Volume 4, Issue 8, August 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Performance Analysis of Black Hole Attack using Different Routing Protocols on WLAN-WiMAX Interface Network

Neha Garg
Master of Technology
Department of Computer Science
Punjabi University, India

Dr. Jyotsna Sengupta
Professor
Department of Computer Science
Punjabi University, India

Abstract: ***We are in advanced world of internet with new technologies. So many new wireless networks technologies have been emerged. WiMAX-WLAN Interface Network is advanced integrated wireless network. These networks are weak against many types of attacks. One of these attacks is the Black Hole. In this attack, a malicious node advertises itself as having freshest or shortest path to specific node to absorb packets to itself. The effect of Black Hole attack on integrated network using AODV, DSR, and TORA as a routing protocol is examined in this paper. Furthermore, we investigate the performance of different routing protocols under black hole attack for increasing over network performance. Simulation results using OPNET simulator depict that AODV gives best performance in the presence of malicious nodes.***

Keywords— WLAN, WiMAX, AODV, DSR, TORA, OPNET.

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 ho me 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.

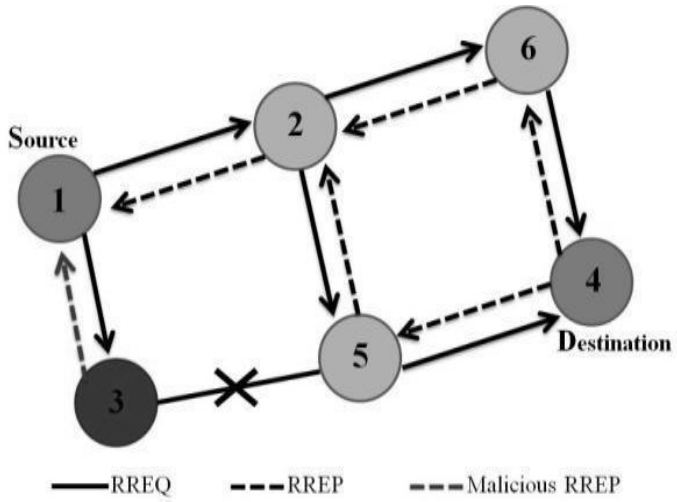
WiMAX - WLAN Comparison[15]

Wi-Fi IEEE802.11(a/g/n)	WiMAX (IEEE802.16e-2005) Market	Synergy Impact
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.
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 severalmiles) for fixed and lower-density deployments.	Economical coverage of large areas; for example, 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.	Commo 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 realtime 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 overIP	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

III. BLACK HOLE ATTACK:

An attacker can drop received routing messages, instead of replaying them as the protocol requires, in order to reduce the quantity of routing information available to the other nodes. This is called Black Hole Attack [3]. It is passive attack and is also a simple way to perform a Denial of Service. Black Holes refer to places in the network where incoming traffic is silently discarded (or dropped), without informing the source that the data did not reach it intended recipients. The method of how malicious node fits in the data routes varies



In above Figure[3], Node 1 is the source node and node 4 is the destination node. Node 3 is a malicious node in which replies makes a false response stating that it has the shortest route to the destination node. Node 1 erroneously starts sending data packets to Node 3 which probably drops or consumes the packets. This suspicious node can be regarded as a Black hole which misroutes the packets easily and the network operation is hindered.

ORGANISATION OF SECTIONS

This paper is organised as follows :

Section I is all about the abstract and brief introduction to WiMAX and WLAN technologies.

Section II described the standards of two technologies i.e. WiMAX and WLAN.

Section III described a brief about Black Hole attack.

Section IV illustrated the WiMAX-WLAN Network Model Implementation, this model is implemented with the help of OPNET MODELER 14.5v.

Section V show the basic parameters set on the Base Station (BS) and Subscriber Station (SS) according to IEEE 802.16 standards.

Section VI is important, we have plotted simulation results to investigate the black hole attack with different routing protocols.

Section VII analysed the Conclusion drawn from the results and

Section VIII On the basis of research found that a work will do in future and it's described in this future scope section.

IV. NETWORK MODEL FOR WiMAX-WLAN INTERFACE

The WiMAX Base Station (BS) may access maximum number of nodes depending on its capacity described in IEEE 802.16 standards. Here we have only one WiMAX node is taken which is covered by one BS. There are two AP in each subnet which are covered by two BS. The AP used is one type of router which takes WiMAX packets from BS and converts it to Wi-Fi packets and route to the WLAN clients, the AP work as a WiMAX clients. The AP contain maximum number of WLAN clients. Each AP consists of seven WLAN nodes. Subnet_1 AP is in connection with the BS WiMAX_BS_A via WiMAX link and Subnet_2 AP is in connection with BS WiMAX_BS_B via same WiMAX link. The AP are within the coverage area of WiMAX BS which is 30KM practically. The WLAN clients are placed in circular fashion which sorrounds their respective AP [13].

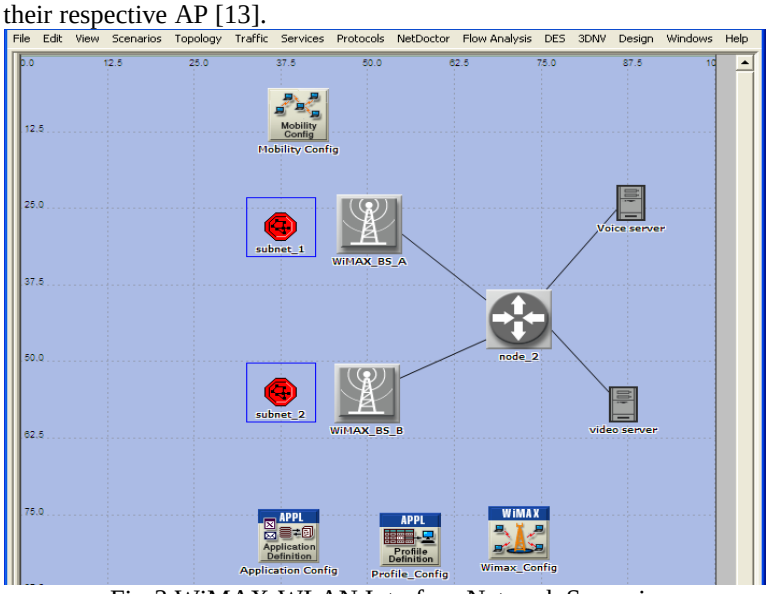


Fig-3 WiMAX-WLAN Interface Network Scenario

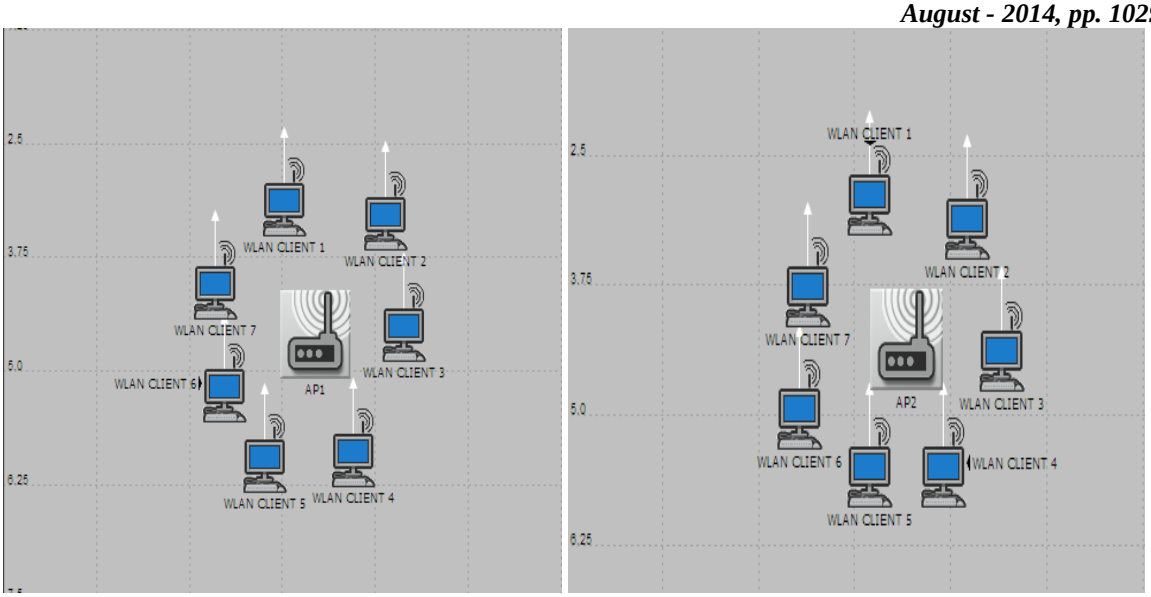


Figure-4 Subnet_1 and Subnet_2 Without attack

V. SIMULATION ENVIRONMENT

There are number of simulators available to perform simulation of the designed network. Basically Simulator is used to evaluate the idea of planning about the network. OPNET 14.5 is one of the best simulators used in the paper. On the above scenario, we applied AODV, DSR, TORA routing protocols under some simulation parameter. The results are computed on the basis of these scenarios and then performance is compared.

Area of Experiment	Campus(100*100km)
Number of nodes	7 nodes in each Subnet
Protocols	AODV,DSR, TORA
Duration of Simulation	600 sec

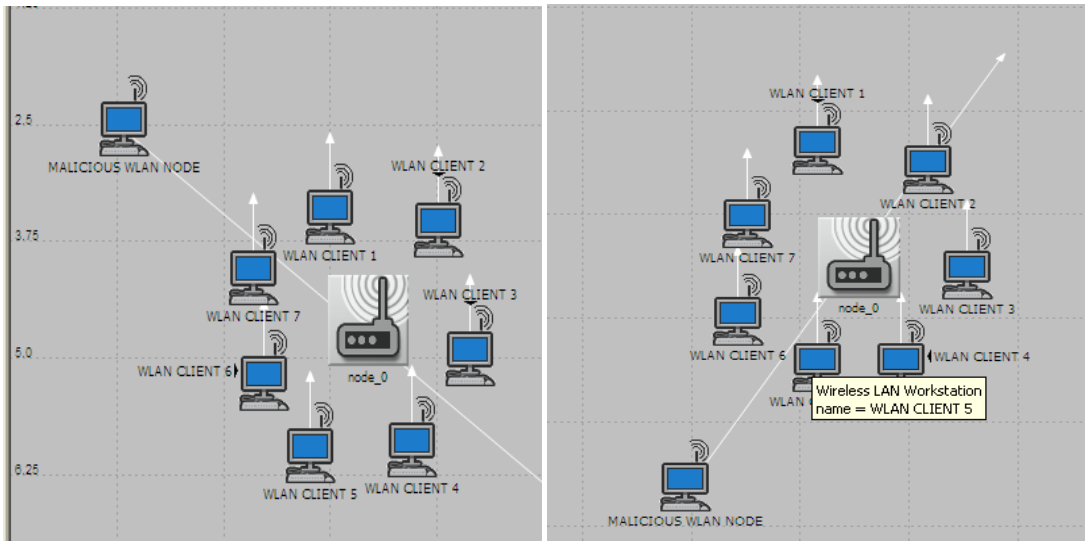


Figure-5 Subnet_1 and Subnet_2 With attack

In this network model, two scenarios are made, in which first s without any attack and in second scenario each subnet have one Black Hole Attack node. These scenarios are tested under 2 application Voice and Video using different routing protocol (AODV, DSR, TORA).

VI. PERFORMANCE RESULTS

- **WIMAX: Delay (Sec)**

This fig 6 and fig 7 shows the comparison of WiMAX Delay using all 3 protocols AODV, DSR, and TORA without Black Hole Attack over the WiMAX-WLAN Interface Network.

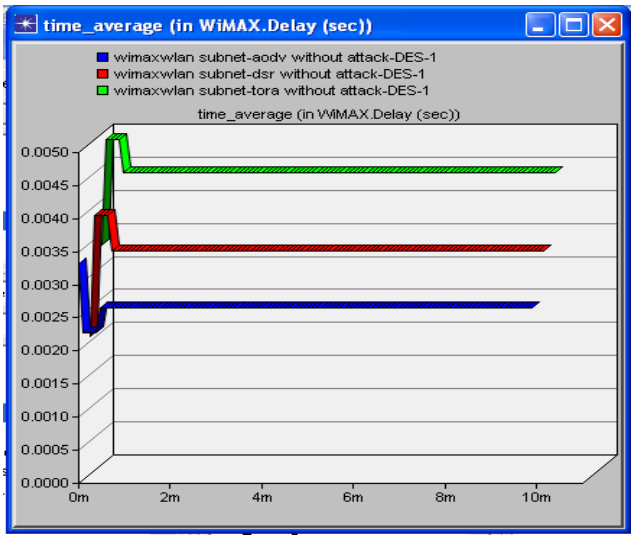


Figure-6 WiMAX Delay without Black Hole Attack

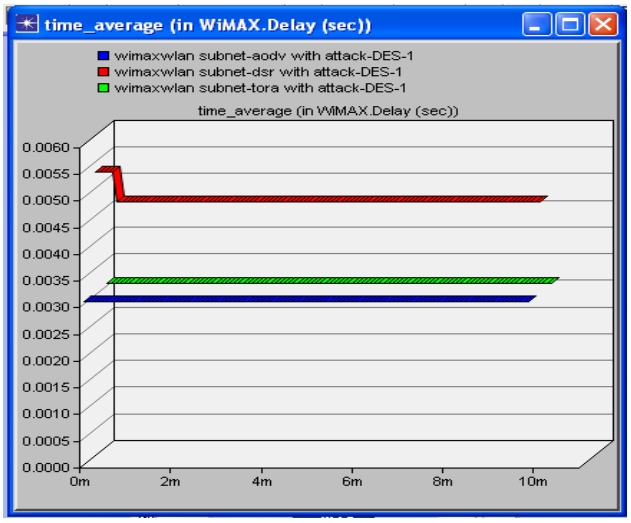


Figure-7 WiMAX Delay with Black Hole Attack

In above results, fig 6 is showing results without any attack in which it is clear that AODV is having least delay but from fig 7 in case of the scenario with Black Hole Attack, here AODV as well as TORA is having least delayand hence giving best performance.

- **WiMAX: Load(Packets/Sec)**

This fig 8 and fig 9 shows comparison of WiMAX load using all three protocols over WiMAX-WLAN interface Network.

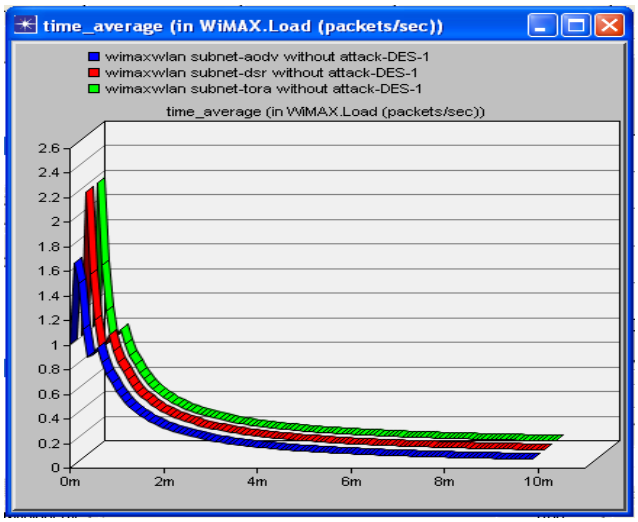


Figure-8 WiMAX Load without Black Hole Attack

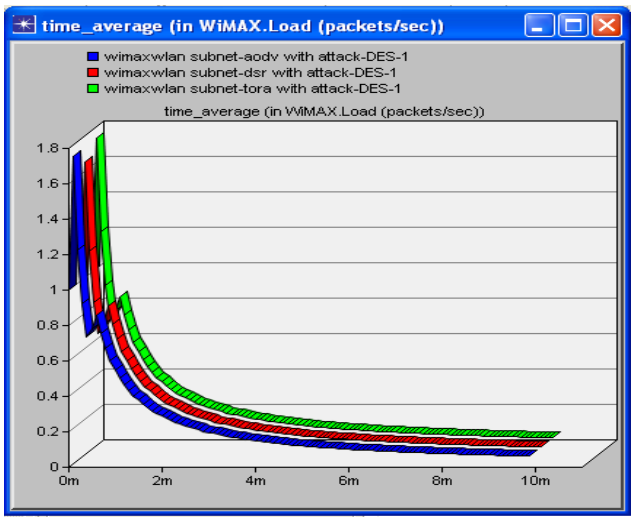


Figure-9 WiMAX Load with Black Hole Attack

In above results, the fig 8 is showing results without attack in which AODV is taking minimum Load over the network but on the other hand , in the fig 9 with Black hole Attack DSR and TORA is taking minimum load over the network as compare to AODV.

- **WiMAX: Throughput(Bits/Sec)**

This fig 10 and fig 11 shows the comparison of WiMAX Throughput using all three protocols over WiMAX-WLAN interface Network.

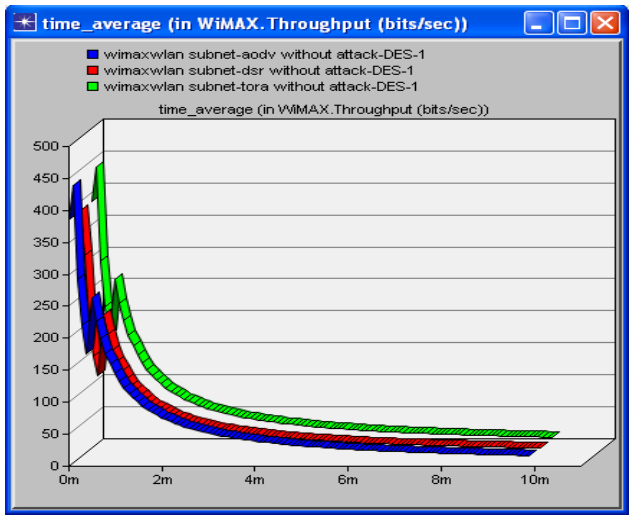


Figure-10 WiMAX Throughput without Black Hole Attack

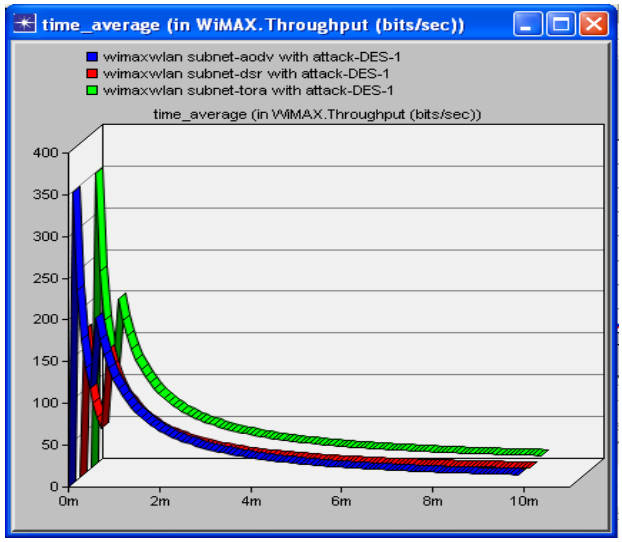


Figure-11 WiMAX Throughput with Black Hole Attack

From above results , it is clear that the Throughput of the scenario without attack shown in fig 10 is best by AODV and TORA but with Black Hole Attack both AODV and TORA is giving maximum throughput but Number of Bits per Seconds is less compared to without attack.

- **WLAN: Delay(Sec)**

This fig 12 and fig 13 shows the comparison of Delay in WLAN using all three protocols over the WiMAX-WLAN interface Network.

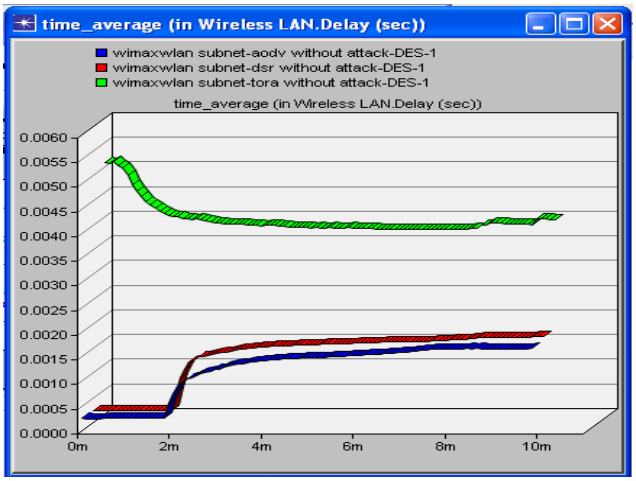


Figure-12 WLAN Delay without Black Hole Attack

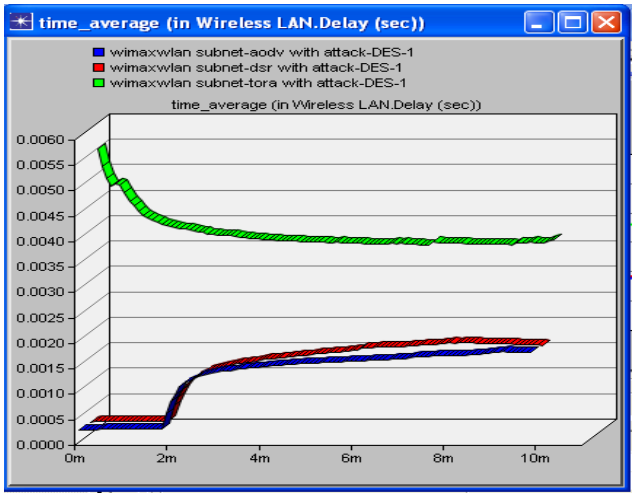


Figure-13 WLAN Delay with Black Hole Attack

It is clear from above results that the WLAN Delay is least given by AODV in both scenario with or without Black Hole Attack. But the value of delay is more in case of attack.

- **WLAN: Load(Bits/Sec)**

This fig 14 and fig 15 shows the comparison of WLAN Load using all three protocols over WiMAX-WLAN interface Network.

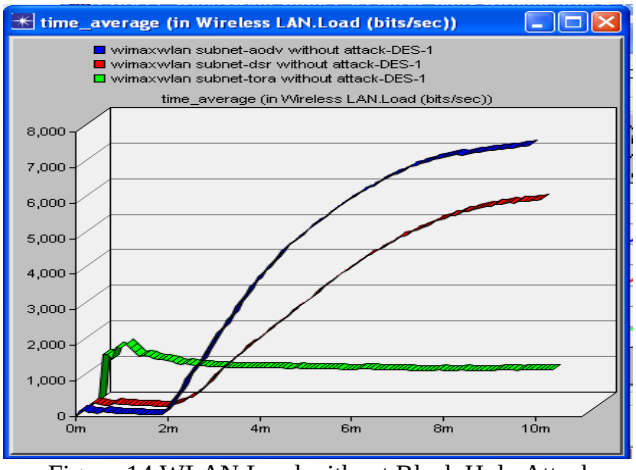


Figure-14 WLAN Load without Black Hole Attack

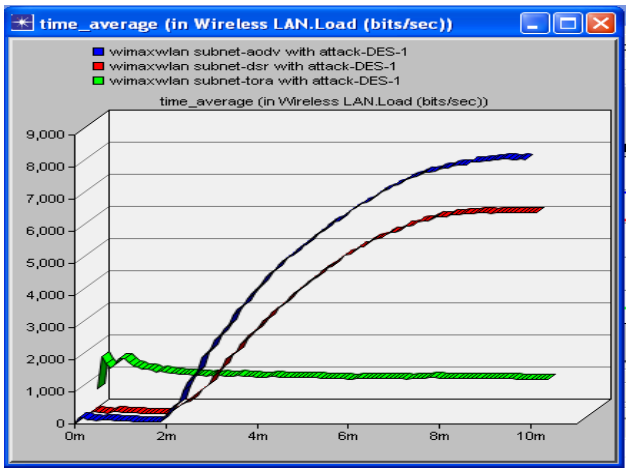


Figure-15 WLAN Load with Black Hole Attack

Above results shows that in both the scenarios with or without attack AODV is taking Maximum Load.

- **WLAN: Data Dropped(Bits/Sec)**

This fig 16 and fig 17 shows the comparison of WLAN Data Dropped using all three protocols over WiMAX-WLAN interface Network.

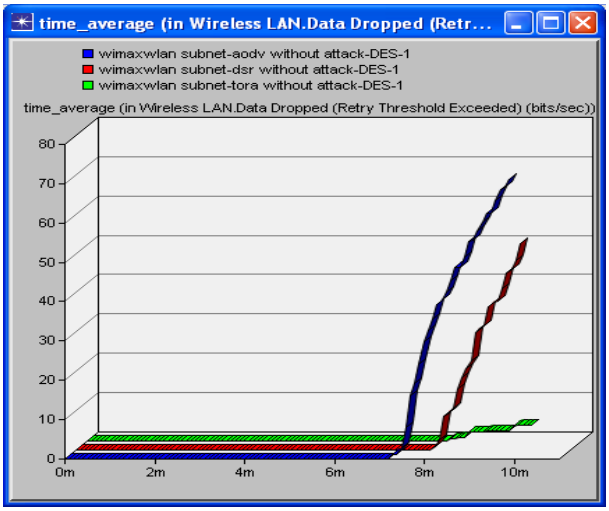


Figure-16 WLAN Data Dropped without Black Hole Attack

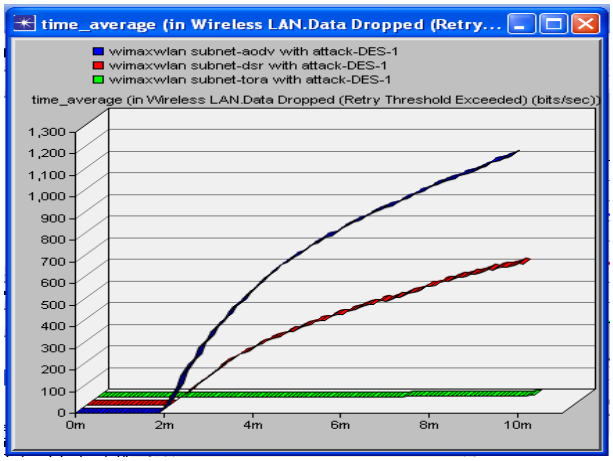


Figure-17 WLAN Data Dropped with Black Hole Attack

It is clear from above results that the WLAN Data Dropped is maximum by AODV in both scenario with or without Black Hole Attack. But the value of number of packets dropped is more in case of scenario with Black Hole Attack.

- **WLAN: Throughput(Bits/Sec)**

This fig 18 and fig 19 shows the comparison of WLAN Throughput using all three protocols over WiMAX-WLAN interface Network.

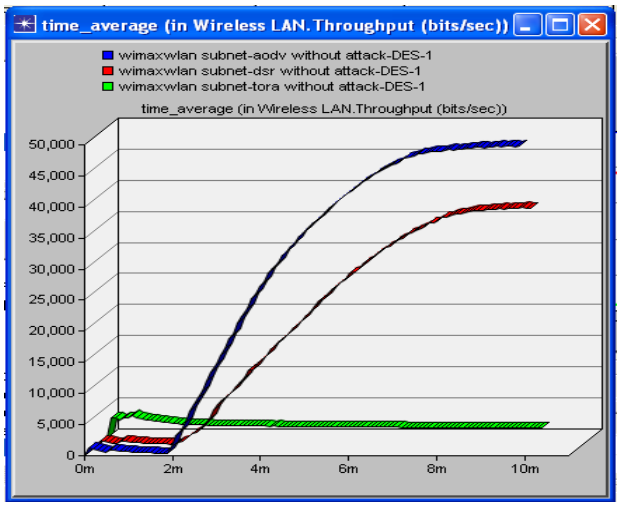


Figure-18 WLAN Data Dropped without Black Hole Attack

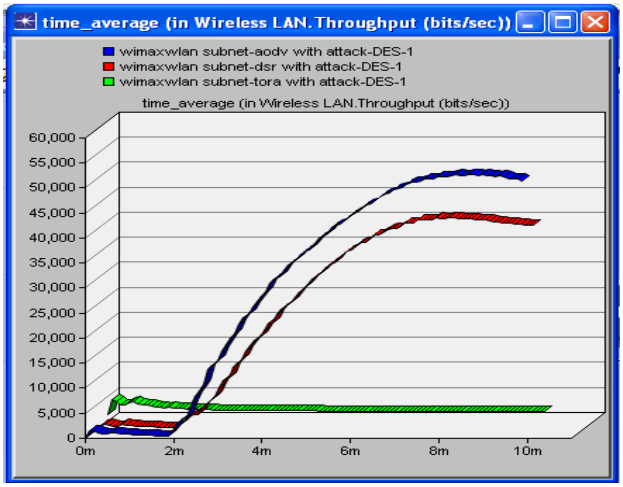


Figure-19 WLAN Throughput with Black Hole Attack

From above results , it is clear that the Throughput of the scenario without attack shown in first graph is best by AODV but also with Black Hole Attack AODV is giving Maximum Throughput.

VII. CONCLUSION

After performing the simulation over the two models that is with and without Black Hole Attack, under the effect of three routing protocols AODV, DSR, TORA; the results are made with the help of OPNET 14.5 modeler. We have made conclusions after analyzing these results. The first thing which is concluded is that on WiMAX, under without Black Hole Attack scenario AODV is performing best under all performance metrics. AODV gives minimum delay, minimum load and maximum throughput but under attacked scenario,AODV as well as TORA is giving best performance under all metrics. Both give minimum delay, minimum load and maximum throughput and the second conclusion is that on WLAN scenario, AODV is giving best performance under without attack and with attack. In both cases it gives minimum Delay, minimum Load and maximum Throughput.

VIII. FUTURE WORK

In future, the research can be done on the integrated scenario of WiMAX and WLAN by taking different 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 woun hole attack, water torture attack, sybil attack, jellyfish attack etc.

ACKNOWLEDGMENTS

I thank Dr. Jyotsna Sengupta who guided me for this work with her support and encouragement throughout the research process.I further like to thank my family for their support, tolerance andencouragement during my work.

REFERENCES

[1] Abdourahime Gaye, Karim Konate," A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc Network" International Journal of Future Generation Communication and Networking Vol. 4, No. 2, June, 2011

[2] Ali Khayatzadeh Mahani, Shervin Ehrampoosh "Secure Routing Protocols: Affections on MANETsPerformance", International Journal of Communications and Information Technology, IJCIT-2011-Vol.1-No.1 Dec. 2011

[3] Ahmad Mebadi, Mehdi Medadian, Elham Shahri , "Combat with Black Hole Attack in AODV Routing Protocol" , Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference, Page(s): 1 – 5.

[4] B.Sridevi, M.Brindha, R.Umamaheswari, Dr.S.Rajaram, "IMPLEMENTATION OF SECURE and COST EFFECTIVE AUTHENTICATION PROCESS IN IEEE 802.16e WiMAX" .

[5] C. K. Nagpal, Chirag Kumar, Bharat Bhushan, Shailender Gupta, "A Study of Black Hole Attack on MANET Performance." International Journal of Modern Education and Computer Science, IJMECS Vol.4, No.8, August 2012, PP.47-53

[6] Kamran Sameni, Nasser Yazdani, Ali Payandeh," Analysis of Attacks in Authentication Protocol of IEEE 802.16e", Int. J. Com. Net. Tech. 1, No. 1, 33-44 (2013)

[7] M. Deva Priya, Dr. M.L.Valarmathi, S. Aishwarya, K. Jaya Bharathi, "A Countermeasure for Black Hole Attack in Mobile WiMAX Networks", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) Volume 2, Issue 3, March 2013

[8] Naïm Qachri, Jean-Michel Dricot," On the Security of WLAN Access Points Integrated in 4G/LTE Architectures", Proc IEEE. in Local and Metropolitan Area Networks (LANMAN), 2013 19th IEEE Workshop, Page(s): 1 – 6

[9] Nidhi Purohit, Richa Sinha and Khushbu Maurya "Simulation study of Black hole and Jellyfish attack on MANET", INTERNATIONAL CONFERENCE ON CURRENT TRENDSiCONE–2011IN" TECHN, Page(s): 1 - 5

[10] Michel Barbeau ,"WiMax/802.16 threat analysis" 2005.

[11] Rakesh Jha, Upena Dalal, "WiMAX System Simulation and Performance Analysis under the influence of jamming for WiMAX systems", Wireless engineering and Technology(WET) journal by scientific research, Vol. 1, No.1, PP.20-26, July 2010

[12] Rakesh Jha, Upena D Dalal, "Location Based Performance of WiMAX Network for QoS with Optimal Base Stations " , Wireless Engineering and Technology, 2011, 2, 135-145

[13] Rakesh Jha, Upena D Dalal, Idris Z. Bholebawa," Performance Analysis of Black Hole Attack on WiMAX-WLAN interface network" 2012 Third International Conference on Computer and Communication Technology, Page(s): 303 – 308

[14] Semih Dokurer, Y. M. Erten, Can Erkin Acar, "Performance analysis of ad-hoc networks under black hole attacks" Proceedings. IEEE , Page(s): 148 - 153

[15] 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, 2011.

