IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. IX (May-Jun. 2014), PP 80-86
www.iosrjournals.org

"WiMAX-WLAN Interface usingTORA, DSR and OLSR protocols with their evaluation under Wormhole Attack on VOICE and HTTP applications"

Sharanbeer Kaur [1], Shivani Khurana [2]
[1](Research Scholar (CSE), CT Institute of Technology/ PTU, INDIA)
[2](Assistant Professor (CSE), CT Institute of Technology/ PTU, INDIA)

Abstract: *We are in advanced world of internet with new technologies in now these days. So many new wireless networks technologies have been emerged. WiMAX is one of the advanced technologies from those. Due to advancement, the security related issues has also been increased in this technology. Information Security has become one of the challenging and important tasks to maintain the confidentiality, integrity and availability of the information. This paper is all about the security of WiMAX technology. During the research we learn that there are several security related threats and attacks in this technology by which the adversary can perform several malicious activities. We also found some security methods which can be applied against several security related threats and attacks. The scope of this paper is to research the security related issues in the WiMAX technology and find the possible security solutions against that issues.*

Keywords: *Authentication, Encryption, HTTP, VOICE, WiMAX Security, WiMAX-WLAN Interface, WiMAX threats/Attacks.*

Organization of sections: Section 1 *is all about the abstract and brief introduction to WiMAX and WLAN technologies.* ***Section 2*** *will describe the standards of two technologies i.e. WiMAX and WLAN.* ***Section 3*** *will include the experimental setup of integrated scenarios that is with and without attack.* ***Section 4 will*** *describe the results which we get after simulations.* ***Section 5*** *concludes the paper. Moreover it is about some discussions and future directions.* ***Section 6*** *is about the references and bibliography.*

I. Introduction

Wlan: Productivity and convenience has dramatically increased by WLAN due to the distribution of high speed internet access from cables, DSL (Digital Subscriber Line) and other fixed broadband connections within wireless hotspots. At present million of offices, homes and public locations such as hotels, cafes, and airports are provided with higher WLAN connections.

Wimax: WiMAX as an extension to WLAN is taking Wireless Internet Access to the next level and with the increase of time; it would have been achieving similar attach rates to devices as WLAN. WiMAX can be considered as an extension to WLAN and can deliver internet access miles away from the nearby WLAN and blanket large areas i.e. WANs.

WLAN / Wimax Synergies: Wireless broadband connectivity is provided by both the wireless technologies i.e. WiMAX and WLAN and both have been optimized for different usage models i.e. WLAN for high speed connectivity and WiMAX for high speed and large range connectivity. By combining WiMAX and WLAN technologies a more complete suite of broadband services can be offered by service providers. Below table is depicting that how WLAN and WiMAX are complimenting each other by taking two perspectives i.e. Implementation and Deployment. (10)

II. Standards

WLAN comes under IEEE 802.11 standard and WiMAX comes under the family of IEEE 802.16. IEEE 802.11n standard is the new high-throughput extension which is designed for digital home and office applications. On the other hand to support Wide Area Mobility, IEEE 802.16e-2005 is established or enhanced from IEEE 802.16e-2004 via scalable OFDMA. Both the technologies i.e. WiMAX and WLAN uses IP based technologies.

III. Wimax And Wlan Comparison[1]

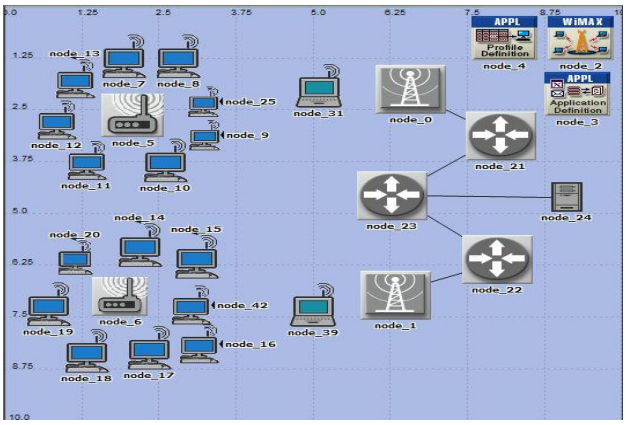
Wi-FI IEEE802.11(a/g/n)	**WiMAX (IEEE802.16e-2005)**	**Synergy Impact**
Market		
Deployed in local coverage areas, such as public hotspot, home and business.	Deployed in wide coverage areas, including metro politan areas for mobile broadband wireless as well as Rural or remote areas for Last mile connectivity And portable services.	"Best connected" model user connects to WiMAX or Wi-Fi depending on their location coverage and QoS requirements.
Products certified by the Wi-Fi Alliance.	Products certified by the WiMAX Forum.	Interoperable clients and access points enable global roaming and multi-vendor competition.
Embedded in 97% of laptops and many handheld and CE Devices.	Customer Premise Equipment (CPE) and PC cards available today; embedded in laptops and handheld devices starting in 2008.	Integration into devices is expected to reduce device subsidies and lower Cost Per Gross Add (CPGA). 6
Characteristics		
Provides fixed and portable solutions.	Provides fixed and portable solutions	Full range of services in the home and office, as well as on the road.
Operates in license- exempt spectrum. Current solutions use the 2.4 and 5 GHz bands.	Operates in licensed spectrum. Current solutions use the 2.3, 2.5, and 3.5 GHz bands.	Service providers can leverage both types of spectrum; for example, license exempt for best effort local area traffic and licensed for wide area and QoS sensitive traffic.
Short range with up to 100 meters for a single access Point.	Metropolitan area mobile coverage of up to several kilometers for a single base station. Longer range (up to several miles) for fixed & lower-density deployments.	Economical coverage of large areas; for ex-ample, Wi-Fi hotspots in cafes, hotels, and airports, and WiMAX for blanket coverage outside of hotspots
OFDM air interface, as defined in IEEE 802.11 a/g/n	Scalable OFDMA air interface, as defined in IEEE 802.16e-2005.	Similar technologies mean cost saving at both the silicon and device levels.
Device connects via a Wi-Fi access point to the operator's IP network and to the internet.	Device connects via base station to the operator's IP network and to the internet.	Common IP network components, such as authentication servers, Service platforms, and access gateways, can be used.
Options		
Evolution to mesh networks metropolitan areas.	Evolution to multi-hop relay to improve range and data rates.	The position for providing extended in coverage and services economically are further expanded.
Access points that include Wi-Fi for access and WiMAX for network connectivity	Leverage digital advances so that the entire base station con now is mounted on tower tops.	Deployment expense is expected to continue downward on a steady cost reduction curve.
Voice over internet protocol (VoIP) is supported with enhancement IEEE 802.11e, k and r.	VoIP is supported by the extended real-time polling class of service.	Both specifications support VoIP; however operations in license exempt spectrum limit QoS assurance.
IEEE 802.11n high throughput will support digital home applications, such as video over IP	WiMAX provides high data rates and QoS classes to support broadcast and multicast video.	Both specifications support VoIP. However, operations in license exempt spectrum limit QoS assurance.

IV. Experimental Setup

In this paper two scenarios are introduced. The results are computed on the basis of these two scenarios and then the performance is compared. Among these two scenarios, the difference is that in second scenario we are introducing Wormhole Attack but the first scenario is without the attack.

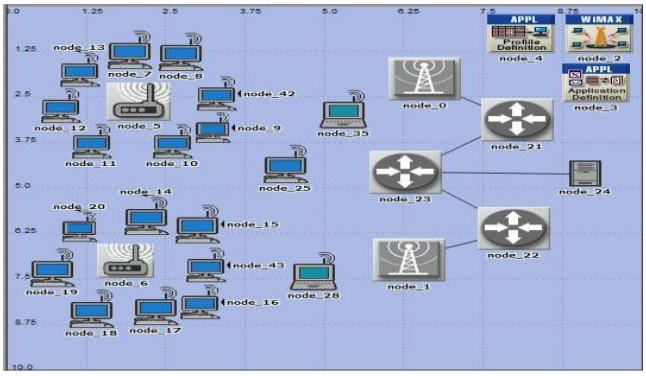
In this network model two scenarios are made in which first scenario is without malicious node. In second scenario one malicious node (wormhole node) is added. These scenarios are tested under VOICE and HTTP application using different protocol (DSR, OLSR, and TORA).

- WiMAX-WLAN Scenario using three Protocols TORA, DSR and OLSR using VOICE traffic without Wormhole Attack.



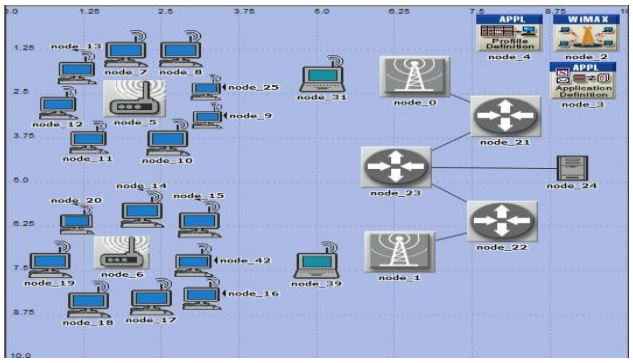
➢ WiMAX-WLAN Scenario using three Protocols TORA, DSR and OLSR using VOICE traffic with Wormhole Attack.

➢

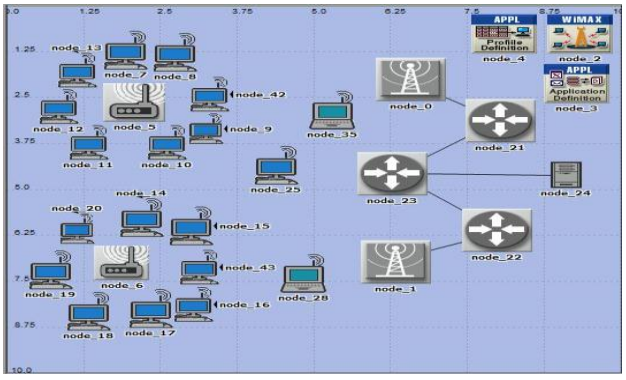


➢ WiMAX-WLAN Scenario using three Protocols TORA, DSR and OLSR using HTTP traffic without Wormhole Attack.

➢



➢ WiMAX-WLAN Scenario using three Protocols TORA, DSR and OLSR using HTTP traffic with Wormhole Attack.



V. Results

➢ Results of VOICE traffic over the two scenarios with and without wormhole attack on WiMAX-WLAN interfaced network.

1. Voice: Jitter (sec)

This figure shows the comparison of Traffic sent by using three protocols TORA, DSR and OLSR without wormhole attack over the WiMAX-WLAN interface network.

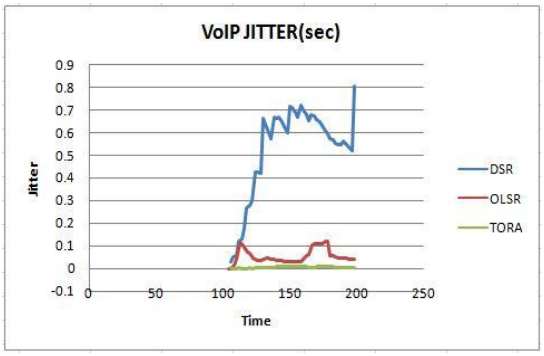


Fig 1.1: - Jitter without wormhole attack

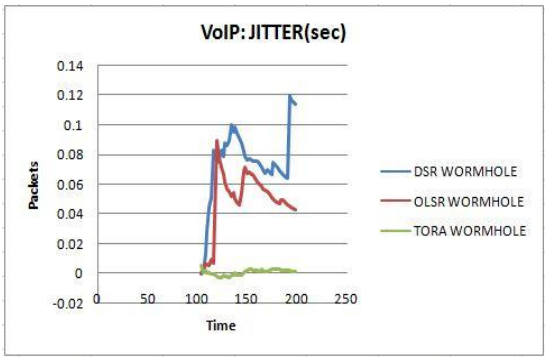


Fig 1.2: - Jitter with wormhole attack

In both the scenarios TORA is giving the minimum jitter among three protocols.

2. Voice: Packet End to End Delay (sec)

This figure shows the comparison of Packet End to End Delay of VOICE traffic over the network by using three protocols TORA, DSR and OLSR without and with wormhole attack over the WiMAX-WLAN interface network.

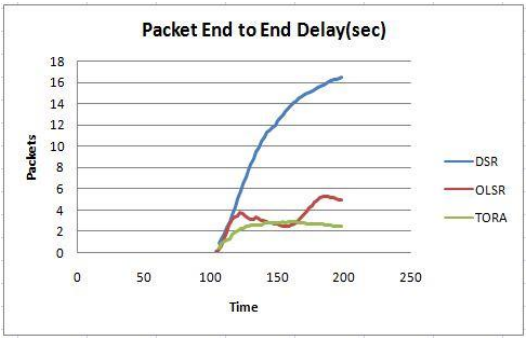


Fig 1.3: - Packet End to End Delay without Wormhole attack

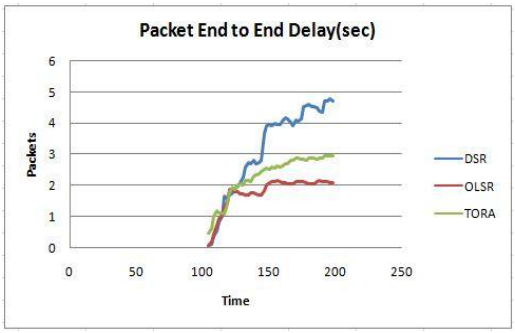


Fig 1.4: - Packet End to End Delay with wormhole attack

It is clear from the above results that without wormhole attack, TORA is giving least delay, but with wormhole attack DSR is having minimum Packet End to End Delay.

1. Voice: Traffic received (bytes/sec)

This figure shows the comparison of Traffic Received by using three protocols TORA, DSR and OLSR without wormhole attack over the WiMAX-WLAN interface network..

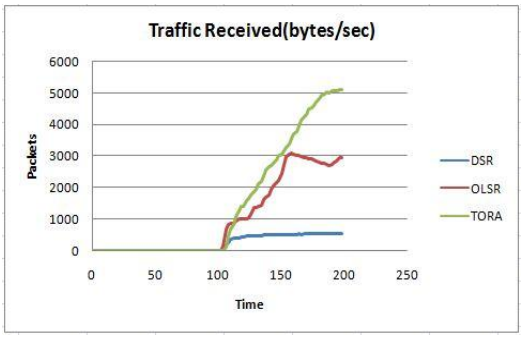


Fig 1.5: - Traffic Received without Wormhole attack

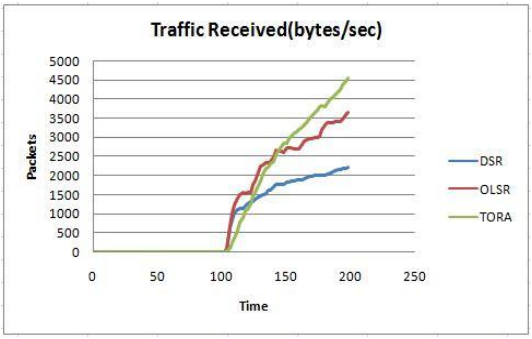


Fig 1.6: - Traffic Received with wormhole attack

By looking into both graphs, it is concluded that in both the scenarios i.e. without and with wormhole attack; TORA is receiving maximum voice traffic.

2. Voice: Traffic Sent (bytes/sec)

This figure shows the comparison of Traffic Received by using three protocols TORA, DSR and OLSR without wormhole attack over the WiMAX-WLAN interface network.

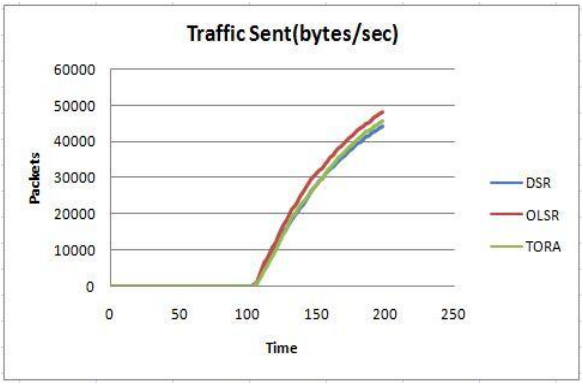


Fig 1.7: - Traffic Sent without wormhole attack

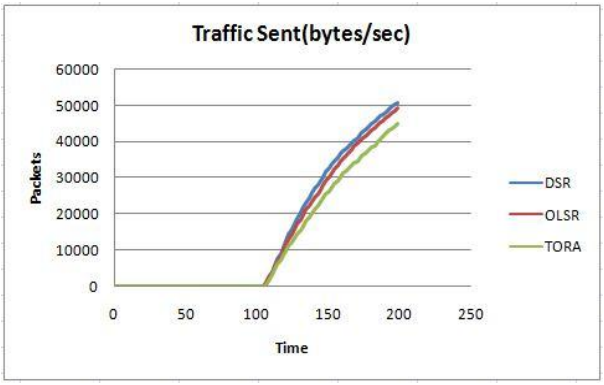


Fig 1.8: - Traffic Sent with wormhole attack

In the first graph which is without wormhole attack; OLSR is sending maximum of the VOICE traffic. On the other hand, in second graph, which is showing the results of the scenario which is under the effect of wormhole attack, it is shown that DSR is sending the maximum of VOICE traffic.

➢ Results of HTTP traffic over the two scenarios with and without wormhole attack on WiMAX-WLAN interfaced network.

1. HTTP: Object Response Time (sec)

This figure shows the comparison of HTTP Object Response Time (sec) using three protocols TORA, OLSR and DSR without wormhole attack over the WiMAX-WLAN interface network.

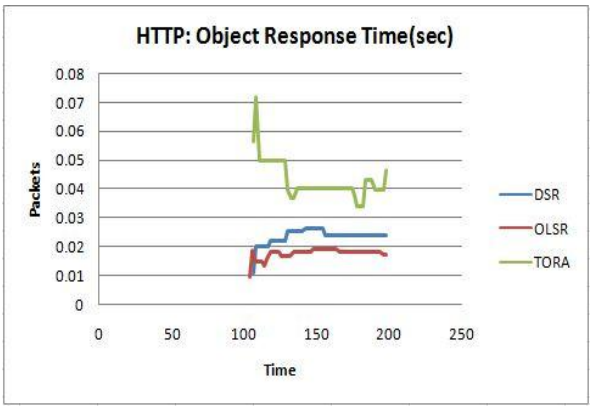


Fig 1.9: - Object Response Time without Wormhole attack

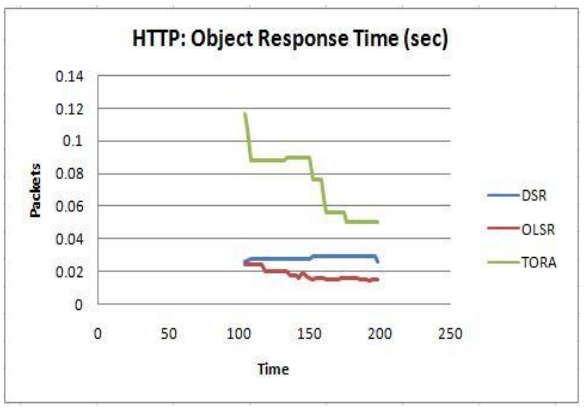


Fig 2.0: - Object Response Time with Wormhole attack

In both the scenarios, OLSR is taking least Object Response Time for HTTP traffic over the interfaced scenario.

6. HTTP: Traffic Received (bytes/sec)

This figure shows comparison of the HTTP traffic Received (bytes/sec) using all three protocol TORA, OLSR and DSR, without and with wormhole attack over the WiMAX-WLAN interface network.

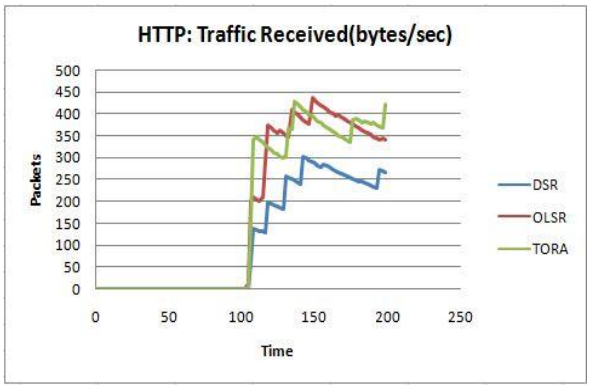


Fig 2.1: - Traffic Received without wormhole attack

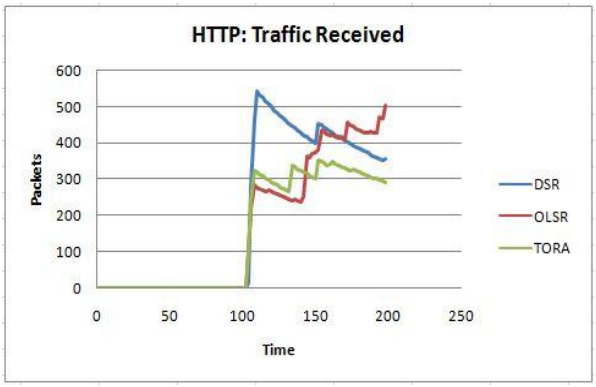


Fig 2.2: - Traffic Received with wormhole attack

The scenario which is without wormhole attack, TORA is receiving maximum traffic of HTTP but on the other hand, under wormhole attack, OLSR is receiving the maximum of HTTP traffic.

7. HTTP: Traffic Sent (bytes/sec)

This figure shows the comparison of HTTP Traffic Sent by using three protocols TORA, OLSR and DSR, without and with wormhole attack over the WiMAX-WLAN interface network.

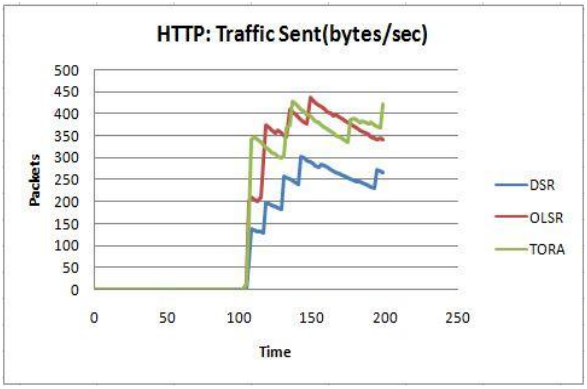


Fig 2.3: - Traffic Sent without wormhole attack

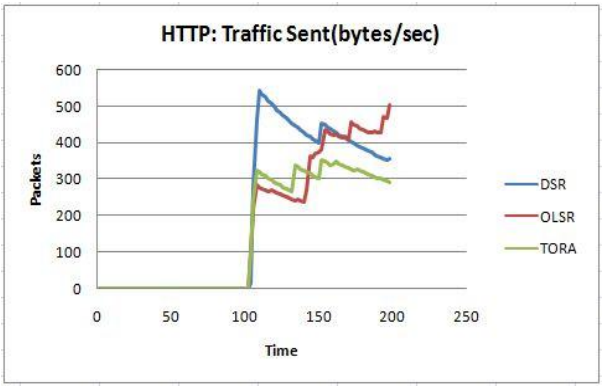


Fig 2.4: - Traffic Sent with wormhole attack

From above graphs it is clear that without wormhole attack, TORA is sending maximum data but under the effect of wormhole attack on same scenario, OLSR is sending the maximum data traffic.

VI. Conclusion

Following are the conclusions which are concluded after taking the simulations over two different applications i.e. HTTP and VOICE.

- **Conclusions under VOICE Application**

1. Under VOICE traffic, without wormhole attack, TORA protocol is giving the best performance among three protocols (TORA, OLSR AND DSR) over the WiMAX-WLAN Interfaced scenario.
2. Under the effect of wormhole attack, it is concluded that TORA is performing superiorly among all the protocols as at last after under-going all the effects, it is receiving maximum VOICE traffic in comparison to other protocols.

- **Conclusions under HTTP Application**

1. Under HTTP traffic, without wormhole attack, TORA protocol is giving the best performance among three protocols (TORA, OLSR AND DSR) over the WiMAX-WLAN Interfaced scenario.
2. Under the effect of wormhole attack, it is concluded that OLSR is performing superiorly among all the protocols as at last after under-going all the effects; it is receiving maximum HTTP traffic in comparison to other protocols.

References

[1] Mrs.M.Rekha ,Dr.C.Chandrasekar, "Trust Based Authentication Technique For Security In WiMAX Networks" in International Journal of Computer Aided Engineering , Volume 03– No.3, Issue: 01, 2012 .
[2] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks" in IEEE, Volume 24, No. 2, 2006.
[3] Michel Barbeau, '' WiMAX/802.16 Threat Analysis'' School of Computer Science Carleton University, ACM 1-59593-241-0/05/0010, 2005.
[4] Cao, Maode Ma, Muhammad Ashaari Bin Ariff, "Security Enhancements in WiMAX Mesh Networks" in IEEE International Conference, ISBN 978-1-61284-159-5, 2011.
[5] Shah-An Yang and John S. Baras, "TORA, Verification, Proofs and Model Checking" MD 20742, USA, 2003
[6] Karen Scarfone, Cyrus Tibbs, Matthew Sexton,"Guide to Securing WiMAX wireless communications"2010.
[7] Rakesh Kumar Jha, Dr Upena D Dalal, " A Journey on WiMAX and its Security Issues" in International Journal of Computer Science and Information Technology, Volume 1 (4) , 256-263, 2010.
[8] Yan Zhang and Nirwan Ansari , "Wireless Telemedicine Service Over Integrated IEEE 802.11/WLAN And IEEE 802.16/WIMAX Networks" in IEEE, volume 17 issue 1, 2010.
[9] Nasreldin, M. MCIT, Cairo Asian, H. ; El-Hennawy, M. ; El-Hennawy, A.,"WiMAX Security" 2008.
[10] Michel Barbeau ,"WiMax/802.16 threat analysis" 2005.