14] S. Chen, J. Xu, Z. Kalbarczyk, K. Iyer, Security vulnerabilities: From analysis to detection and masking techniques, Proceedings of the IEEE 94 (2006), pp. 407–418.

[15] R. K. Jha, I. Z. Bholebawa, U. D. Dalal, A. V. Wankhede, Detection and fortification analysis of wimax network: With misbehavior node attack, Int'l J. of Communications, Network and System Sciences, 2012,pp. 353–367.

[16] C.-T. Huang, J. M. Chang, Responding to security issues in wimax networks, IT Professional, 2008, pp. 15–21.

[17] L. Cuilan, A simple encryption scheme based on wimax, International Conference on E-Business and Information System Security, EBISS'09. IEEE, 2009, pp. 1–4.

[18] M. Habib, M. Ahmad, A review of some security aspects of wimax and converged network, 2nd International Conference on Communication Software and Networks. IEEE, 2010, pp. 372–376.

[19] M. Bogdanoski, P. Latkoski, A. Risteski, B. Popovski, Ieee 802.16 security issues: a survey (2008).

[20] D. Ourston, S. Matzner, W. Stump, B. Hopkins, Coordinated internet attacks: responding to attack complexity, Journal of Computer Security, 2004, pp. 165–190.

[21] I. . W. Group, et al., Ieee standard for local and metropolitan area networks, part 16: Air interface for fixed broadband wireless access systems, IEEE Std 802, 2004, pp. 16–2004.

[22] T. Shon, W. Choi, An analysis of mobile wimax security: vulnerabilities and solutions, Network-Based Information Systems, Springer, 2007, pp. 88–97.

[23] D. Johnston, J. Walker, Overview of ieee 802.16 securit y, Security & Privacy, IEEE , 2004, pp. 40–48.

[24] P. Rengaraju, C.-H. Lung, Y. Qu, A. Srinivasan, Analysis on mobile wimax security, Toronto International Conference on Science and Technology for Humanity (TIC-STH), IEEE, 2009, pp. 439–444.

[25] S. S. Hasan, M. A. Qadeer, Security concerns in wimax, First Asian Himalayas International Conference on Internet, AH-ICI'09., IEEE, 2009, pp. 1–5.

[26] D. Hu, Y. Wang, Security research on wimax with neural cryptography, International Conference on Information Security and Assurance, ISA'08., IEEE, 2008, pp. 370–373.

[27] M. Barbeau, J. Hall, E. Kranakis, Detecting impersonation attacks in future wireless and mobile networks, Secure Mobile Ad-hoc Networks and Sensors, Springer, 2006, pp. 80–95.

[28] P.-W. Chi, C.-L. Lei, A prevention approach to scrambling attacks in wimax networks, IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks & Workshops, WoWMoM'09., IEEE, 2009, pp. 1–8.

[29] H. Yu, M. Kaminsky, P. B. Gibbons, A. Flaxman, Sybilguard: defending against sybil attacks via social networks, ACM SIGCOMM Computer Communication Review , 2006, pp. 267–278.

[30] B. M. Lail, V. Foreword By-Chang, Broadband network & device security, McGraw-Hill, Inc., 2002.

[31] V. Lima, V. Ruivo, M. Curado, Securing wireless mesh net works: a winning combination of routing and forwarding mechanisms, Proceedings of the 5th International Latin American Networking Conference, ACM, 2009, pp. 11–17.

[32] J. Cao, M. Ma, M. A. B. Ariff, Security enhancements in wimax mesh networks, 4th IEEE International Conference on Broadband Network and Multimedia Technology (ICBNMT), IEEE, 2011, pp. 572–578.

[33] A. Deininger, S. Kiyomoto, J. Kurihara, T. Tanaka, Security vulnerabilities and solutions in mobile wimax, Int. Journal of Computer Science and Network Security (IJCSNS), 2007, pp. 7–15.

[34] H. Yang, F. Ricciato, S. Lu, L. Zhang, Securing a wireless world, Proceedings of the IEEE , 2006,pp. 442–454.

[35] R. M. Hashmi, A. M. Siddiqui, M. Jabeen, K. Shehzad, A. Zubair, K. Alimgeer, Improved secure network authentication protocol (isnap) for ieee 802.16, International Conference on Information and Communication Technologies (ICICT'09), IEEE, 2009, pp. 101–105.

[36] J. R. Douceur, The sybil attack, in: Peer-to-peer Systems, Springer, 2002, pp. 251–260.

[37] D. Pareek, Economics of wimax, The Business of WiMAX, 173–210.

[38] H. Yu, P. B. Gibbons, M. Kaminsky, Toward an optimal social network defense against sybil attacks, Proceedings of the twenty-sixth annual ACM symposium on Principles of distributed computing, ACM, 2007, pp. 376–377.

[39] Y. Zhang, H.-H. Chen, Mobile WiMAX: Toward broadband wireless metropolitan area networks, CRC Press, 2007.

[40] K. Sameni, N. Yazdani, A. Payandeh, Analysis of attacks in authentication protocol of ieee 802.16 e, Int. J. Com. Net. Tech , 2013, pp. 33–44.

[41] M. Rodoper, A. Baliga, E. Jung, W. Trappe, An efficient security framework for mobile wimax, Proceedings of the 27th Annual ACM Symposium on Applied Computing, ACM, 2012, pp. 1494–1501.

[42] R. Jha, U. D. Dalal, A journey on wimax and its security issues, International Journal of Computer Science and Information Technologies, 2010, pp. 256–263.

[43] F. Ohrtman, K. Roeder, Wi-Fi Handbook: Building 802.11 b Wireless Networks, volume 67, McGraw-Hill, 2003.

[44] M. Nasreldin, H. AsIan, M. El-Hennawy, A. El-Hennawy, Wimax security, 22nd Int. Conference on Advanced Information Networking and ApplicationsWorkshops (AINAW).,IEEE, 2008, pp. 1335–1340.

[45] A. Kaushik, Mobile wimax security, architecture and assessment, International Journal of Electronics and Computer Science Engineering (IJECSE, ISSN: 2277-1956), 2012, pp. 07–14.

[46] B. Bhargava, Y. Zhang, N. Idika, L. Lilien, M. Azarmi, Collaborative attacks in wimax networks, Security and Communication Networks, Wiley InterScience, 2009, pp. 373–391.

[47] http://www.dshield.org.

[48] S. Cheung, U. Lindqvist, M. W. Fong, Modeling multistep cyber attacks for scenario recognition, in: DARPA Information Survivability Conference and Exposition, 2003. Proceedings, volume 1, IEEE, 2003, pp. 284–292.

[49] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, R. Govindan, Cossack: Coordinated suppression of simultaneous attacks, in: Proceedings of DARPA Information Survivability Conference and Exposition, volume 1, IEEE, 2003, pp. 2–13.

[50] V. K. Jatav, M. Tripathi, M. S. Gaur, & V. Laxmi, (2012, February). Wireless Sensor Networks: Attack Models and Detection. In 2012 IACSIT Hong Kong Conferences, IPCSIT vol. 30 (2012)©(2012) IACSIT Press, Singapore

[51] A. Andreadis, S. Rizzuto, R. Zambon, A new ns2 tool to inv estigate qos management over mobile wimax, Proceedings of the 4th International Conference on Simulation Tools and Techniques, ICST, 2011, pp. 240–248.

[52] J. Farooq, T. Turletti, An ieee 802.16 wimax module for the ns-3 simulator, Proceedings of the 2nd International Conference on Simulation Tools and Techniques, ICST, 2009, p. 8.

[53] N. Chauhan, R. K. Yadav, Security analysis of identity based cryptography and certificate based in wimax network using omnet++ simulator, in: 2nd International Conference on Advanced Computing & Communication Technologies (ACCT), , IEEE, 2012, pp. 509–512.

[54] J. F. Borin, N. L. da Fonseca, Simulator for wimax networks, Simulation Modelling Practice and Theory, 2008, pp. 817–833.

[55] S.M. Huang, Y.C. Sung, S.Y. Wang, Y.B. Lin, Nctuns simulation tool for wimax modeling, Proceedings of the 3rd international conference on Wireless internet, ICST, 2007, p. 20.

[56] https://www.opnet.com/solutions/brochures/R&D_Defense.pdf