Indian Journal of Science and Technology, *Vol 11(19), DOI: 10.17485/ijst/2018/v11i19/122659,* May 2018 *ISSN (Print) : 0974-6846*
ISSN (Online) : 0974-5645

Simulation of a Novel Authentication Scheme to Solve DoS Attack in Mobile WiMAX

Reena Dadhich[1], Geetika Narang[2] and D. M. Yadav[3]

[1]University of Kota, Kota – 324005, Rajasthan, India; reena.dadhich@gmail.com
[2]Vansthali Vidyapith, Vanasthali - 304022, Rajasthan, India; teenabagga18@gmail.com
[3]College of Engineering, Malegaon, Pune – 413115, Maharashtra, India; dineshyadav@gmail.com

Abstract

Objectives: Main Objective of this research is towards the avoidance of Denial of Service (DoS) Attack in Mobile WiMAX. For this a secure authentication mechanism is required and we present a highly secure authentication mechanism. It gives a mutual authentication between Client and Server and the server resources would consume less. **Methods/Statistical Analysis:** For implementation of this secure authentication, a puzzle approach has been used wherein a puzzle is sent by Base Station to Mobile Station. Unless and until the client do not solve this puzzle, server will not verify its certificates. For the implementation of this work, NS-2 as a simulator, has been used. Where three scenario have been implemented: 1) normal current working scenario of Mobile WiMAX, 2) DoS attack have been simulated without puzzle approach and 3) when under DoS attack with puzzle approach implementation. **Findings:** The proposed puzzle approach shows an increase of overall throughput of network as compared to the existing report and also the number of secure packets are increasing. It is because of the probability of unauthenticated user becomes almost negligible. **Application/Improvements:** This research work can be helpful in any of the working environment where security is the most important concern as in the case of defense where availability of network and security of network is always at the highest priority.

Keywords: Base Station, Connectivity Service Network, Denial of Service, Puzzle, 802.16e

1. Introduction

Today's era demands the fast and reliable service, and the Broadband Wireless subscribers demand for uninterrupted and high-speed services. 4G is promising as we able to provide such high speed. 4G is based on two core technologies: LTE (Long-Term Evaluation) and Mobile WiMAX (Worldwide Interoperability for Microwave Access). LTE and Wi-MAX system architectures are optimized for data transference. These technologies can provide higher data rate traffic in comparison to Cellular system's architecture. It provides improved respond time and reliability both of these be the all-IP backbone. These new network architectures benefit not only the subscribers but also the mobile wireless operators[1], but their applications area is different. Like LTE mainly focuses on Mobile subscribers where the motive of WiMAX is to implement Wireless Metropolitan area network. Following are the major components used in WiMAX network as shown in Figure 1.

1.1 CSN Server

These servers actually acts as backbone server in the architecture of WiMAX. Ultimately these servers are responsible for giving the IP connectivity to the clients which can be any mobile device or any other kind of subscriber. Because of it, the role of CSN can be seen with all Internet service Providers. Here, it is the duty of CSN

**Author for correspondence*

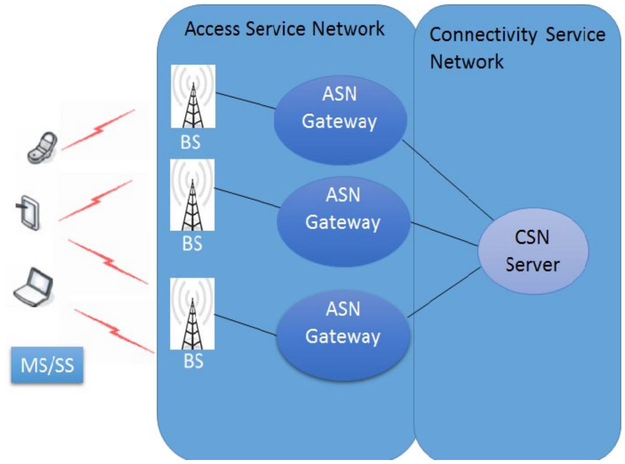

Figure 1. *WiMAX Network Architecture*[1].

server to allot IP address, doing the verification in terms of authentication and authorization. It also manages network switching of any subscriber between multiple ASNs.

1.2 The client as MS/SS

In WiMAX role of the client means Subscriber station or Mobile Station. These clients can exist as of multiple devices like Smartphone, Laptop, Tablet and much more.

The server as BS: Role of the server is performed by Base Station (BS) also called as BTS which stand on Base Transceiver station. Base Station is an electronic device having a tower. Every BS covers a vast range, which is called as Cell. Any Mobile station or Subscriber station situated in the cell can get access to that Base station network. The maximum range of cell in WiMAX is about 30 mile.

1.3 Access Service Network (ASN)

ASN provides some network functions to its client including IP address allocation by the use of Dynamic host configuration protocol service. It also acts as a proxy server between Client and CSN server. It does the work of doing the Authentication, Authorization, and Accounting and called ass AAA server. It also performs the work of network management of IP-based resources. Number of Access Service Network and Base Station forms a whole Radio Access Network

It also plays an important role at the time of handover procedure, versatility administration, Quality of Service and radio asset administration.[2]

2. Related Theory

2.1 Introduction

Mobile WiMAX is the version of WiMAX with Mobility feature. The architecture of WiMAX network is similar to Cellular architecture.[2,3] It has been deployed not only to provide the service in an urban area but also to a rural area. Figure 2 represents the topology of WiMAX wherein one or more Base station along with a number of Mobile station together configures WiMAX. Configuration is in Line of Sight or Non-line of Sight; this depends on which version of IEEE 802.16 standard is used. If network range has to be increased, then Repeater stations are denoted as RSs are used.[4]

WiMAX with its mobility feature makes possible for the user to access broadband service even if at the speed of 120 Km/h and this version called as Mobile WiMAX which as per its name provide mobility facility to its subscribers. IEEE 802.16e not only provides the mobility, but also date rate increased from 40 Mbps (supported by IEEE 802.16d) to 75 Mbps.[5]

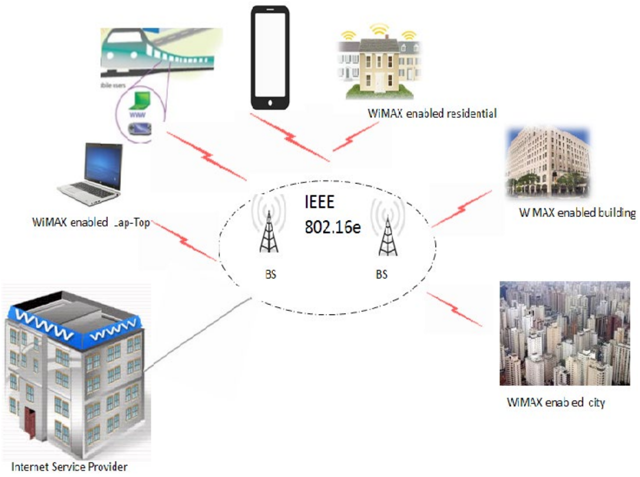

Figure 2. WiMAX network topology[6].

2.2 Mobile WiMAX

As, per the physical layer characteristics of WiMAX, it works on frequency ranges from 2-6 GHz. It works in Non-line of sight mode. Its cell radius is 2-7 km[4]. It uses Quadrature Amplitude Modulation, which provides higher data rate as compared to Amplitude modulation or phase modulation. And for efficiently using the spectrum bandwidth and to provide minimal co-channel interference it uses OFDMA which stands on orthogonal frequency division multiple Accesses. Also, to allow asymmetric traffic and for providing flexible bandwidth allocation, it supports Time Division Duplexing.

Key features of IEEE 802.16

OFDMA: -
OFDMA is one of the key features of IEEE 802.16, which gives maximum use of spectrum because of its overlapping feature. OFDMA uses Fast Fourier Transformation technique because of which it becomes more efficient for doing modulation.

Supports higher data rates:-
IEEE 802.16 supports higher data rates because of physical level configuration component like the use of QAM, OFDMA, MIMO antenna which improves the reception of Space-Time Code transmitted signals.

Robust quality of Service: -
IEEE 802.16e provides the quality of service (QoS), it can be analyzed from its Medium Access Control Architecture (MAC) architecture.

Scalability: -
Mobile WiMAX provides the flexibility as well as scalability regarding spectrum allocation because it uses an additional feature of OFDMA called S-OFDMA. Where 'S' signifies the word Scalability. IEEE 802.16e is capable of operating from 1.25 to 20 MHz spectrum worldwide.

Mobility: -
IEEE 802.16 ensures to provide optimized handover scheme when the subscriber moves from one Base Station coverage area to other Base station range. Its handover scheme works with latencies less than 50 ms.

3. Security in Mobile WiMAX

Security is an important concern in any of the network and becomes more critical in a wireless environment. For secure data transmission in WiMAX, it uses Advance Encryption Std. AES is used, but encryption is used after the authentication is performed, but although attack can occur before that.

3.1 Security Process for IEEE 802.16e

The process of WiMAX Security is divided into three steps[6] as shown in Figure 3. PKM which stands on Privacy key management protocol is used in WiMAX. It provides three types of authentication:1) RSA (Rivest-Shami-Adleman) where X.509 digital certificates are used. These certificates are handover to Mobile stations from their manufacturer. So, for authentication BS request to Mobile Station for providing this certificate[7]. 2) *Extensible Authentication Protocol authentication or called EAP,* where not only the use of X.509 is supported but also by other authorizations proof like SIM (Subscriber Identity Module) is acceptable. *3) The combination of previous two,* after applying RSA, for more secure authentication EAP is also performed.

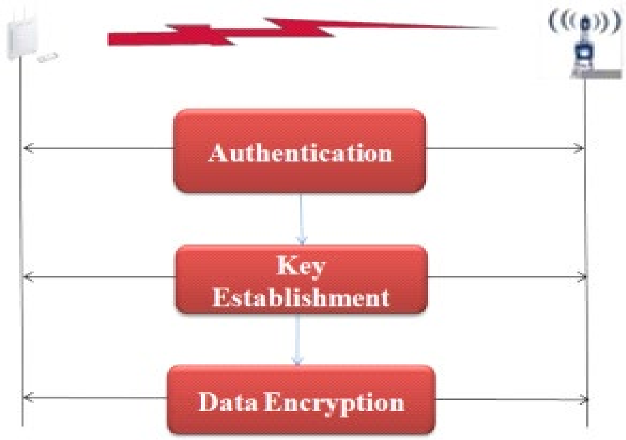

Figure 3. Security Framework for IEEE 802.16e[4].

Once authentication is completed at Key Establishment phase occurs where both sides share an Authentication key. This phase is also called as Data key exchange because this is the key after which only data transference occurs.

After key exchange Data, encryption phase takes place, where the use of AES algorithm occurs. Plain text is converted to cipher text which is sent over the network and receiver by the use of shared key decrypt the ciphertext to get the original text[8].

Proposed Research presented in this paper is related to the attack called as DoS which mainly occurs at the Authentication stage. Under Denial of Service attack, the client sends multiple forged requests to Server. In IEEE 802.16e, forged MS acts as a client and makes BS busy in attending illegitimate requests. Moreover, BS becomes unable to give service to its legitimate Subscriber and leads toward Denial of service attack or called as DoS. Also some time DoS occurs when attacker snoops credentials of an MS and uses it to send multiple requests to BS. In this case, BS has to ignore multiple requests even from authenticated user and again leads toward DoS attack.

Proposed Research work provides two-way security which means neither Base Station can be an illegitimate or Mobile station. The solution is based on puzzle approach along with additional encryption mechanism.

3.2 Security Flaws in IEEE 802.16e

Messages for Authentication

Messages which are related to authentication, are encrypted using Hash Based message authentication code or Cipher-based authentication code. But there are some messages which are not under the authentication but are crucial which introduces vulnerability.

Even, by the use of broadband management connection number of management messages is sent[9].

Request Messages

This message is also unauthenticated. This Message plays a major role because of being used by Base Station at the time of eliminating any Mobile station from a polling group. Whenever a Mobile station gets this kind of message, then MS deletes itself from polling group. Actually, this polling group is used to allow Bandwidth to Mobile stations.

Again if these messages would not be encrypted, then an attacker can send this kind of fake messages to MS, which will result in removal of that MS from the network itself. Fake data having information related to neighbor BS can also be sent by the attacker.

Ranging Request Messages

These Ranging Request messages are used at the time of Initial network entry, and for this no authentication key is available. To provide security the message digest must be used here as if authentication key is present. Addition to these there are messages which are also not encrypted, but information carried by those messages are comparable less crucial for the operability of the protocol.

4. Algorithm Design

This study proposed an Algorithm which can effectively and efficiently work in the 802.16e environment. While designing, the very first challenge was to design the algorithm in such a way that can provide two-way security i.e. neither BS nor MS can be illegitimate. After doing the Literature Survey, it is observed that, although security in terms of data encryption and PKI is provided, but still threats are there and are more crucial at the time of authentication. Similar observations have also been observed by others[10,11]. Solutions provided in the literature like Third-party Server, Diffie-Hellman with some modification or Visual cryptography does not show the noticeable results. However, while designing the various algorithm strategies proposed by authors in above techniques were very useful, like Use of Time Stamp, Digital signature, encryption, etc. Our algorithm also uses these techniques but along with a different strategy i.e. Puzzle Approach where a puzzle, as well as the solution of puzzles, are stored at Base Station. Whenever an MS or SS wants to be authenticated from BS, it has to solve a puzzle. It has been taken care that Puzzle would be designed in such a way that it would be able to solve only by legitimate users. Also with the help of two-way puzzle security has been implemented so, neither MS nor BS can play an illegitimate role.

4.1 Algorithm

Designed algorithm is having three entities MS, BS, and Certification Authority (CA)[12]. Mobile Station will initiate communication as per following Steps.

Step 1. Both Mobile Station and Base Station will be preloaded with a table of puzzle having I_1, I_2, I_3, I_4… I_n of 64 bit.

Step 2. Subscriber and Base Station will share a decryption key K of 64 bit out of which 56 bits are used.

Step 3. After setting up the network whenever a subscriber will come in the range of Base Station, it will Send INIT_REQ.

Step 4. BS will pick a random string/puzzle from I_j its pool of puzzle.

Step 5. BS will encode as E_j.

Step 6. MS will receive the puzzle E_j.

Step 7. The puzzle will be decoded at BS by K and will obtain I_j.

Step 8. MS will find the solution correspondence to I_j.

Step 9. MS sends S_j and MS_{ID} and MS_{DS} to BS.

Step 10. BS verifies solution and sends MS_{ID} and MS_{DS} to Certification Authority for Verification.

Step 11. BS sends a Positive or Negative acknowledgment to MS.

Step 12. If authenticated then BS and MS can do data transmission else not.

5. Implementation and Result

For simulation, we could have various options like Qualnet, Opnet, Omnet+ and Ns-2. However, out of these NS-2 was opted which is most widely used for research purposes. The reason behind this popularity of NS-2 is its strong features; it is the only open Source tool which can provide the environment of simulating the wireless network along with its supporting protocols. Simulation (Table 1) has been used while applying the proposed technique.

Table 1. Simulation Parameter

PARAMETER	USED IN SIMULATION
Simulator	NS-2.35
Channel Type	Channel/Wireless Channel
Antenna Type	Omnidirectional
Radio-Propagation model	Propagation/OFDMA
Network interface type	Phy/WirelessPhy/OFDMA
Link Layer Type	LL
MAC Type	MAC/802_16
Routing Protocols	DSDV
X dimension	2000
Y dimension	2000
Traffic type	Constant Bit Rate (UDP)
Packet Size	1500,2500 Bytes

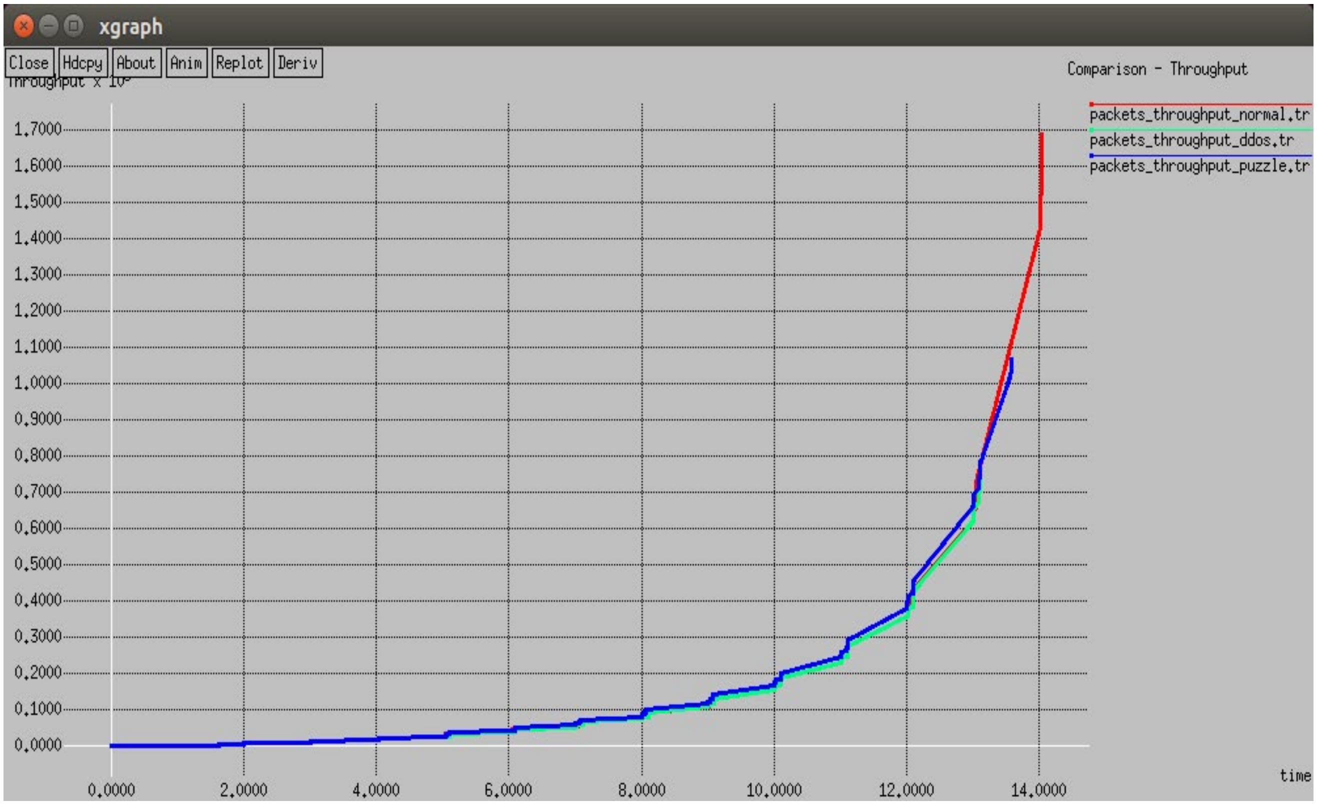

Figure 4. Throughput comparison in three scenarios. First, the red line indicates throughput in normal condition without any attack. The green line indicates throughput under Denial of Service (DoS) attack and the blue line indicates throughput after implementing puzzle approach. Where throughput has been calculated by applying formula Throughput = Total number of Request / Accepted request.

Figure 4 shows a Throughput comparison between the proposed approach and without it. The results shows that the Throughput increases from 0.6 Kbps to 1.1 Kbps. Figure 5 is related to Packet Delivery ratio (PDR) which is signifying that PDR with proposed approach is around 78% under DoS attack which is more than 70% of PDR without DoS attack and 65% with DoS attack. Figure 6 is related to secure transmission vs Unsecure Transmission which shows number of secure transmission packet is around 75 whereas few unsecure transmission is 35.

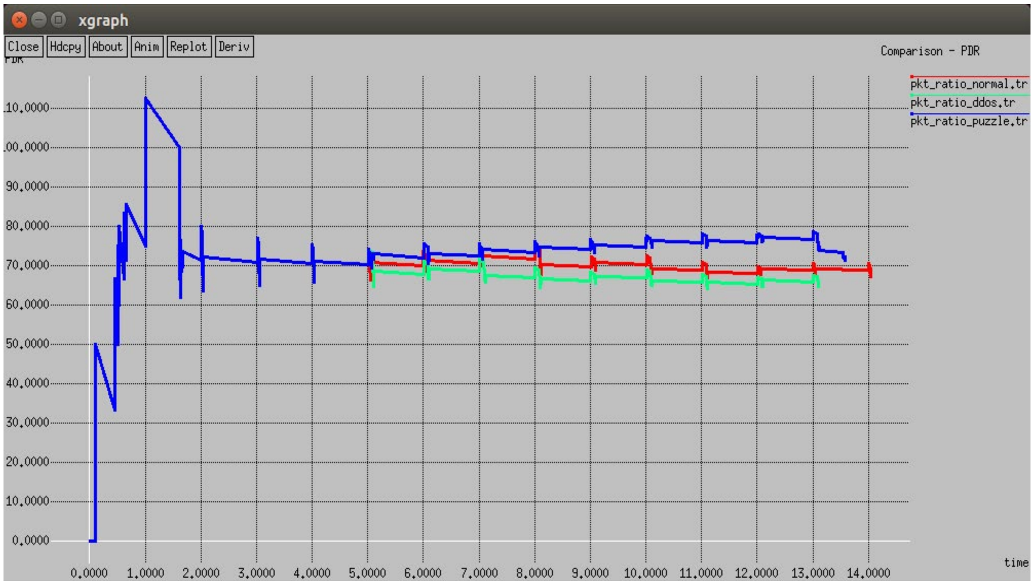

Figure 5. A Packet Delivery Ratio (PDR) comparison in three scenarios. First, the Blue line indicates highest PDR after implementing puzzle approach, Red line indicates (PDR) in a normal condition without any attack, the Green line indicates the lowest PDR when under Denial of Service (DoS) attack.

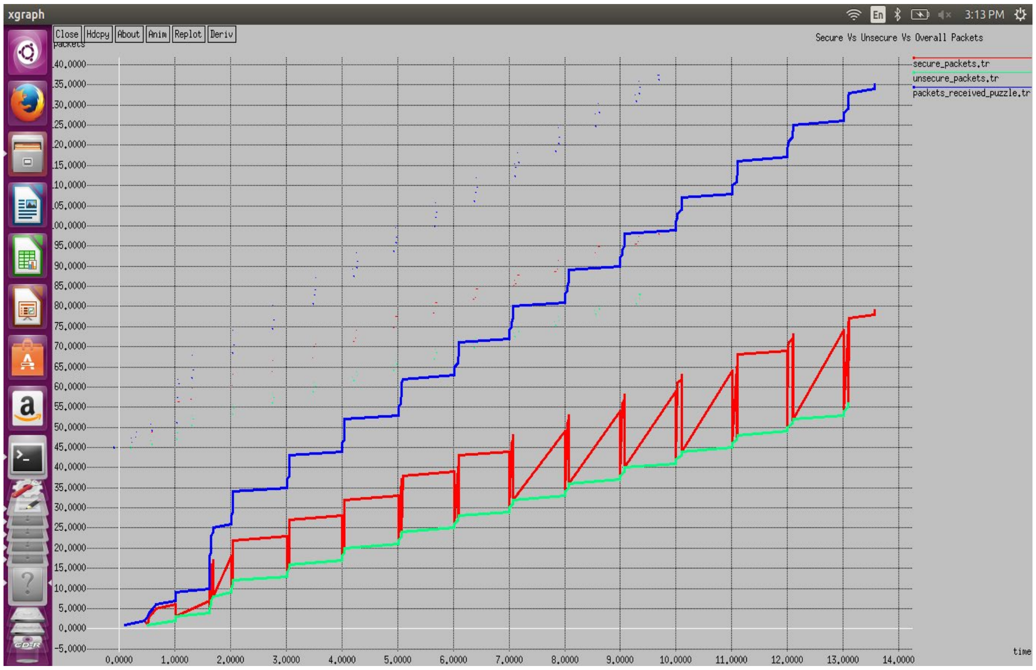

Figure 6. Packet transmission scenarios under puzzle approach. The Blue line indicates total packet transmission; Red line indicates secured transmission which is much higher as compare to the green line which indicates unsecured transmission.

6. Conclusion

Authentication is the most crucial phase in any of the applications. It is more prone to attacks when authentication is on to the network. In Mobile WiMAX too where users are using Broadband service definitely expect highly secure authentication mechanism. This paper proposed a solution for such a secure authentication. It provides a mutual authentication where neither MS nor BS can be illegitimate. It is a puzzle based mechanism. The BS sends a puzzle to the subscriber which is supposed to be solved only by the legitimate subscriber. As a correct result would always be present in the legitimate subscriber database. A correct solution of Puzzle indicates to Base Station that subscriber is genuine. Also a correct puzzle intimates the subscriber that comes from the legitimate Base station.

7. References

1. Fuden T, Anjali S. A Review of Privacy and Key Management Protocol in IEEE 802.16e. International Journal of Computer Applications. 2011; 20(2):1–7.
2. Introduction to Wireless MIMO Theory and Applications. Available from: crossref. Date accessed: 15/11/2006.
3. Bart S. Security issues and proposed solutions concerning authentication and authorization for WiMAX (IEEE 802.16e). Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente, the Netherlands; 2008. p. 1–7.
4. Seok-Yee T, Peter M, Hamid RS. WiMAX Security And Quality of Service. 1st Edition. John Wiley & Sons Ltd; 2010.
5. John KHH, Mohamad YAlias, Bok-Min G. Simulating Denial of Service Attack Using WiMAX Experimental Setup. International Journal of Network and Mobile Technologies (IJNMT). 2011; 2(1):30–5.
6. Guide to Securing WiMAX Wireless Communications. Available from: crossref. Date accessed: 30/09/2010.
7. 802.16 Working Group info from IEEE-SA.IEEE 802.16 Published Standards and Drafts; 2005. p. 1–16.
8. Tao H, Ning Z, Kaiming L, Bihua T. Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions. In 5th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems; 2008. p. 828–33.
9. Frank AI. Security Issues in Mobile WiMAX (IEEE 802.16e). Proceedings of the IEEE conference on Mobile WiMAX; 2009. p. 117–22.
10. Gaurav S, Sandeep K. Analysis of security issues of mobile WiMAX 802.16e and their solutions. International Journal of Computing and Corporate Research. 2011; 1(3):1–24.
11. Ismat A. LTE and WiMAX: Comparison and Future Perspectives. Computer Science & Communications. 2013, 5 (4), pp. 360-368.
12. Jihyuk C, Sang-Yoon C, Diko K, Yih-Chun H. Secure MAC-Layer Protocol for Captive Portals in Wireless Hotspots. IEEE International Conference on Communications (ICC); 2011. p. 1–5.