# WiMAX - WLAN interface using TORA, DSR and OLSR Protocols with their Evaluation under Wormhole Attack

Sharanbeer Kaur
Research Scholar
Department of Computer Science
CT inst. Of Engg. Management technology

Shivani Khurana
Assistant Professor
Department of Computer Science
CT inst. Of Engg. Management technology

## ABSTRACT

As it is know that WiMAX and WLAN are two wireless developing technologies. The researchers are working on the integrated scenarios of these two technologies so as to approach the maximum benefits out of these technologies. Therefore in this paper we are performing simulations over the two scenarios i.e. with wormhole attack and without wormhole attack. The evaluation is taken on three different protocols i.e. DSR, OLSR and TORA. The results are shown in graphical figures and according to them results are made.

## Keywords

WiMAX, WLAN, WIMAX-WLAN Integrated circuit, OLSR, DSR, TORA.

## 1. INTRODUCTION

Wireless transmission is the technology used in current phase of technical environment. The transmission of signals or we can say transmission of data using Radio waves instead of wires is known as Wireless Transmission. Wireless Technologies are the simplest ways to transmit signals and hence are deploying to new technologies under wireless concept. WLAN and WiMAX are such techniques which come under wireless technologies and are widely or worldly used in today's life. Both wireless technologies i.e. WiMAX and WLAN are Showing different characteristics and features except one small thing that they transmit signals without wires. WiMAX is the advanced wireless technology among all other wireless technologies. In this paper the work is done by taking the integrated scenario of two wireless technologies i.e. WLAN and WiMAX.

**WLAN**:-WLAN is Wireless Local Area Network and hence it comes under wireless technologies and it provides different features which are suitable for users to transmit signals or to have better communication over the air. In other words for WLAN we can say that it provides all the features of Local Area Network but without Wires.

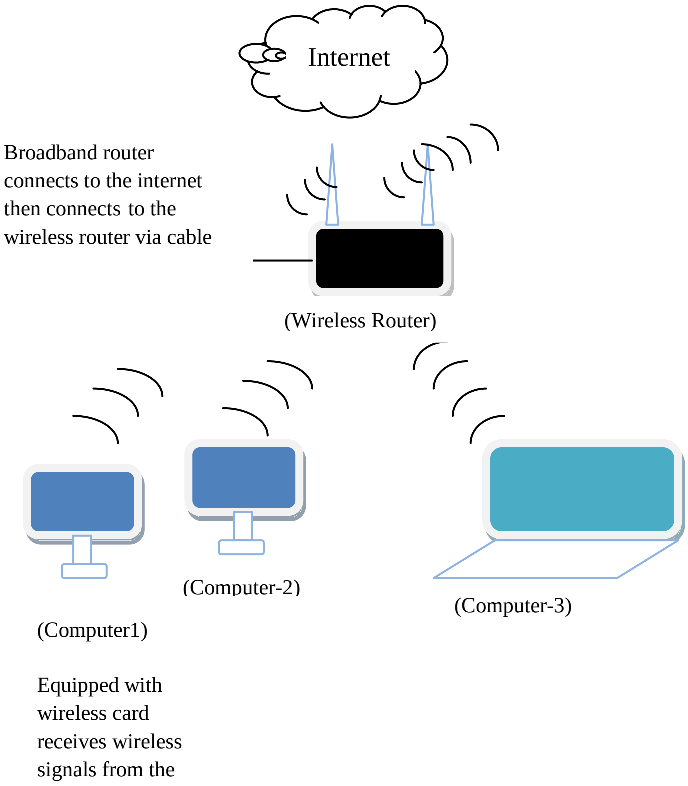

**Fig1:- Simple Architecture of WLAN**

In the above diagram we are given with the simple architecture of WLAN. We are having two routers in the diagram in which one is Broadband router connects to the internet and then connects to the second router i.e. Wireless router via cable (wire).This Wireless router acts as Access Point (AP) and the users or working nodes will get signals from this AP another name which can be used for this AP is Modem.

**WiMAX**:-WiMAX is a Worldwide Interoperability for Microwave Access. It is wireless broadband technology which is based on IEEE 802.16 standard. A cellular system is setup in Wireless Broadband Access [1], which uses base stations, serves as a radius of long distances i.e. miles/kilometers. Residing on the towers is not the compulsion for the base stations. For the purpose of transmission or communication over air, IEEE 802.16 is designed to operate in 10-66GHz spectrum which specifies the Physical Layer (PHY) and Media Access Control Layer (MAC) of BWA system which is on air Interface system. In the range of 10-66 GHz, for signal transforming, LOS is required i.e. Line of Sight. But the Physical Layer is not suitable for lower frequency applications where NLOS (Non-Line of Sight) operations are required. Therefore NLOS accommodates in the range of 2-11GHz. WiMAX base stations can offer greater wireless coverage of about 5 miles with LOS transmission within bandwidth of up to 70 Mbps.

**WiMAX Services**: - The use of one or more base stations makes it possible to make Metro Politian Area Network. It can provide services up to 30 mile radius. It can provide two forms of services:

Non Line Of Sight (NLOS) Services: This is the sort of service where small antenna on the computer connects WiMAX tower. The range of this type of service is 2GHz to 11GHz which is similar to Wi-Fi.

Line Of Sight (LOS) Services: In this type of Service dish antenna points straight at the WiMAX tower from a roof top. This connection is more stable and stronger and this is the reason why it can send lots of data with fewer errors. Its range is 66GHz.

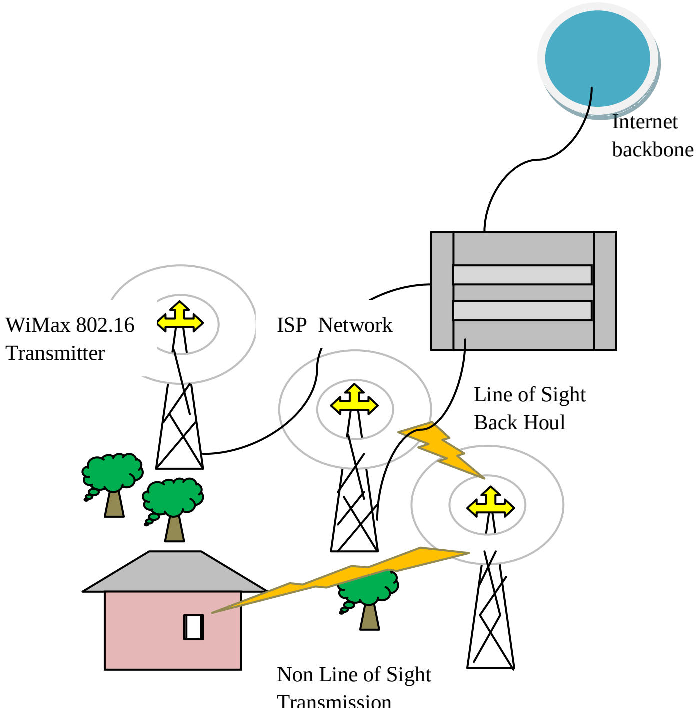

**Fig2:- Architecture of WiMAX with LOS and NLOS both services**

In the above diagram of architecture of WiMAX both the services are shown and hence the differentiation is cleared .The base stations are connecting the users to the INTERNET Backbone through ISP Network.

## 2. CAPACITY OF Wi-Fi vs. WiMAX

Distance of two connection points to which we call antennas, the connectivity of both WLAN and WiMAX depends upon [11] . In the case of WLAN if one will talk about IEEE 802.11g standard of WLAN, which is the latest and most common standard used on today's equipments, the data rate is around 54Mbps and the range indoors is around 30 meters. The range and the data rate can be varied and changed with the conditions of the area and the Line Of Sight of devices used. On the other hand WiMAX will deliver 70Mbps, 50 kms in theory; but these numbers can be changed according to conditions.

## 3. ROUTING

During network communication, we require a path to transfer the data signals. Hence, routing is the name given to the process of choosing a path. Therefore routing is to pick out a suitable and a right path from source to destination. This basic terminology is used in different types of networks. For the process of routing, routing tables are available which are based on different special algorithms and are chosen according to the requirements of the users. In other words, we can say that protocols are the set of rules binding as an algorithm through which two or more devices can communicate with each other.

## 4. ROUTING PROTOCOLS

Routing protocols are used to search the different routes so that the sender could be able to send the data from the source to the destination over the network. A number of routing protocols are available and the user can choose among them in accordance with the mode of

its communication. Routing Protocols are mainly divided into two categories i.e. Proactive or Table Driven Protocols and Reactive or On-Demand Protocols.

In Proactive Routing Protocols or Table driven protocols, as per its name, the nodes always maintains the routing information updating in the Routing Table. This is achieved by getting or updating the periodic updates in the routing table by each connecting node. OLSR (Optimized Link State Routing Protocol) is the example of this kind of protocols.

In Reactive Protocols or On-Demand Routing Protocols, distance vector routing algorithm is used and the route is found on the demands of the nodes which are acting as the sender users. Here no routing table is available and hence no periodic update is required.

## 5. WiMAX-WLAN INTEGRATED TECHNOLOGY

WiMAX and WLAN are both wireless broadband technologies, but they differ in the execution. The fundamental changes are bringing out to data networking and telecommunication through Wireless Communication Revolution and are making integrated network- 'a reality'.

## 6. THREATS/ATTACKS

Some of the following threats/attacks which are acting as the issues to be discussed compulsory so as to provide the most possible security to wireless links. Some major threats are discussed below[4] [7] [8] [9]:

### 6.1 Jamming

Introduction of noise so as to reduce the capacity of the channel is called Jamming attack. To be performed intentionally or unintentionally, the jamming attack is quite easy.

### 6.2 Scrambling

Scrambling is a kind of jamming attack but for short time of interval. The attacker attacks over the management information in order to hit on the normal or controlled operations of the network.

### 6.3 Water Torture Attack

In this attack the attacker attacks on the SS (subscriber station) and then absorbs all the computing resources by sending series of bogus frames.

### 6.4 Black Hole Attack

It is also named as Packet Drop Attack. It is called so because the attacker in this type of attack acts as malicious node and falsely claim a fresh route to the destination and in this way it absorbs the transmitted data from source to that destination and drop that data instead of forwarding.

### 6.5 Wormhole Attack

In a wormhole attack, an adversary connects two distant points in the network with low-latency communication link. This link is named as the wormhole link. Once the wormhole link is established, the malicious node captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

## 7. SCENARIO

In this paper we are introducing two scenarios. 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.

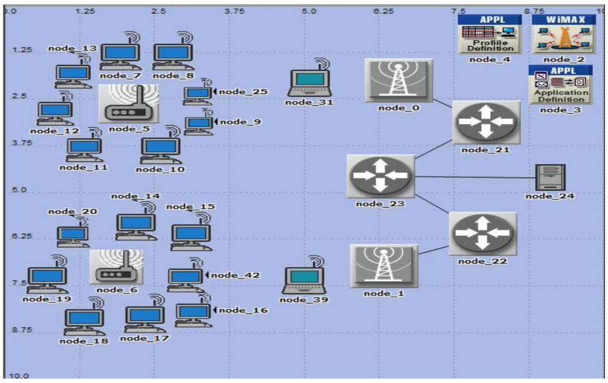

**Fig3: Network Model without Wormhole Attack**

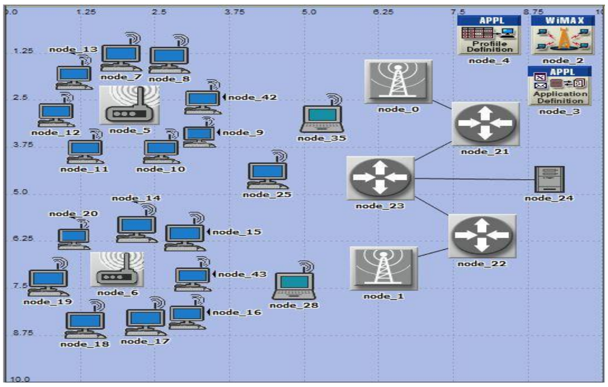

**Fig4: Network Model with Wormhole Attack**

## 8. SIMULATION PARAMETER

In this network model 2 scenarios are made. In which first scenario is without malicious node in second scenario with one malicious node (wormhole node). These scenarios are tested under VOICE application using different protocol (DSR, OLSR, and TORA).

Performance of WiMAX-WLAN Scenario using Three Protocols TORA, DSR and OLSR over VOICE traffic without Wormhole Attack Under the following Parameters

### 8.1 Voice: Traffic Sent (bytes /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.

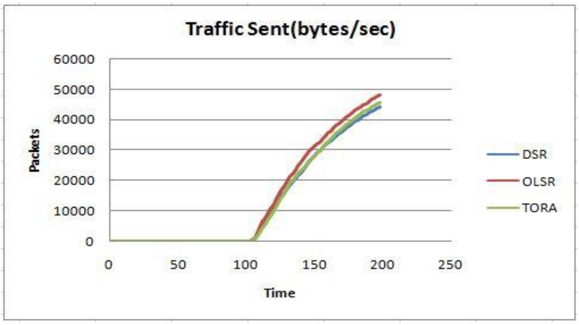

**Fig5: Traffic Sent without Wormhole Attack**

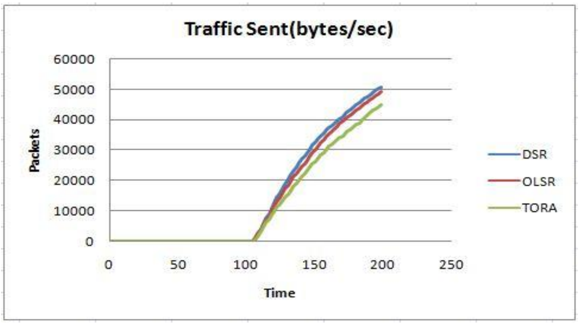

**Fig6: Traffic Sent with Wormhole Attack**

In above results the first graph is showing results without attack in which OLSR is sending the maximum data over the network but on the other hand; in the graph which is showing results with wormhole attack, DSR is sending the maximum data over the network.

### 8.2 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.

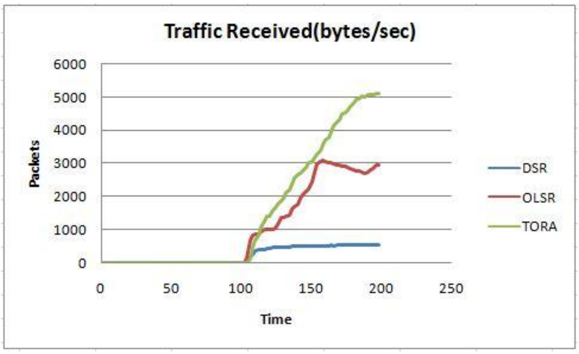

**Fig7: Traffic Received without Wormhole Attack**

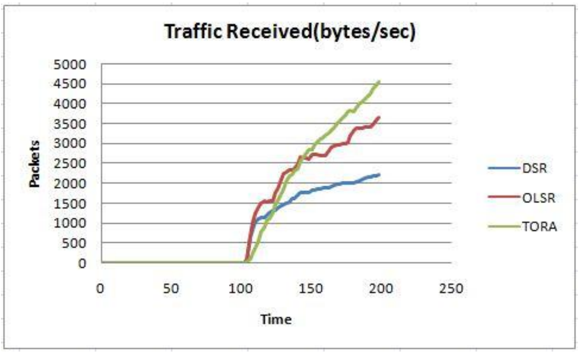

**Fig8: Traffic Received with Worm Hole Attack**

In above results, in both cases i.e. without and with attack, TORA is receiving the maximum data over the network.

## 8.3 WiMAX: Delay (sec)

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

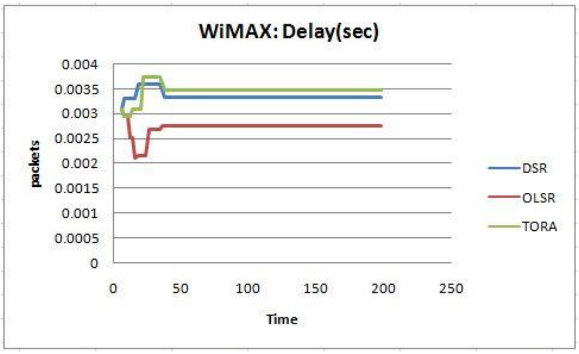

**Fig9: WiMAX Delay without Wormhole Attack**

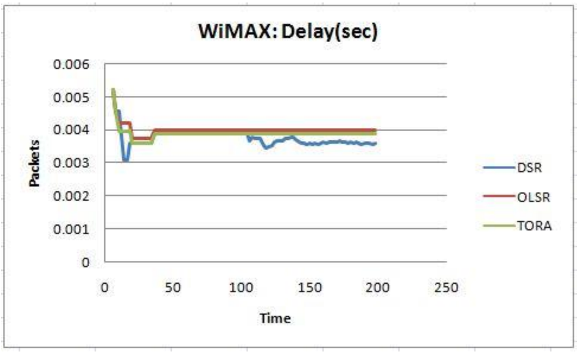

**Fig10: WiMAX Delay with Worm Hole Attack**

In above results the first graph is showing results without attack in which it is clear that OLSR is having the least delay but in the case of the scenario with wormhole attack, here, DSR is having the least delay and hence giving best performance.

## 8.4 WiMAX: Load (bits/sec)

This figure shows comparison of the WiMAX Load using all three protocols over the WiMAX-WLAN interface network.

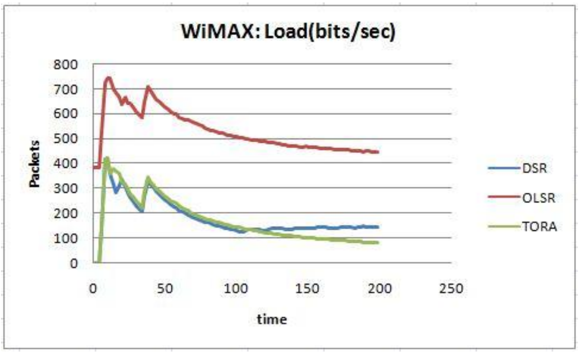

**Fig11: WiMAX Load without Worm Hole Attack**

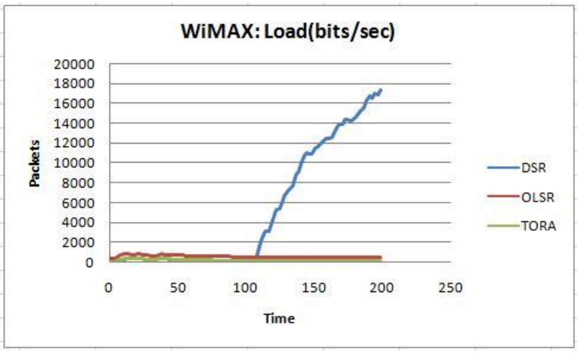

**Fig12: WiMAX Load with Worm Hole Attack**

In above results the first graph is showing results without attack in which OLSR is taking the maximum load over the network but on the other hand; in the graph which is showing results with wormhole attack, DSR is taking the maximum load over the network.

## 8.5 WiMAX: Throughput (bits/sec)

This figure shows the comparison of WiMAX Throughput Load using all three protocols over the WiMAX-WLAN interface network.

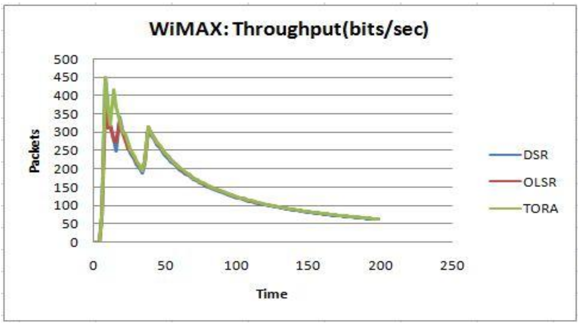

**Fig13: WiMAX Throughput without Wormhole Attack**

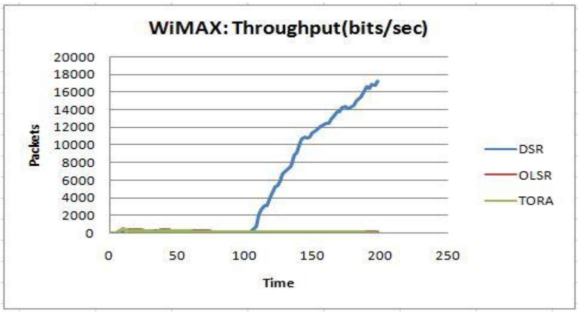

**Fig14: WiMAX Throughput with Wormhole Attack**

From above results it is clear that the throughput of the scenario without wormhole attack which is shown in first graph, is shown best by the TORA but with wormhole attack, DSR is giving the maximum throughput.

## 8.6 WLAN: Delay (sec)

This figure shows the comparison of Delay in WLAN using all three protocols over the WiMAX-WLAN interface network.

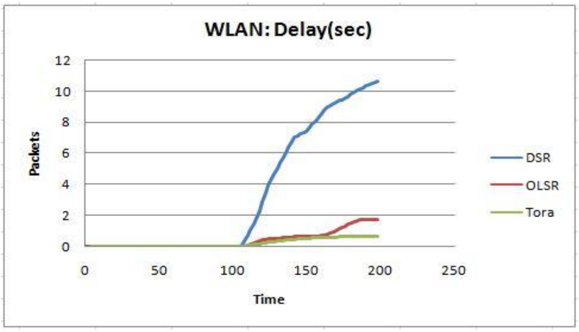

**Fig15: WLAN Delay without Wormhole Attack**

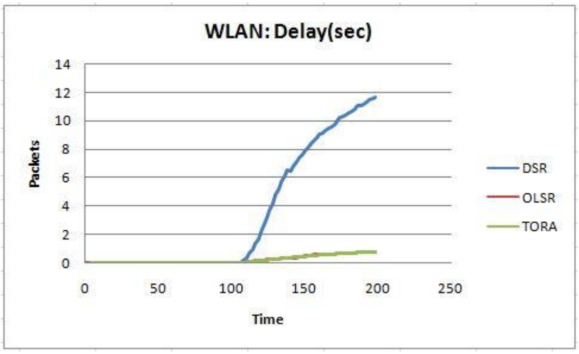

**Fig16: WLAN Delay with Wormhole Attack**

It is clear from above results that WLAN Delay is least given by OLSR in the scenario without wormhole attack but on the other hand, with the scenario in which wormhole attack is applied, TORA is showing least WLAN Delay.

## 8.7 WLAN: Load (bits/sec)

This figure shows the comparison of Load in WLAN using all three protocols over the WiMAX-WLAN interface network.

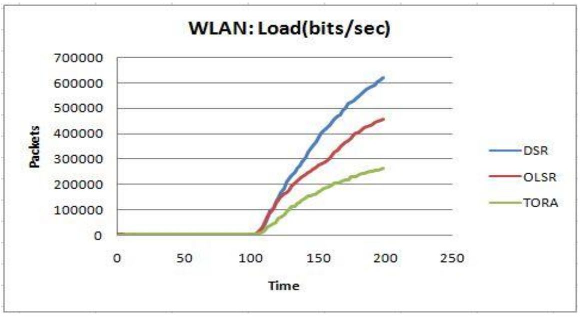

**Fig17: WLAN Load without Wormhole Attack**

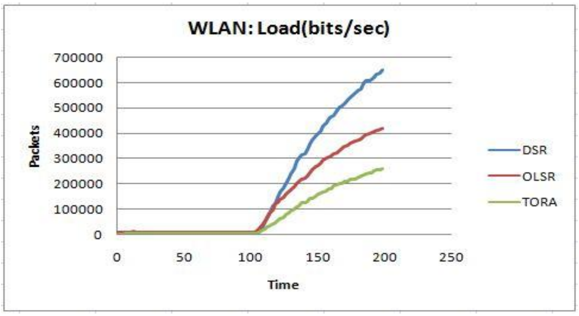

**Fig18: WLAN Load with Wormhole Attack**

Above results sho

ws that in both the scenarios; either with or without wormhole attack; DSR is taking maximum load.

## 8.8 WLAN: Media Access Delay (sec)

This figure shows the comparison of Media Access Delay in WLAN using allthree protocols over the WiMAX-WLAN interface network.

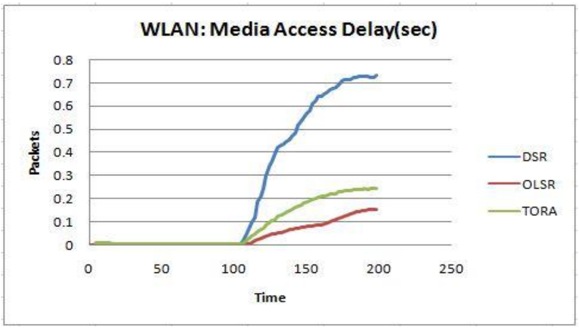

**Fig19: WLAN Media Access Delay without Wormhole Attack**

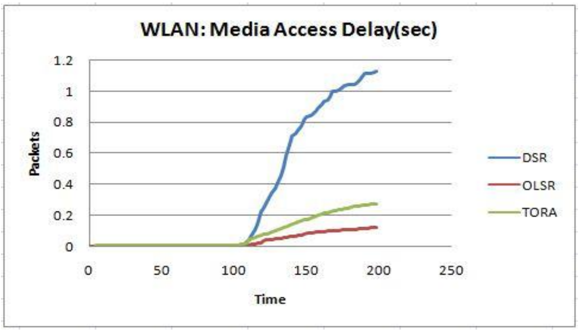

**Fig20: WLAN Media Access Delay with Wormhole Attack**

In both cases; OLSR is showing least Media Access Delay of WLAN.

### 8.9 WLAN: Throughput (bits/sec)

This figure shows the comparison of throughput in WLAN using all three protocols over the WiMAX-WLAN interface network.

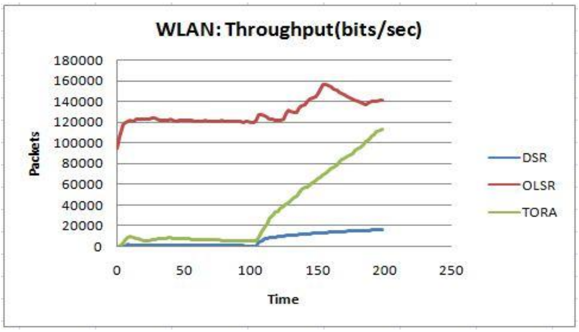

**Fig21: WLAN Throughput without Wormhole Attack**

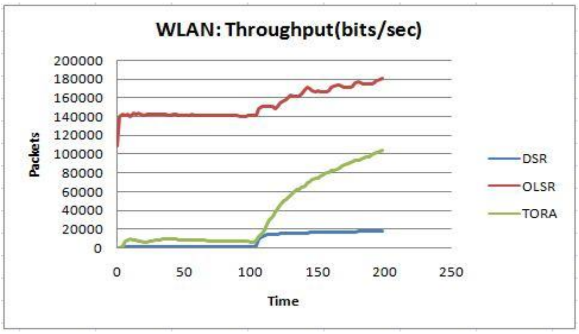

**Fig22: WLAN Throughput with Wormhole Attack**

In above results the first graph is showing results without attack in which OLSR is showing the maximum throughput over the network and same can be seen in the graph which is showing results with wormhole attack i.e. OLSR is showing the maximum throughput over the network.

## 9. CONCLUSION

After performing the simulation over the two models that is with and without wormhole attack, under the effect of three protocols TORA, DSR and OLSR; the results are made with the help of OPNET modeller. We have made two conclusions after getting results. The first thing which is concluded is that, on WiMAX, under un-attacked scenario OLSR is performing best but under attacked scenario DSR is giving best performance. And second conclusion is that, on WLAN Scenario OLSR is giving the best performance under both attacked and un-attacked scenarios.

## 10. FUTURE SCOPE

In future, the research can be done on the integrated scenario of WiMAX and WLAN by taking evaluation parameters and choosing other protocols. There are various attacks which are becoming the issues for the network communication; hence, the simulations can be taken with different attacks like black hole attack, water torture attack etc.

## 11. REFERENCES

[1] Mrs. M. Rekha , Dr. C. Chanderasekar ”Trust based authentication technique for security in WiMax networks” 2012.http://ijcae.org/admin/journals/Journals465.pdf

[2] Chauhan, N , Yadav, R.K ,”Security Analysis of Identity Based Cryptography and Certificate Based in Wimax Network ) “ 2012.http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6168423&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6168423

[3] Adnan Shahid Khan, Norsheila Fisal, Sharifah, Kamilah, Sharifah Hafizah, Mazlina Esa, Zurkarmawan, Abu Bakar, M. Abbas,” An Efficient Self-Organized Authentication and Key Management Scheme for Distributed Multihop Relay-Based IEEE 802.16 Networks” 2011http://sites.google.com/site/ijcsis/, ISSN 1947-5500

[4] Jin Cao , Nanyang , Maode Ma ; Ariff, M.A.B “Security enhancements in WiMAX mesh networks”2011.http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6156000&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F6153216%2F6155882%2F06156000.pdf%3Farnumber%3D6156000

[5] Hashmi, R.M. Politec. di Milano, Milan, Italy Siddiqui, A.M. ; Jabeen, M. ; Alimgeer, K.S.,” Towards secure wireless MAN: Revisiting and evaluating authentication in WiMAX , 2011. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6020925&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6020925

[6] Karen Scarfone, Cyrus Tibbs, Matthew Sexton,”Guide to Securing WiMAX wireless communications”2010.http://dl.acm.org/citation.cfm?id=2206213

[7] Shojaee, M. , Iran Movahhedinia, N Ladani, B.T.”Traffic analysis for WiMAX network under DDoS attack,”2010.http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5626885&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5626885

[8] N. Seddigh, B. Nandy, R. Makkar J.F. Beaumont ,”Security Advances and Challenges in 4G Wireless Networks”2010.http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5593244&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5593244

[9] Nasreldin, M. MCIT, Cairo Asian, H. ; El-Hennawy, M. ; El-Hennawy, A.,”WiMAX Security” 2008.http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4483104&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4483104

[10] Michel Barbeau ,”WiMax/802.16 threat analysis” 2005.http://www.multiinfocom.ru/ru/artpdf/iq2-barbeau.pdf

[11] “Comparison of the basic features of Wi-Fi (802.11b/g) - WiMAX (802.16)”.Wi-Fi Mail.baskent.edu.tr/.../0401/.../burak-usgurlu-lastHW-wifiVSwimax.pdf.