Denial-of-Service

Black-hole Attack

Haril Mehta
Sonam Dhadiwal

INDEX

Chapter 1

Network Creation

ABSTRACT

1.1 Abstract

Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. In this period of wireless devices, Mobile Ad-hoc Network (MANET) has become an inseparable element for communication for mobile device. Consequently, significance in research of Mobile Ad-hoc Network has been growing since last few years. Due to this it is vulnerable to various kinds of security threats. A black-hole attack is such type of Denial-of-Service attack in which the attacker makes the source node send all the data packets to a black-hole node that ends up dropping all the packets. This project emphasis on developing and analyzing the attack and then detecting and preventing the malicious node by using AODV protocol in order to secure the overall network. AODV is an on-demand routing protocol that tries to discover a path only at the time when there is a requirement from mobile nodes in the network.

1.2 Introduction:

In Computer Networking, Black-hole attack or also called a packet drop attack is a denial-of-service attack, in which the router is supposed to relay packets instead of discarding them. In this attack, the attacker receives requests for routes. Black-hole is a place in the network where incoming and outgoing traffic is silently dropped, without giving the information to the source that data did not reach its targeted recipient. When the attacker receives a request for a route to the target node, the attacker creates a reply consisting of an extremely short route. If the malicious reply reaches the requesting node before the reply from the actual node, a forged route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to drop the packets to perform a Denial-of-Service attack. When checking on the topology, the black-holes are invisible and it cannot be detected by monitoring the lost traffic.

Main aim of this simulation is to evaluate and improve the performance of AODV routing protocol under Blackhole attacks. Mobile ad hoc network(MANET) is simulated using OPNET modeler and three scenarios are created. First scenario has normal MANET working conditions with AODV routing protocol, second scenario has Blackhole attacks and third scenario has improved AODV working conditions. AODV routing protocol parameters and wireless LAN parameters are configured.

1.3 Steps to create network for Blackhole attack:

1. Open the software **Riverbed Modeler Academic Integration** that we are going to use to build the project.

2.Click **file** Menu and select the option **New**

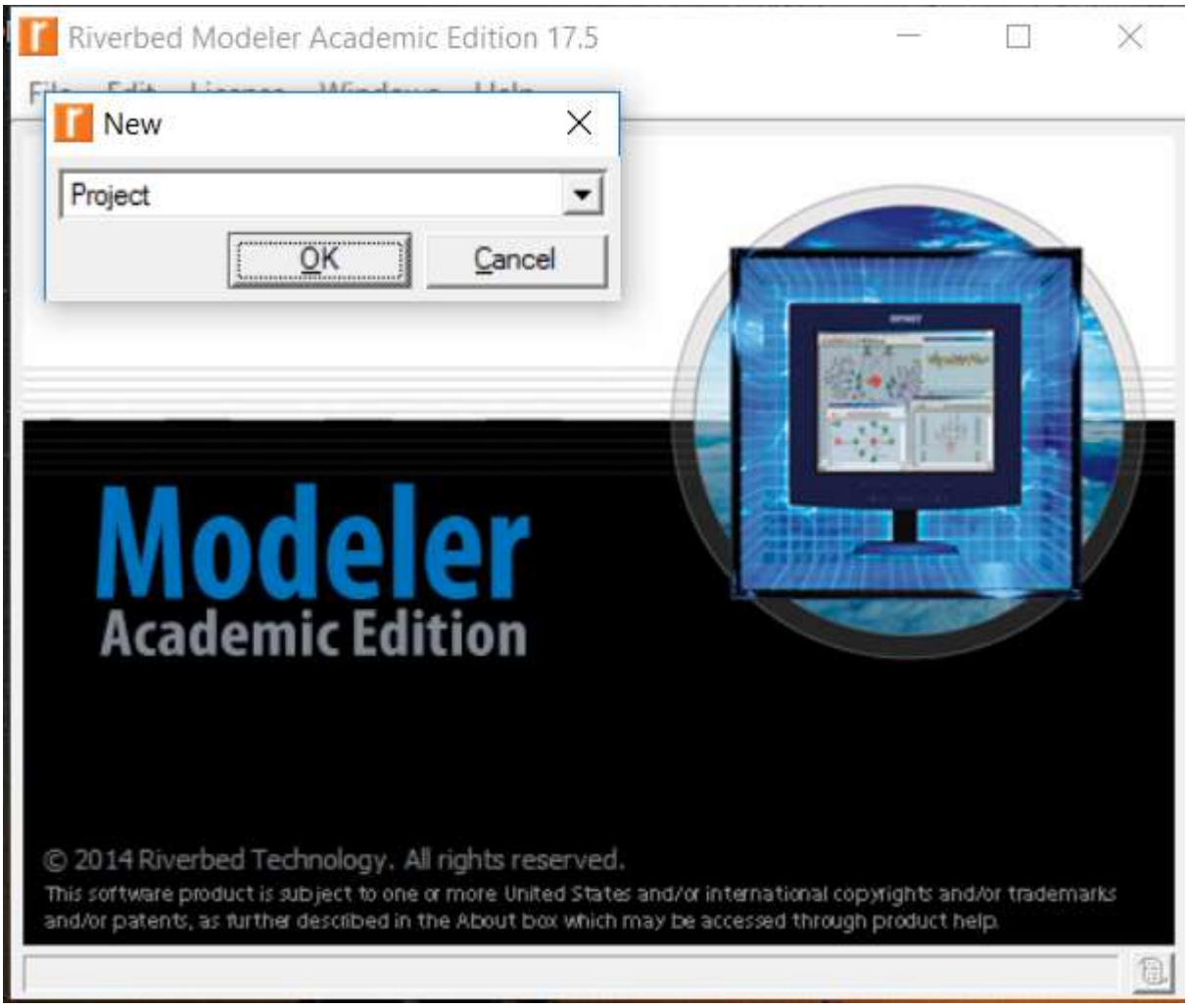


Figure 1.1

3. Click **ok** and then give the name for the project **Blackhole Attack** and name the scenario as **Normal scenario**. Do not forget to enable the checkbox of Startup Wizard.

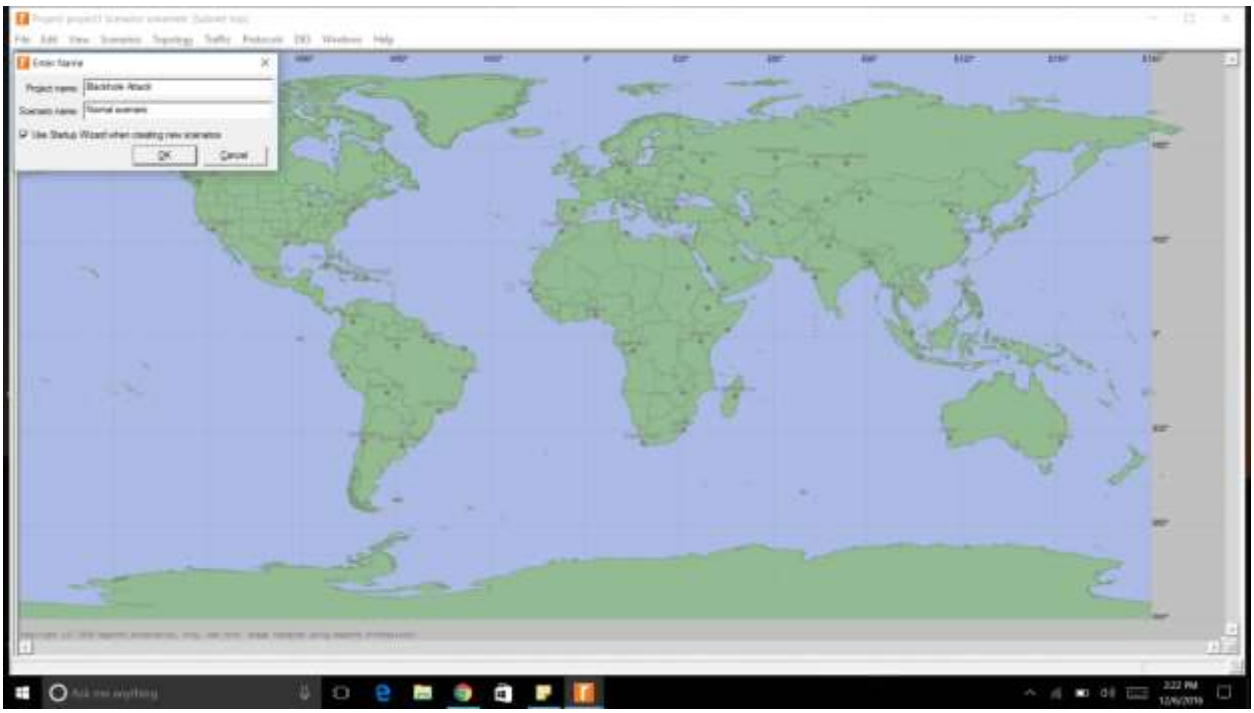


Figure 1.2

4. In the startup wizard: Initial toplogy dialog box, select **create empty scenario** and click **next**

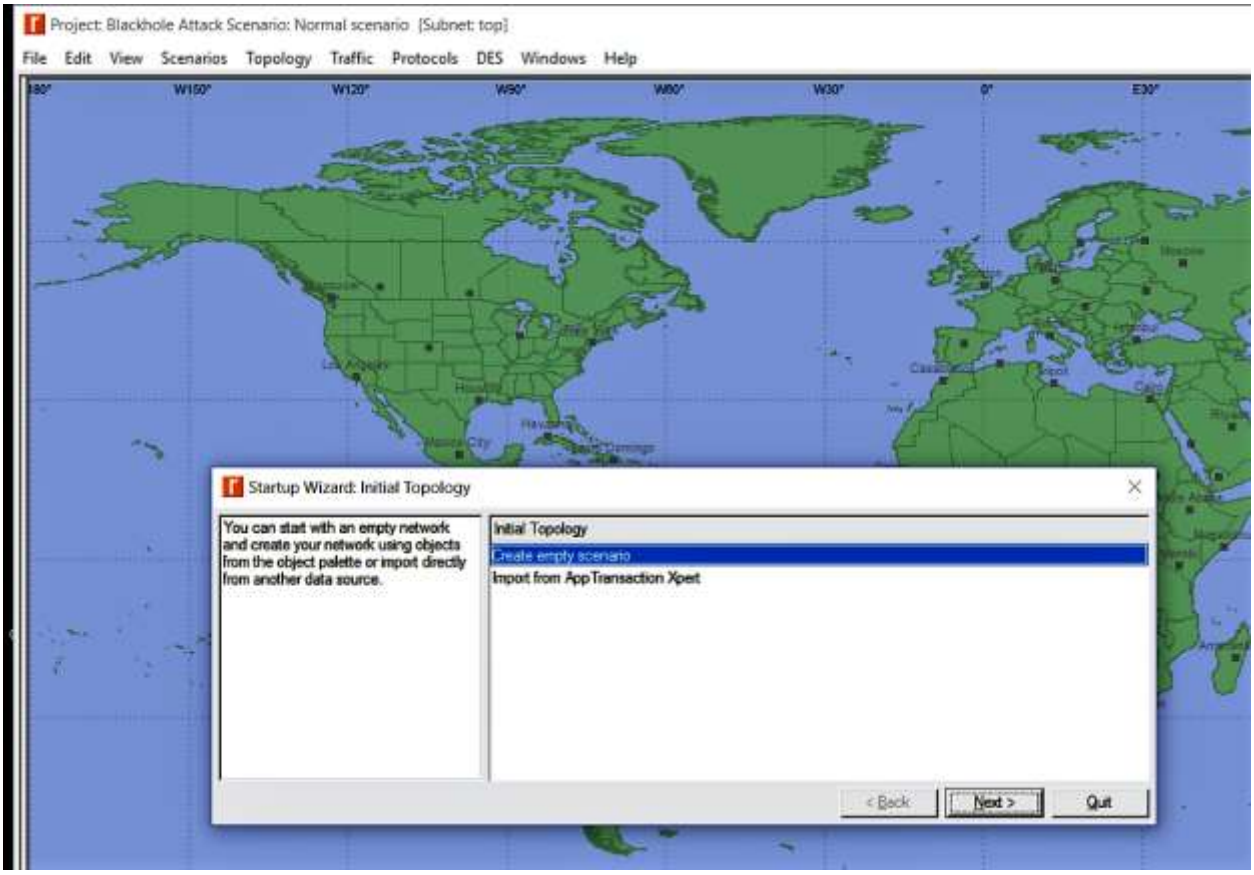


Figure 1.3

5. Select **campus**. Check use metric system. Click **next**

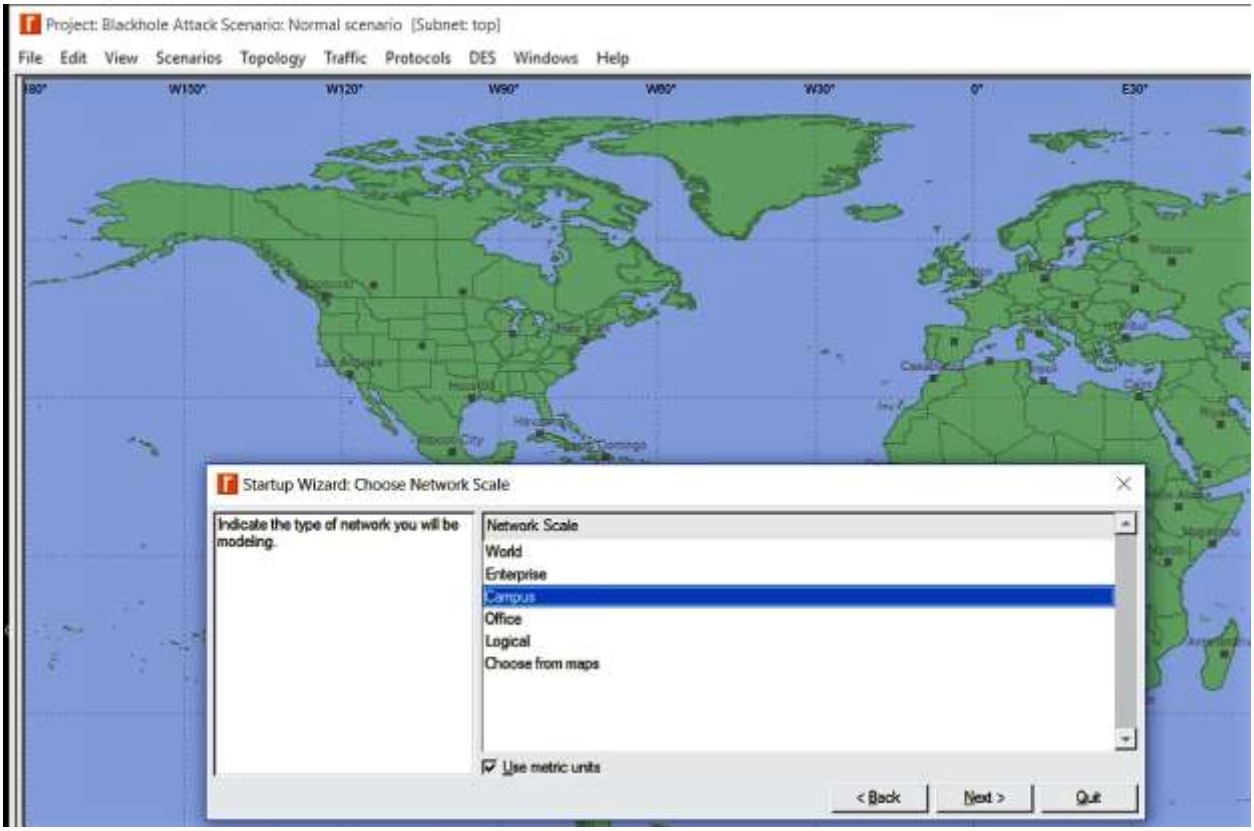


Figure 1.4

6. Specify Size in the wizard as follows:

X span :1000 **Y span : 1000** **Units :Meters** Click **next**

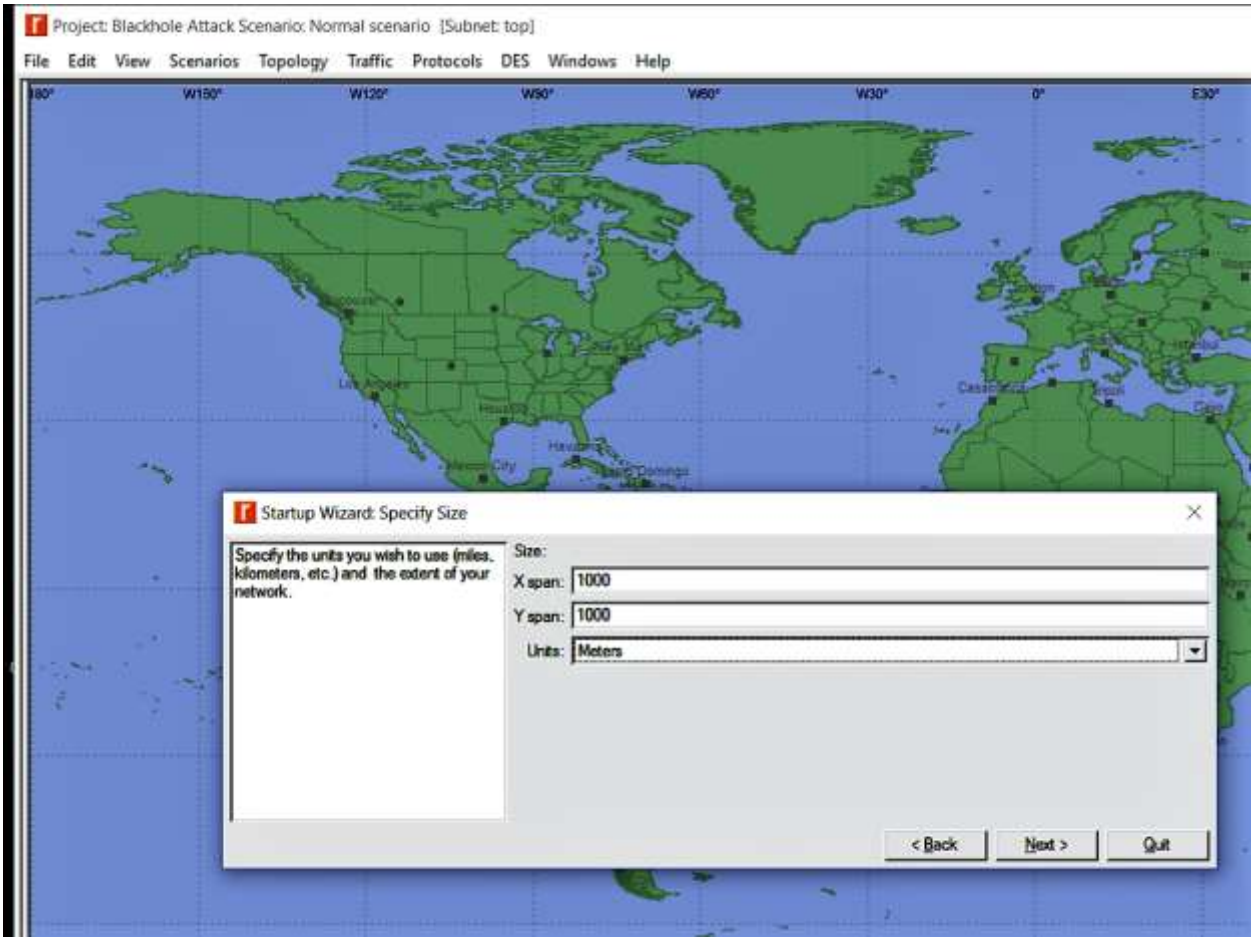


Figure 1.5

7. In select technology choose **MANET** and set its value to '**YES**'. Click **next.**

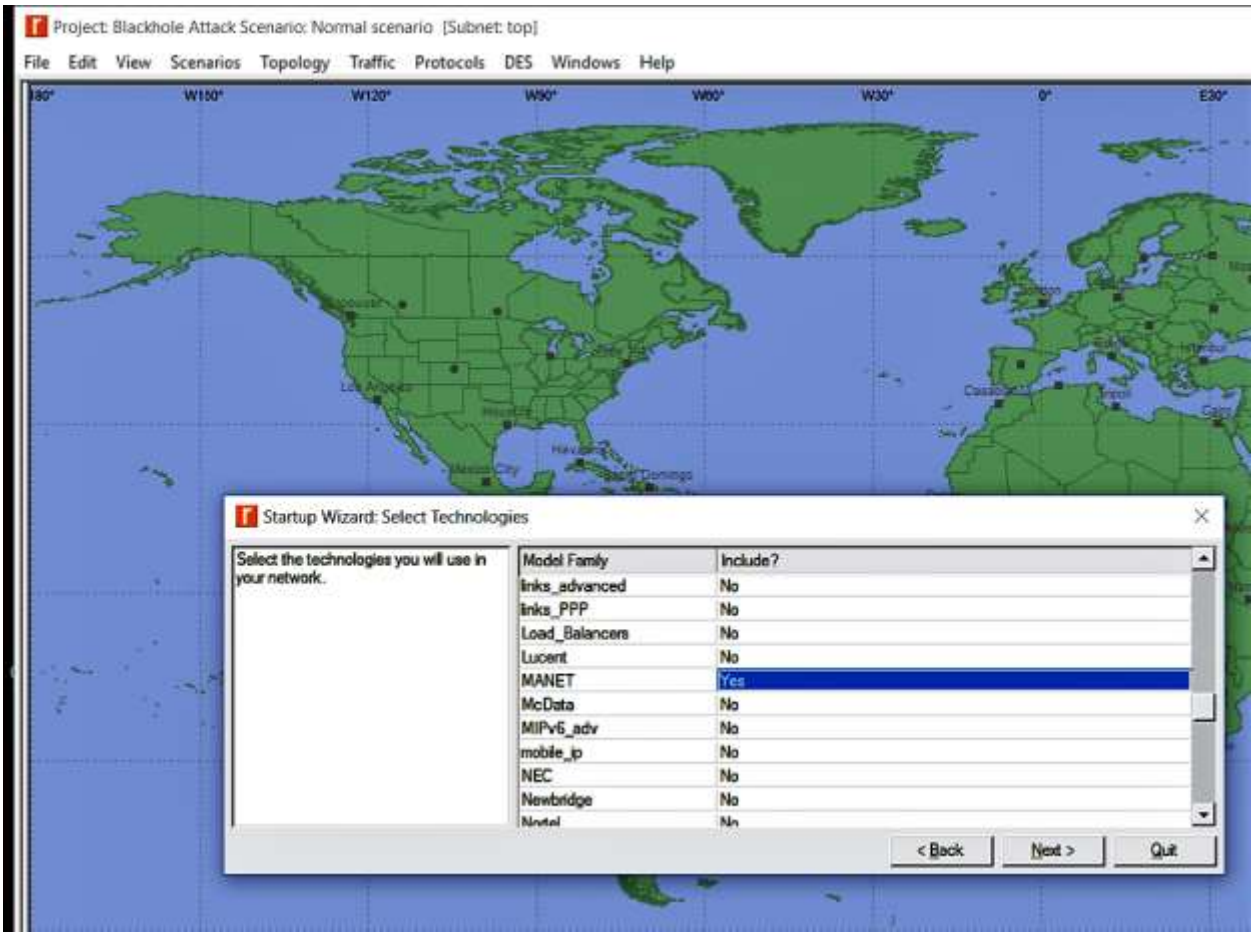


Figure 1.6

8.Open the **object palette** . In Node Module select **wlan wkstn**.

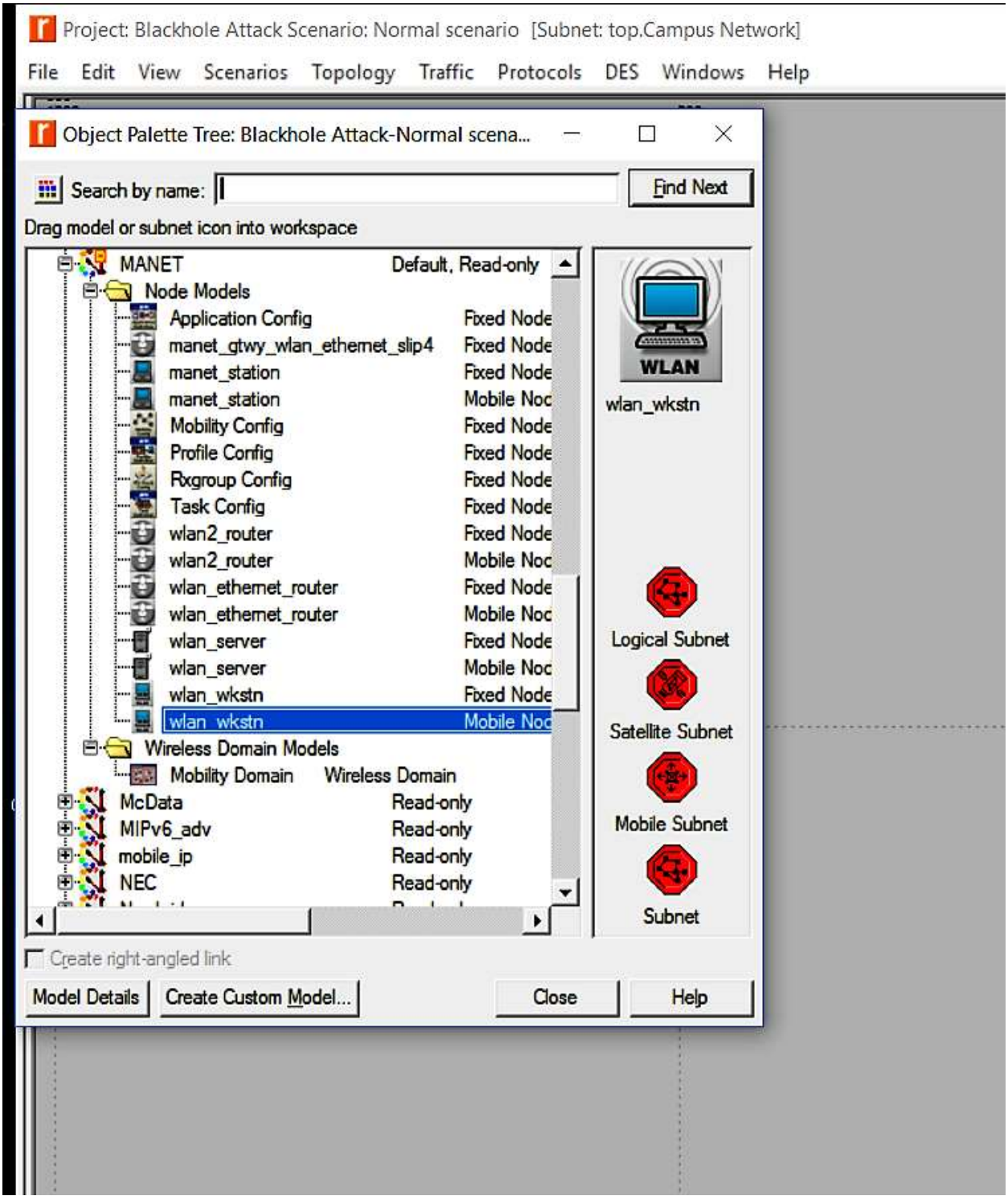


Figure 1.7

9.Similar to node creation from above step get **application definition, profile definition and mobility config.**

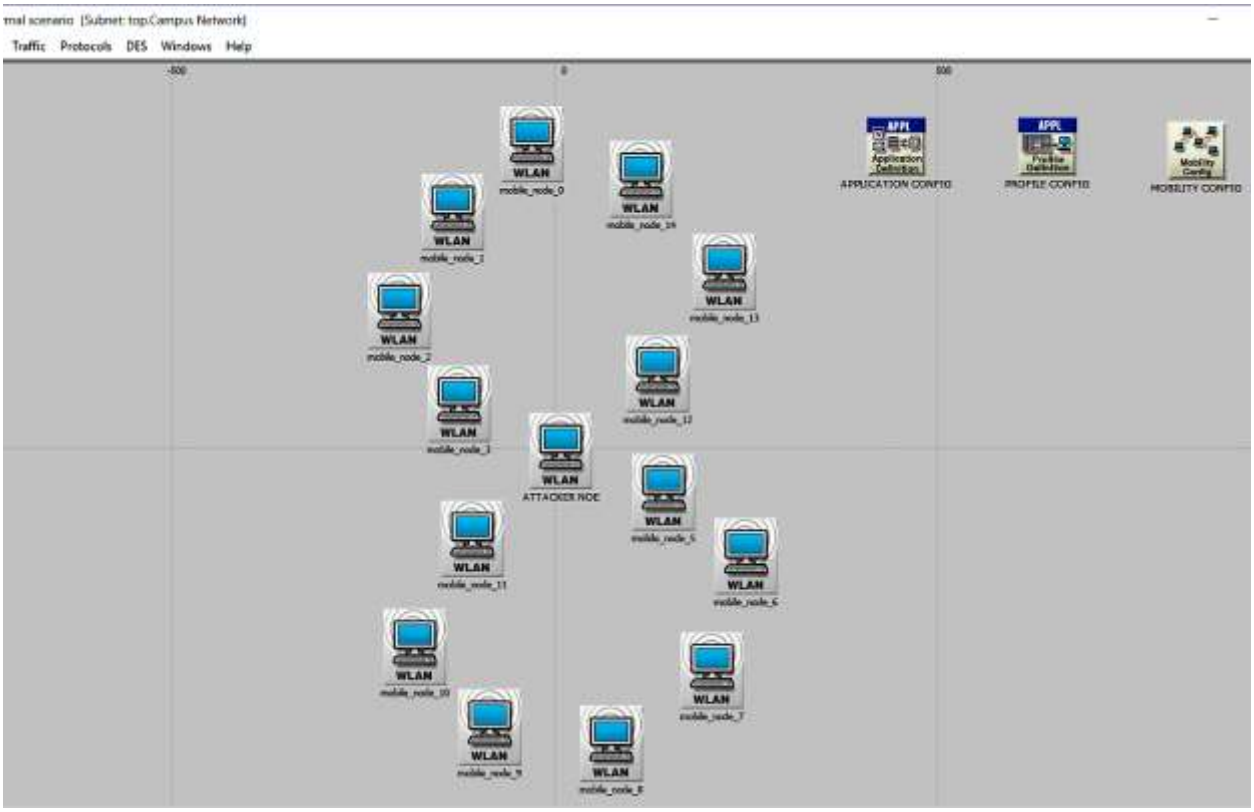


Figure 1.8: Plain network creation without any attachments

Chapter 2

Application Config Configurations

Once you are done with creation of network as specified in chapter 1 you can now do the configuration of application config created in chapter 1.

Steps for configuration:

1)Right click on application config and select attributes. In attributes under utility select the **Medium level** from drop down menu of **ftp attribute**

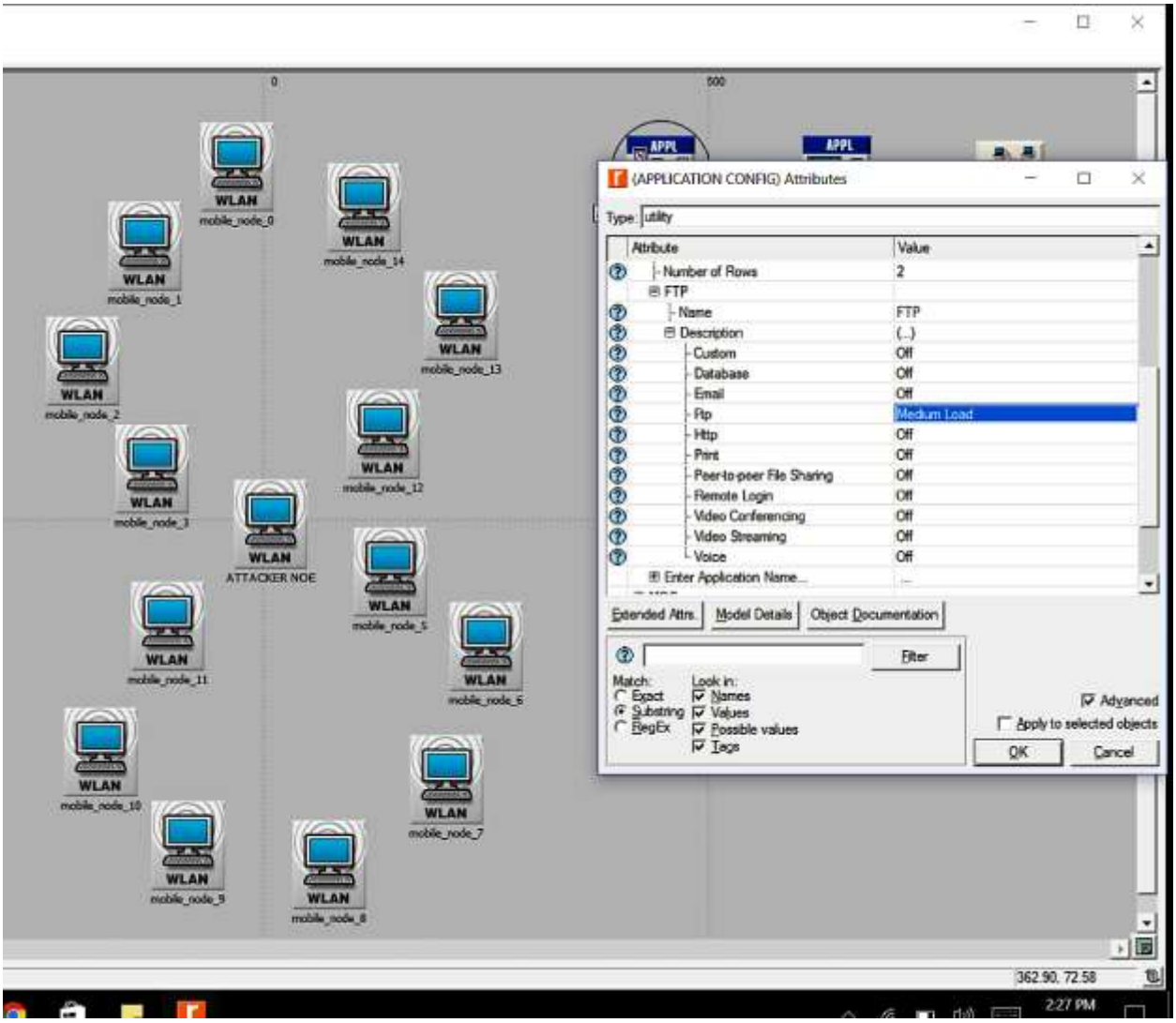


Figure 2.1

2) In http attribute select heavy browsing. Select radio button of substring. Check boxes-> Names,Values, Possible values, Tags,Advanced and then click OK.

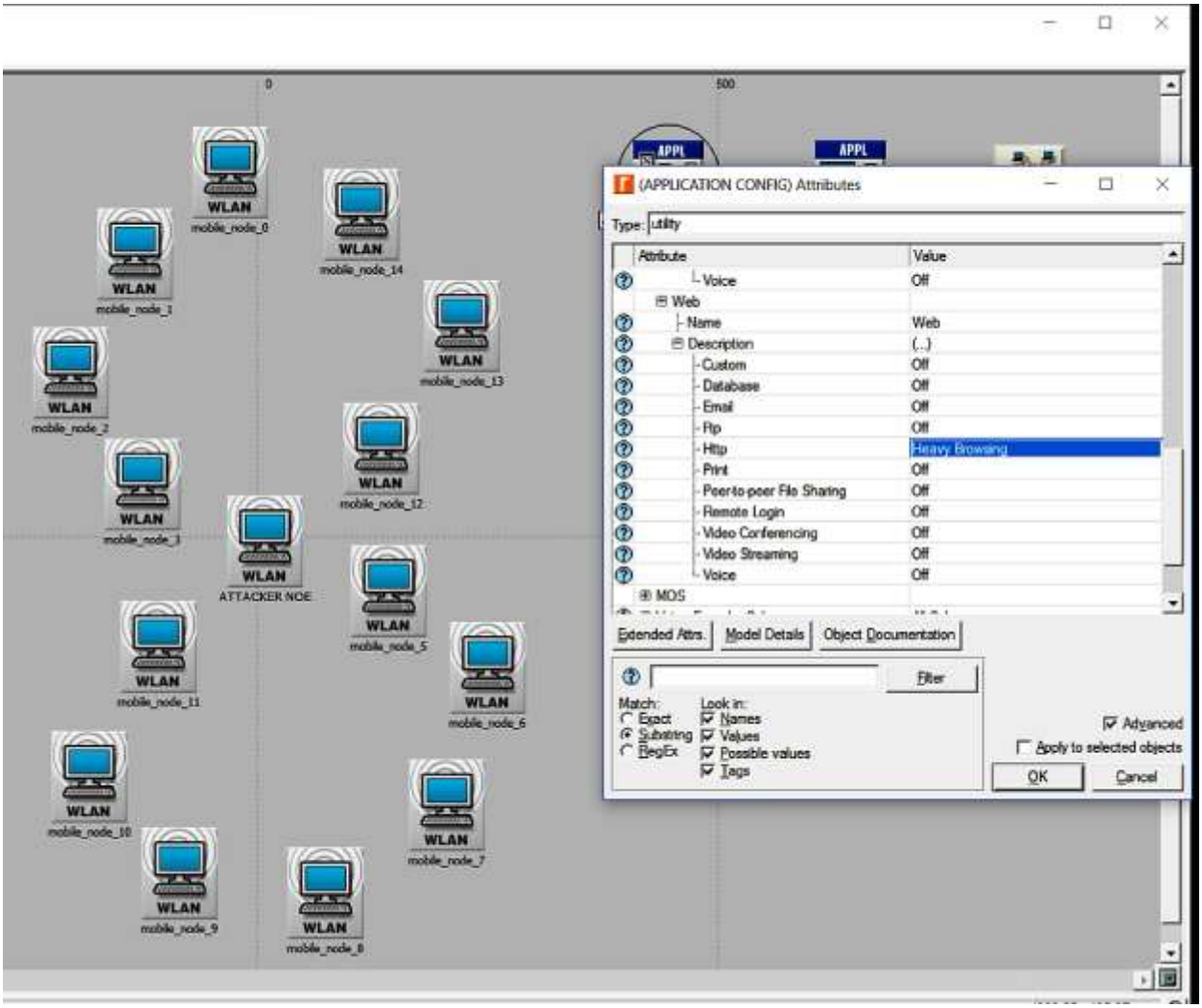


Figure 2.2

Chapter 3

Profile Config Configurations

In this chapter we will do configurations of profile config created in chapter1

Steps to create profile config configurations:

1.Right click profile config->select attributes->in utilities select ftp->set Repeatabiity to unlimited and in start time keep it **constant(100).** Select radio button of substring. Check boxes-> Names,Values, Possible values, Tags,Advanced and then click OK.

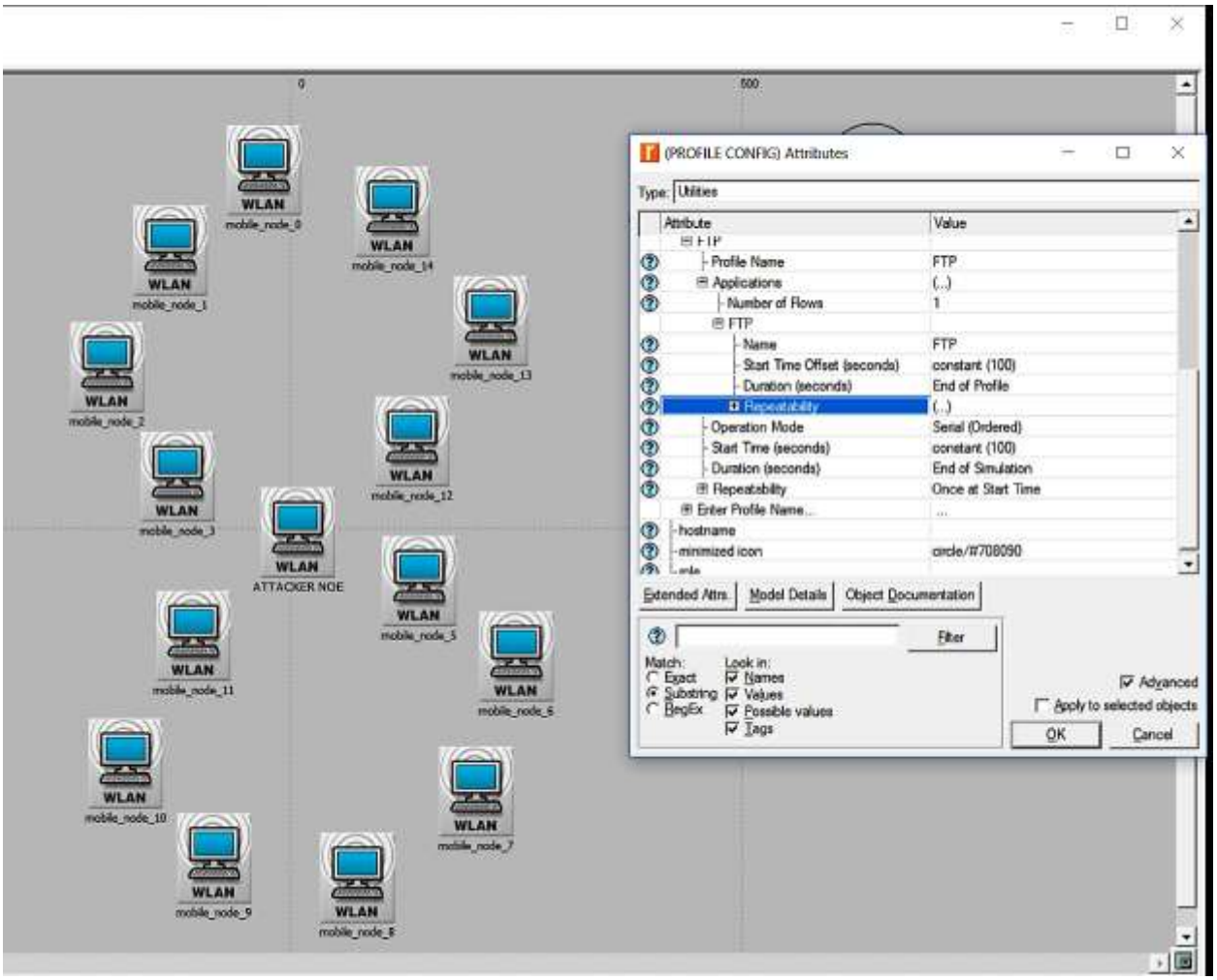


Figure 3.1

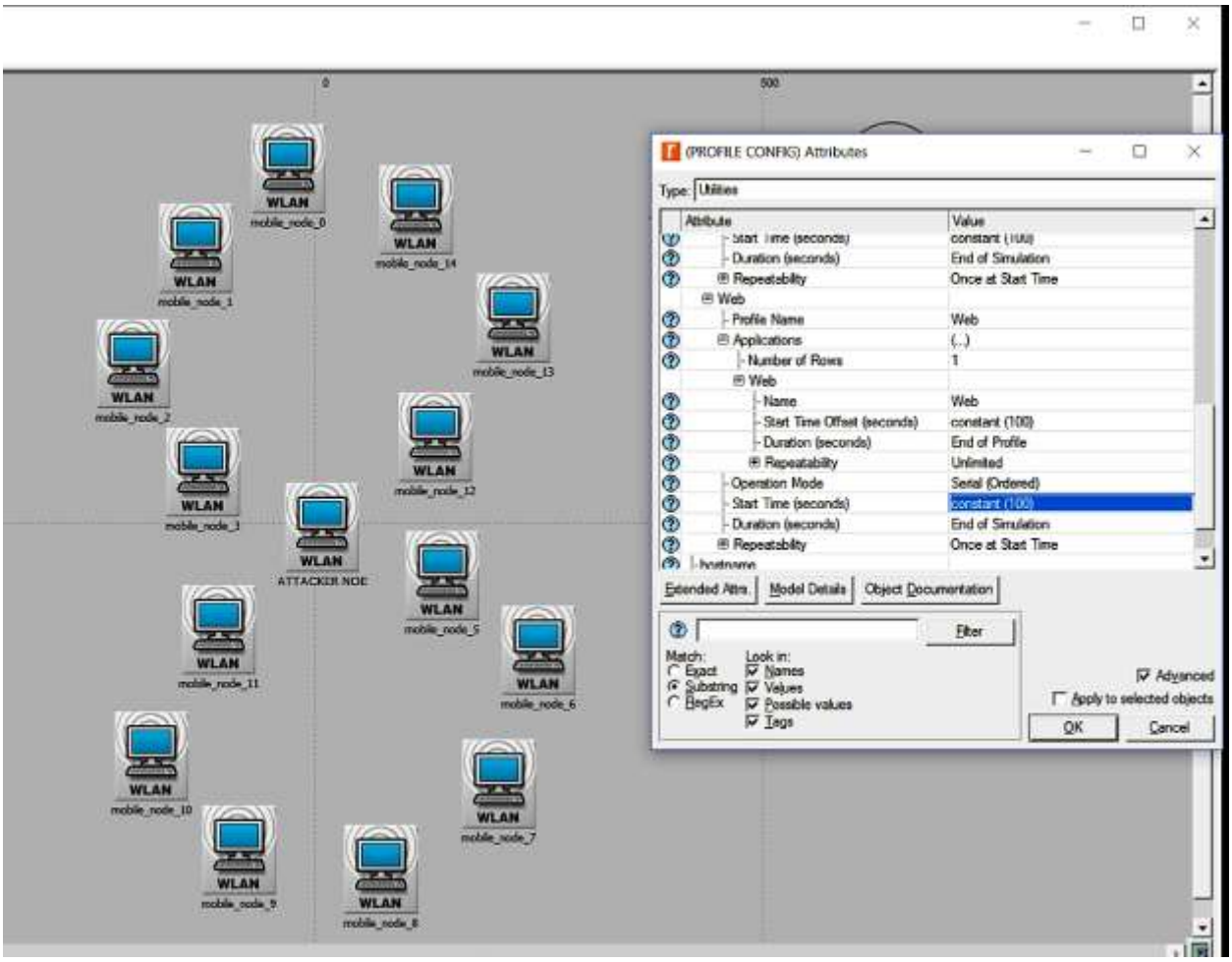

(PROFILE CONFIG) Attributes
Type: Utilities
Attribute
Value
Duration (seconds)
End of Simulation
Repeatability
Once at Start Time
Web
Profile Name
Applications
Number of Rows
Name
Start Time Offset (seconds)
constant (100)
End of Profile
Unlimited
Operation Mode
Serial (Ordered)
Start Time (seconds)
End of Simulation
Extended Attrs.
Model Details
Object Documentation
Filter
Match:
Exact
Substring
RegEx
Look in:
Names
Values
Possible values
Tags
Advanced
Apply to selected objects
OK
Cancel
WLAN
ATTACKER NOE

Figure 3.2

Chapter 4

Mobility Config Configurations

Let’s configure Mobility config created in chapter 1

In attribute tab of Mobility config under utilities select start time keep it **constant(15)** and click **OK.**

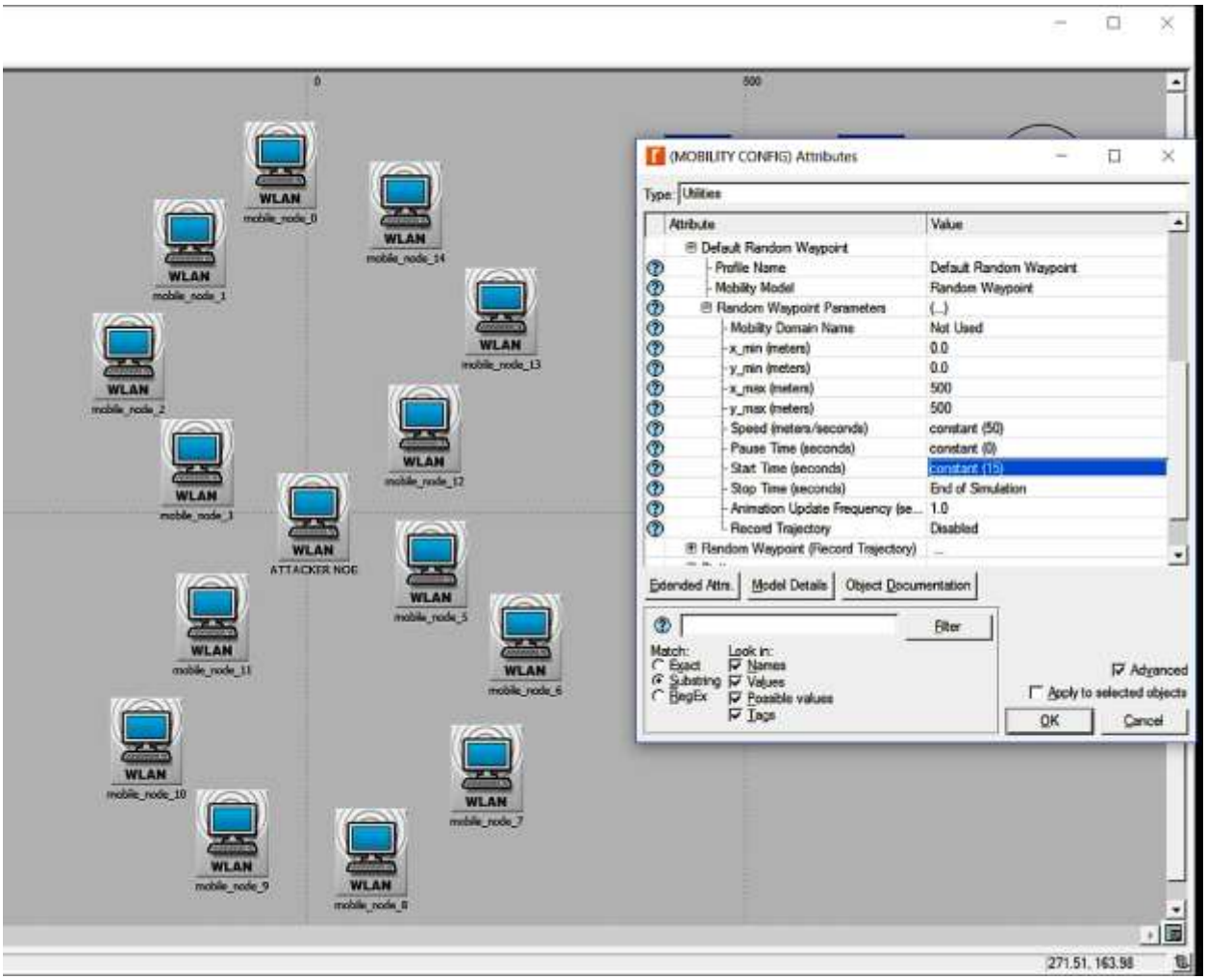


Figure 4.1

Chapter 5

Mobile Nodes Configuration

Steps to configure Mobile nodes:

1) Select all nodes->click attributes -> In trajectory attribute click **vector.**

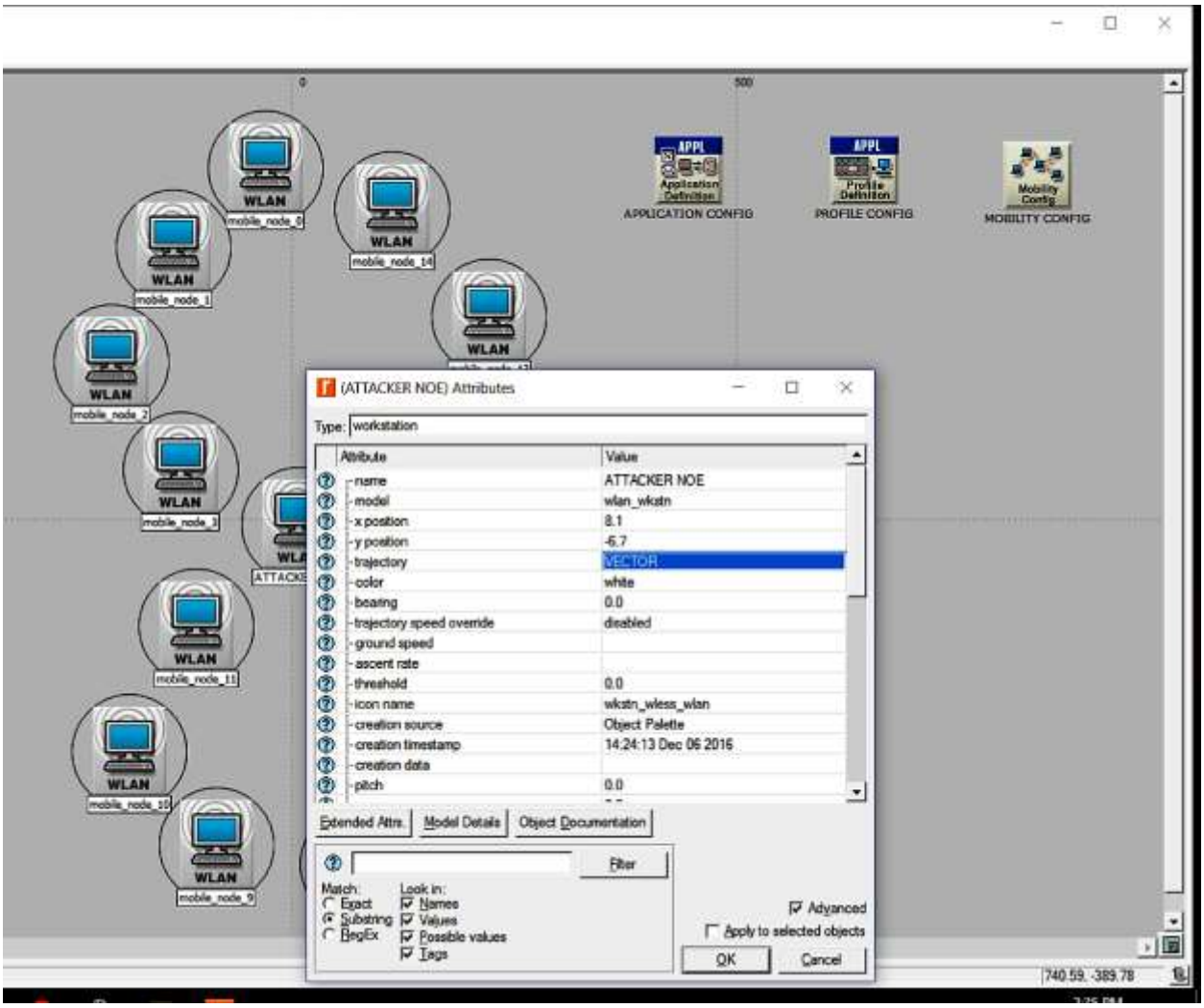


Figure 5.1

2) In AD-HOC routing protocol attribute select **AODV**

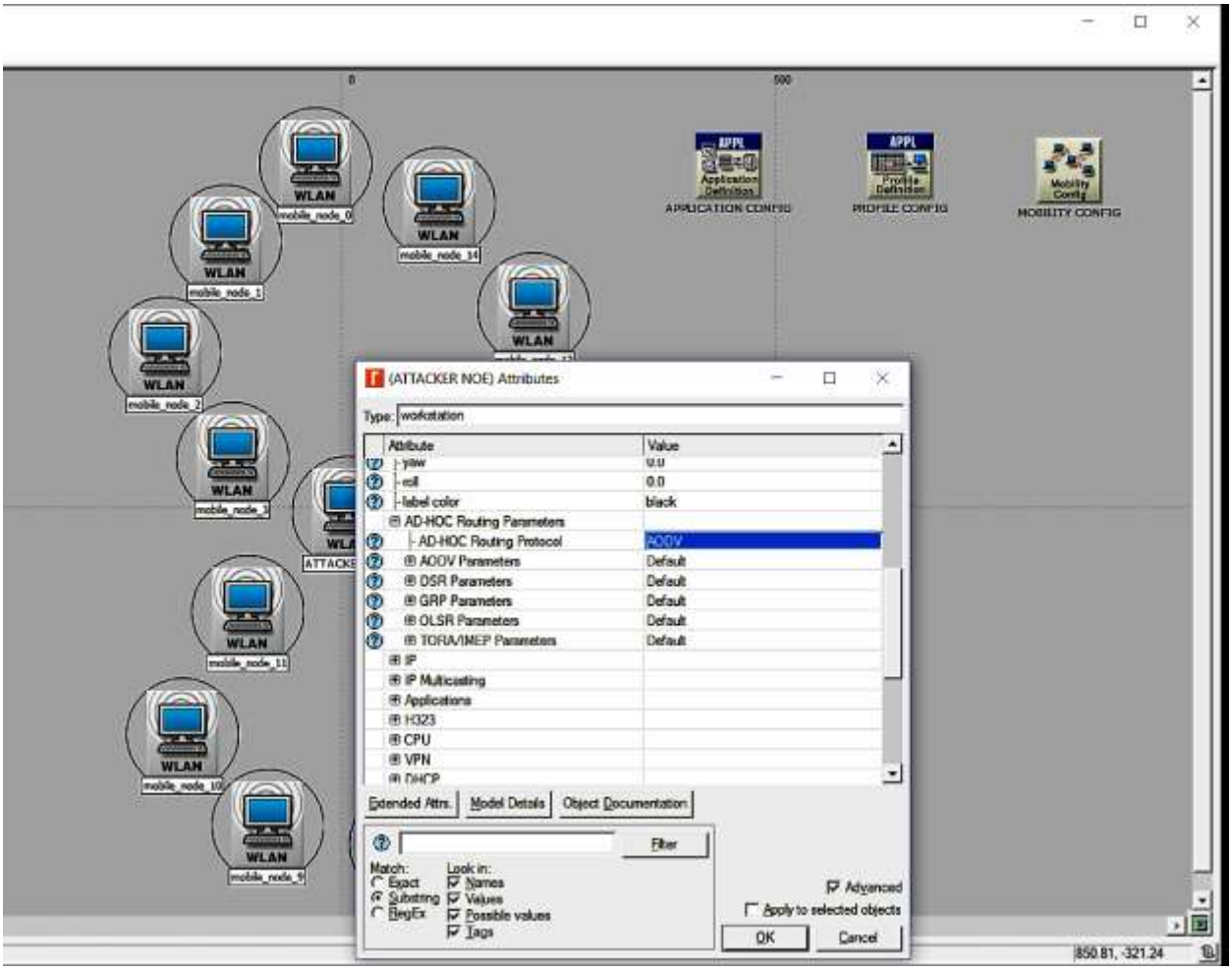


Figure 5.2

3) In wireless LAN parameters

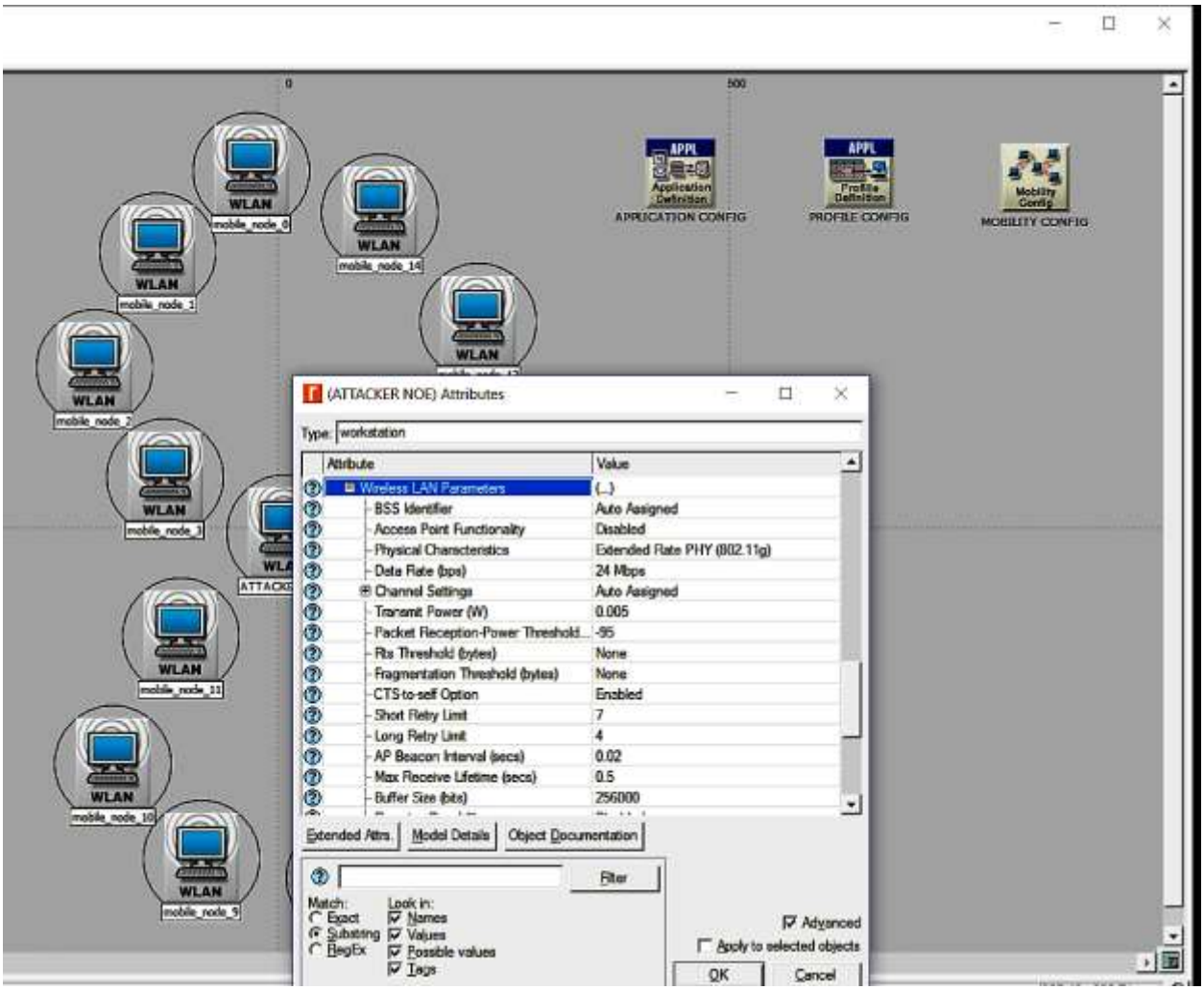


Figure 5.3

4.The following diagram shows how the whole figure will look once all attributes are set.

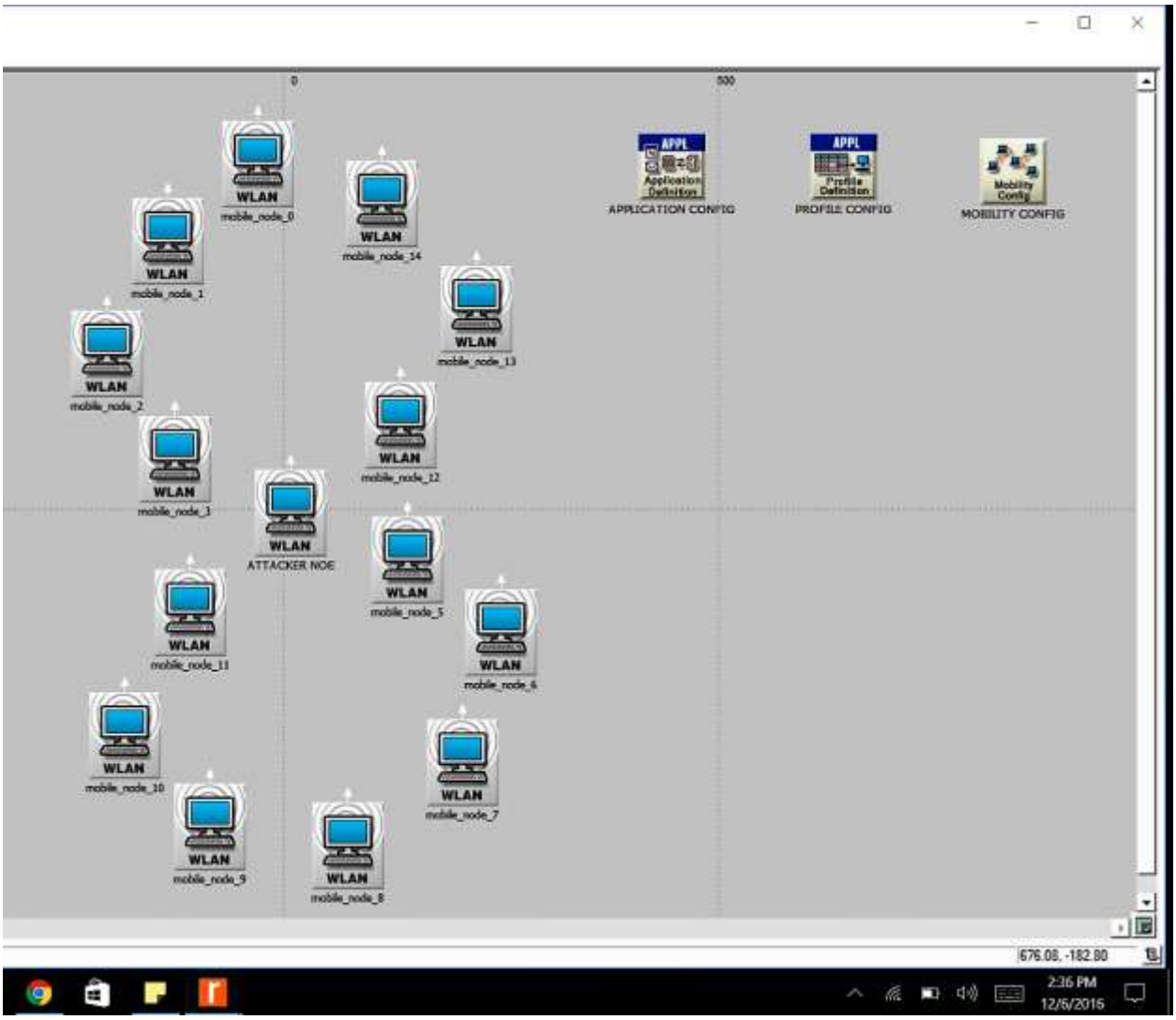


Figure 5.4

5.Now deploy the application

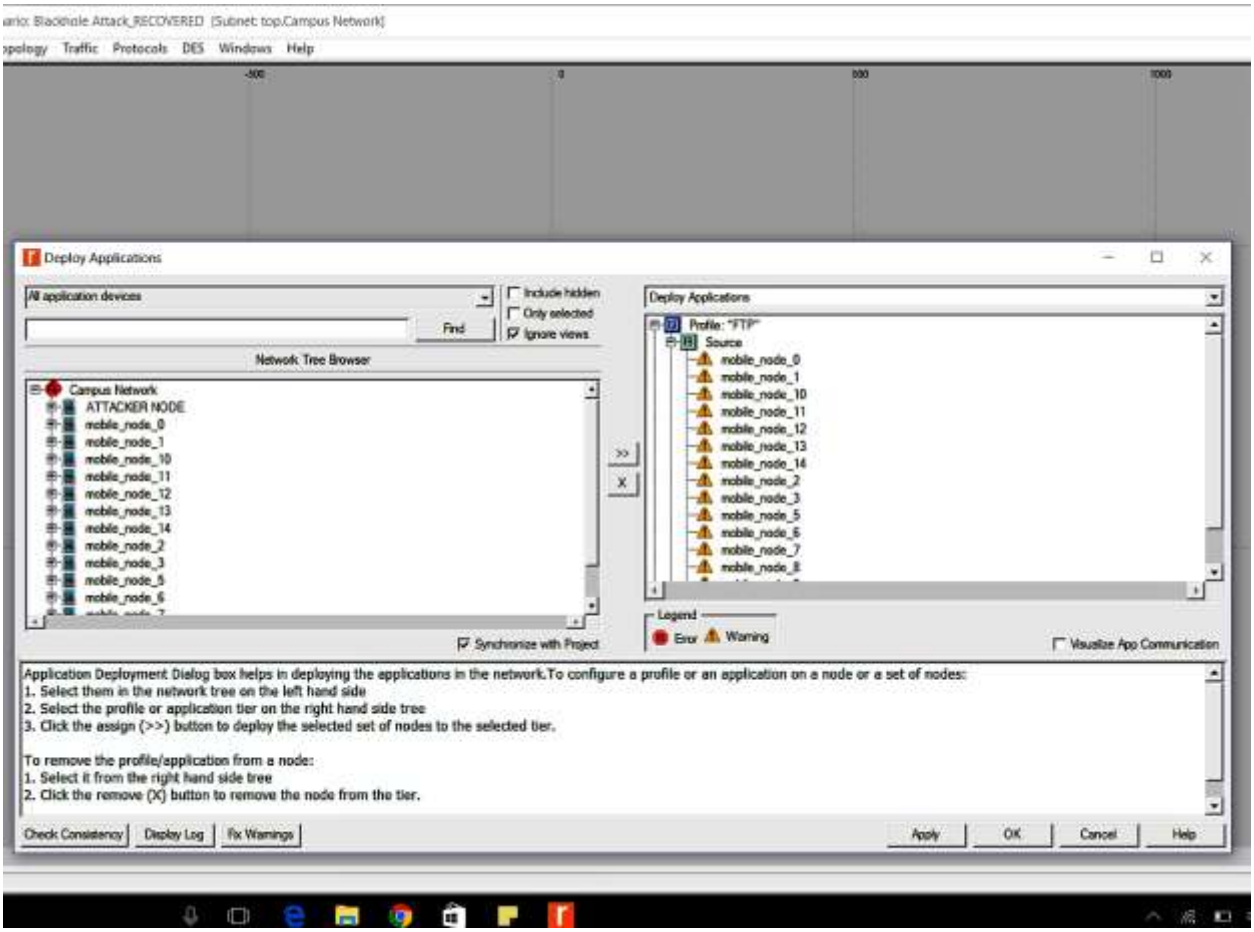


Figure 5.5:

6. You will see the attack performed:

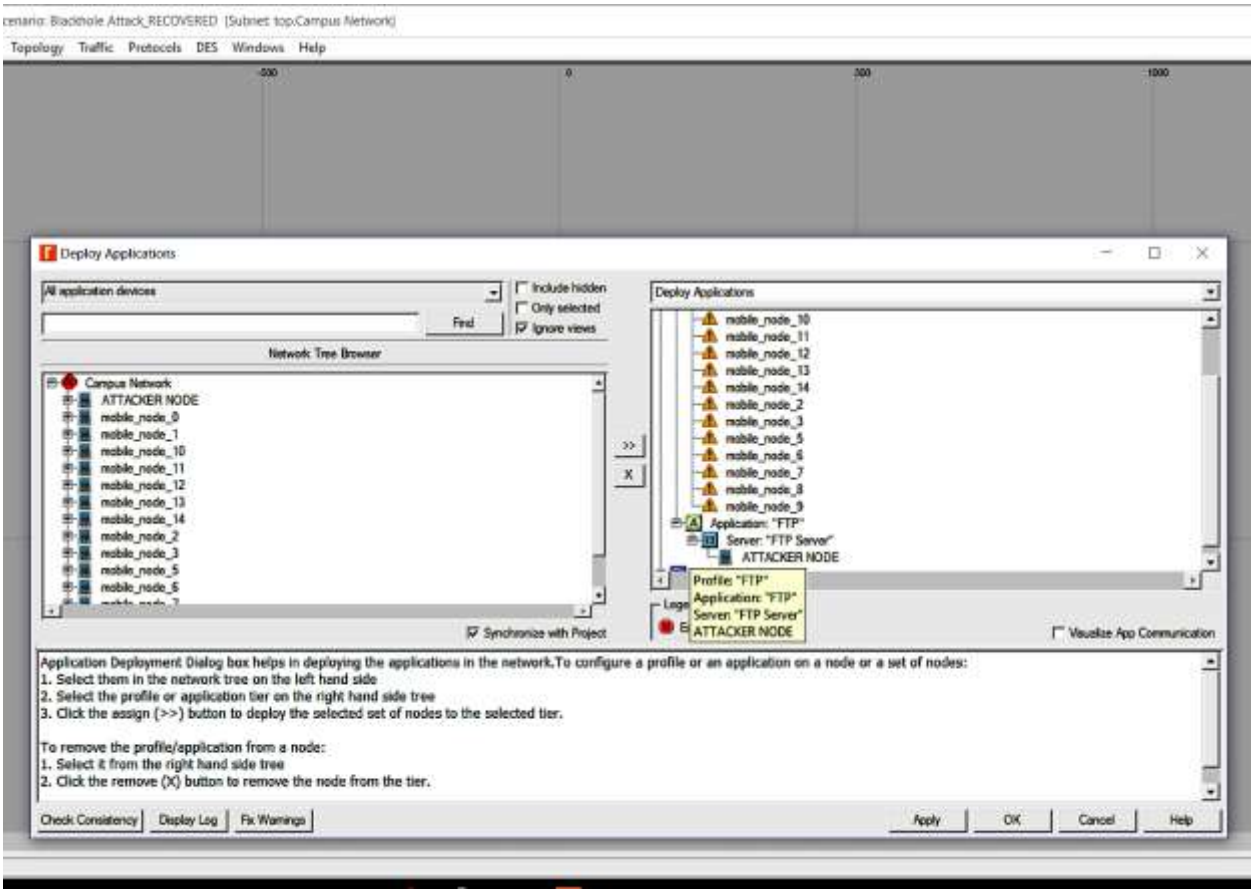


Figure 5.6:

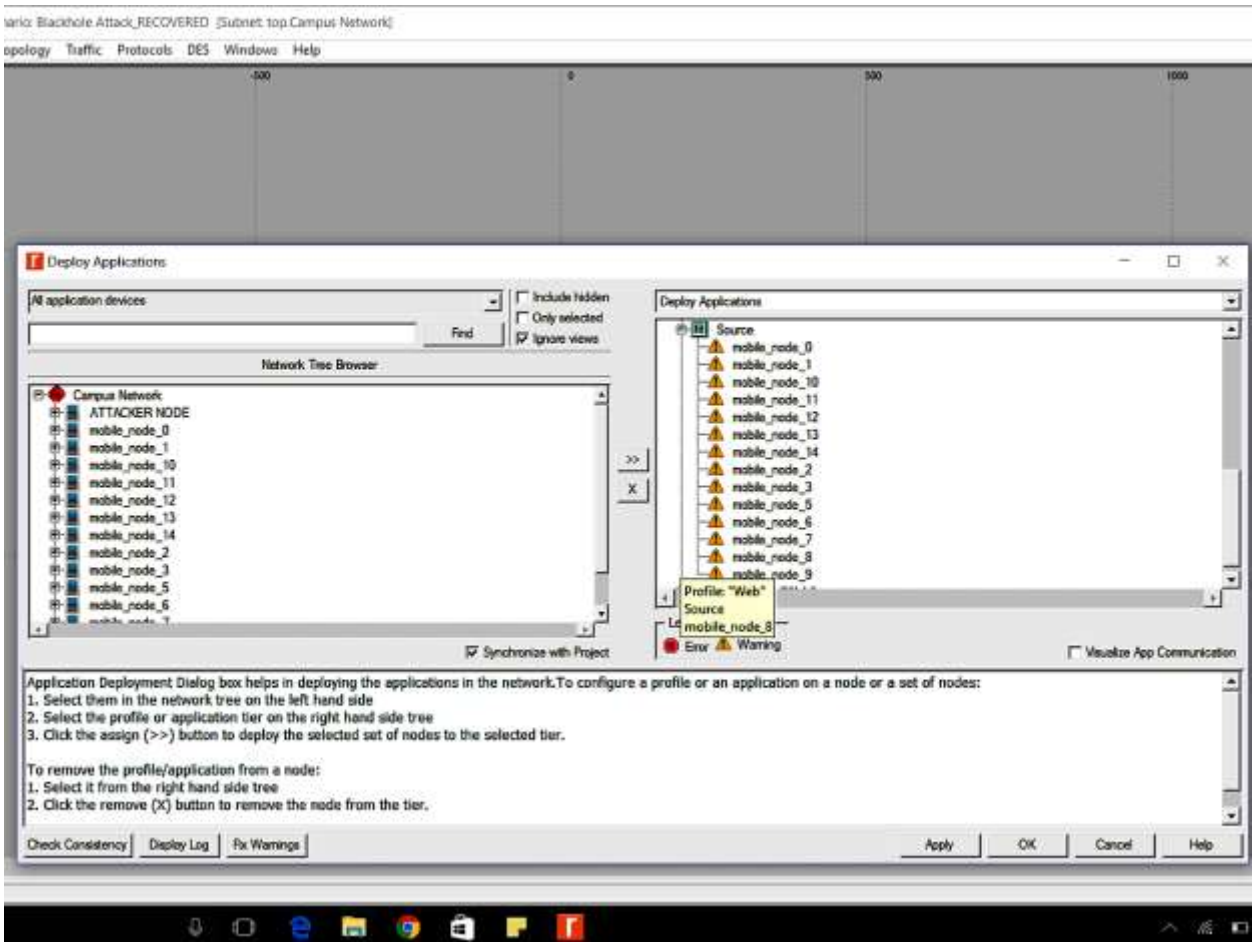

Deploy Applications
All application devices
Include hidden
Only selected
Ignore views
Find
Network Tree Browser
Campus Network
ATTACKER NODE
mobile_node_0
mobile_node_1
mobile_node_10
mobile_node_11
mobile_node_12
mobile_node_13
mobile_node_14
mobile_node_2
mobile_node_3
mobile_node_5
mobile_node_6
Synchronize with Project
Deploy Applications
Source
mobile_node_0
mobile_node_1
mobile_node_10
mobile_node_11
mobile_node_12
mobile_node_13
mobile_node_14
mobile_node_2
mobile_node_3
mobile_node_5
mobile_node_6
mobile_node_7
mobile_node_8
mobile_node_9
Profile: "Web"
Source
mobile_node_8
Error
Warning
Visualize App Communication
Application Deployment Dialog box helps in deploying the applications in the network.To configure a profile or an application on a node or a set of nodes:
1. Select them in the network tree on the left hand side
2. Select the profile or application tier on the right hand side tree
3. Click the assign (>>) button to deploy the selected set of nodes to the selected tier.
To remove the profile/application from a node:
1. Select it from the right hand side tree
2. Click the remove (X) button to remove the node from the tier.
Check Consistency
Display Log
Fix Warnings
Apply
OK
Cancel
Help

Figure 5.7:

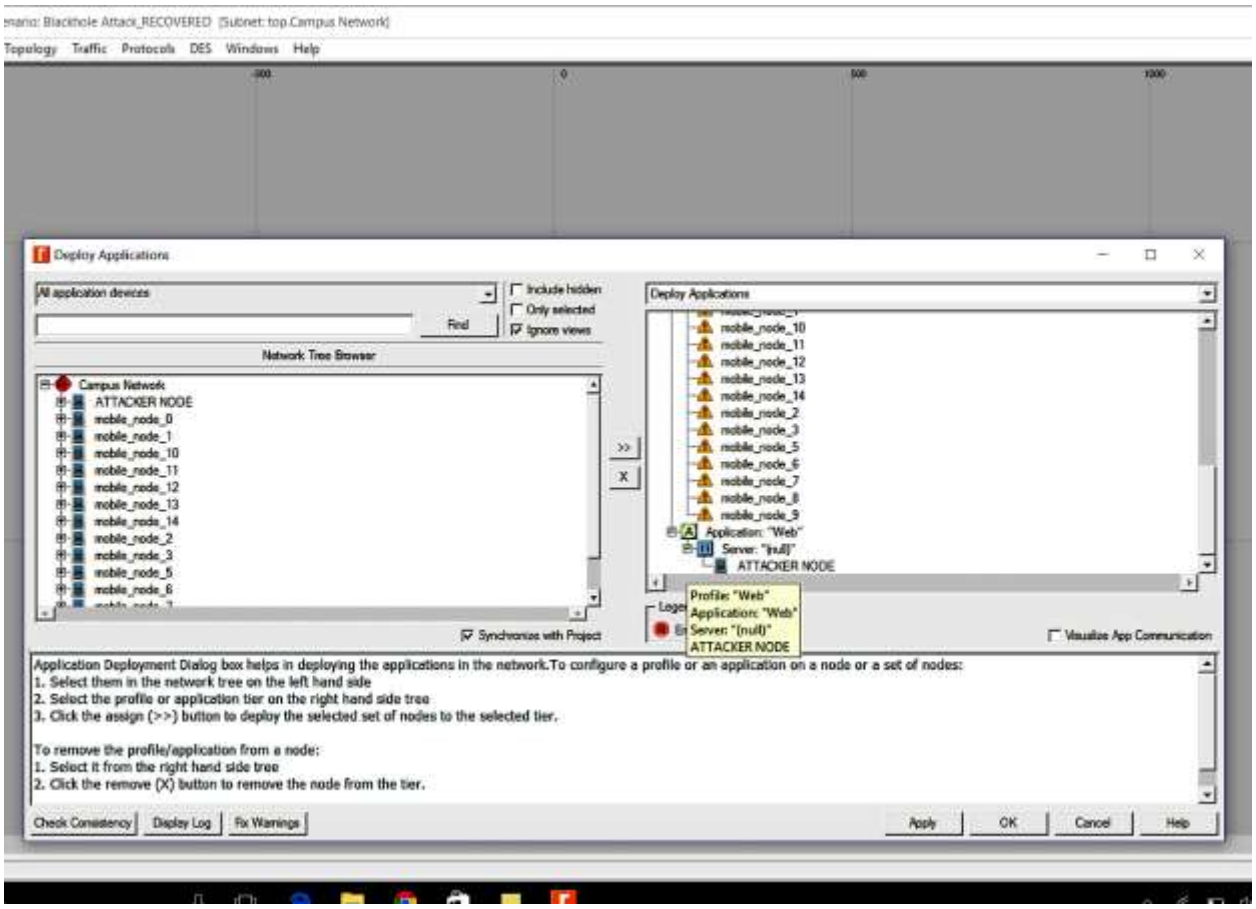

Topology Traffic Protocols DES Windows Help
Deploy Applications
All application devices
Include hidden
Only selected
Ignore views
Find
Network Tree Browser
Campus Network
ATTACKER NODE
mobile_node_0
mobile_node_1
mobile_node_10
mobile_node_11
mobile_node_12
mobile_node_13
mobile_node_14
mobile_node_2
mobile_node_3
mobile_node_5
mobile_node_6
mobile_node_7
mobile_node_8
mobile_node_9
Deploy Applications
Application: "Web"
Server: "(null)"
ATTACKER NODE
Profile: "Web"
Application: "Web"
Server: "(null)"
ATTACKER NODE
Synchronize with Project
Visualize App Communication
Application Deployment Dialog box helps in deploying the applications in the network.To configure a profile or an application on a node or a set of nodes:
1. Select them in the network tree on the left hand side
2. Select the profile or application tier on the right hand side tree
3. Click the assign (>>) button to deploy the selected set of nodes to the selected tier.
To remove the profile/application from a node:
1. Select it from the right hand side tree
2. Click the remove (X) button to remove the node from the tier.
Check Consistency
Display Log
Fix Warnings
Apply
OK
Cancel
Help

Figure 5.8:

Chapter 6:

Global statistics and simulation

Let’s start with simulation now.

Steps for simulation:

1)In choose results select AODV,FTP, HTTP ,Wireless LAN and click ok

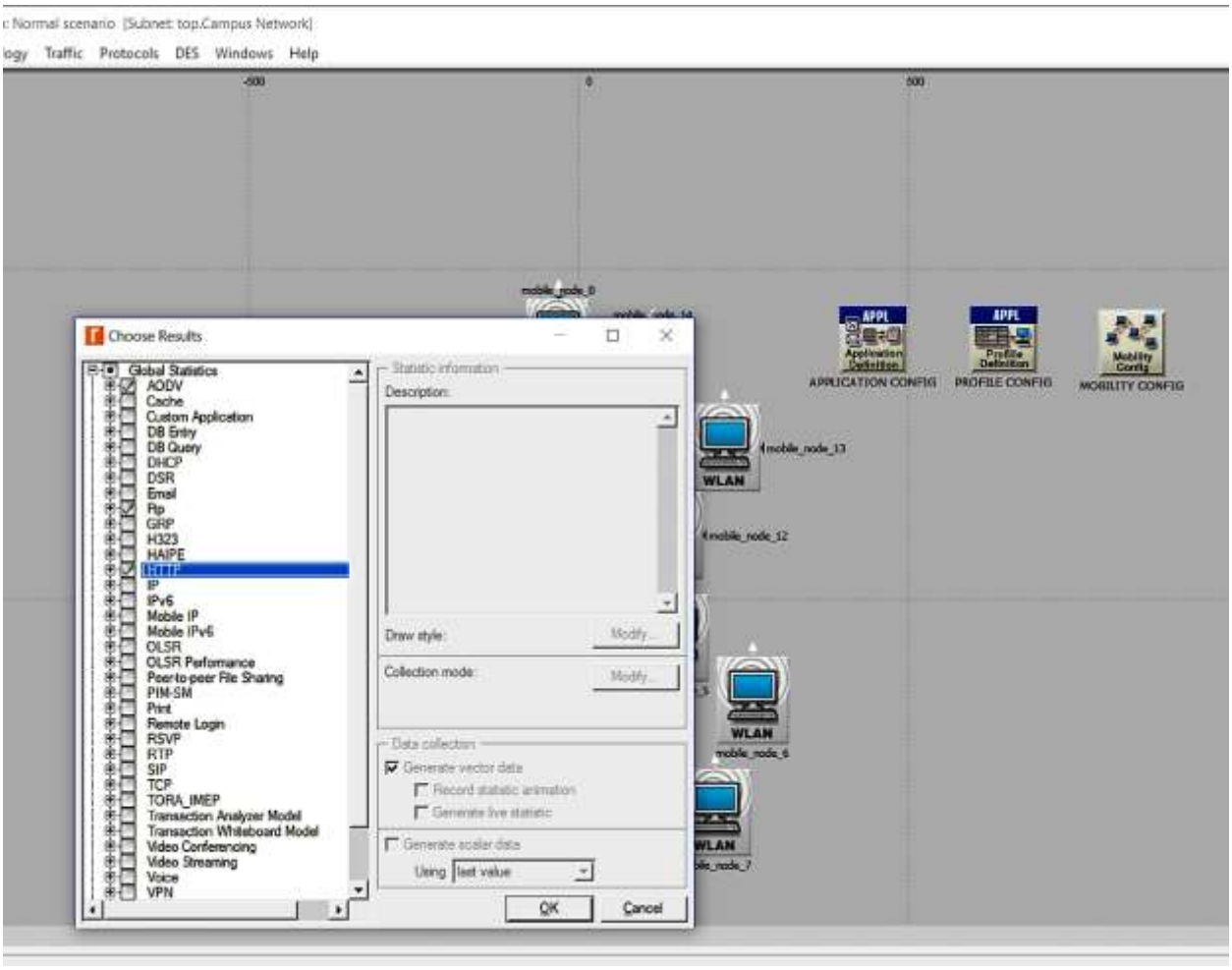


Figure 6.1:

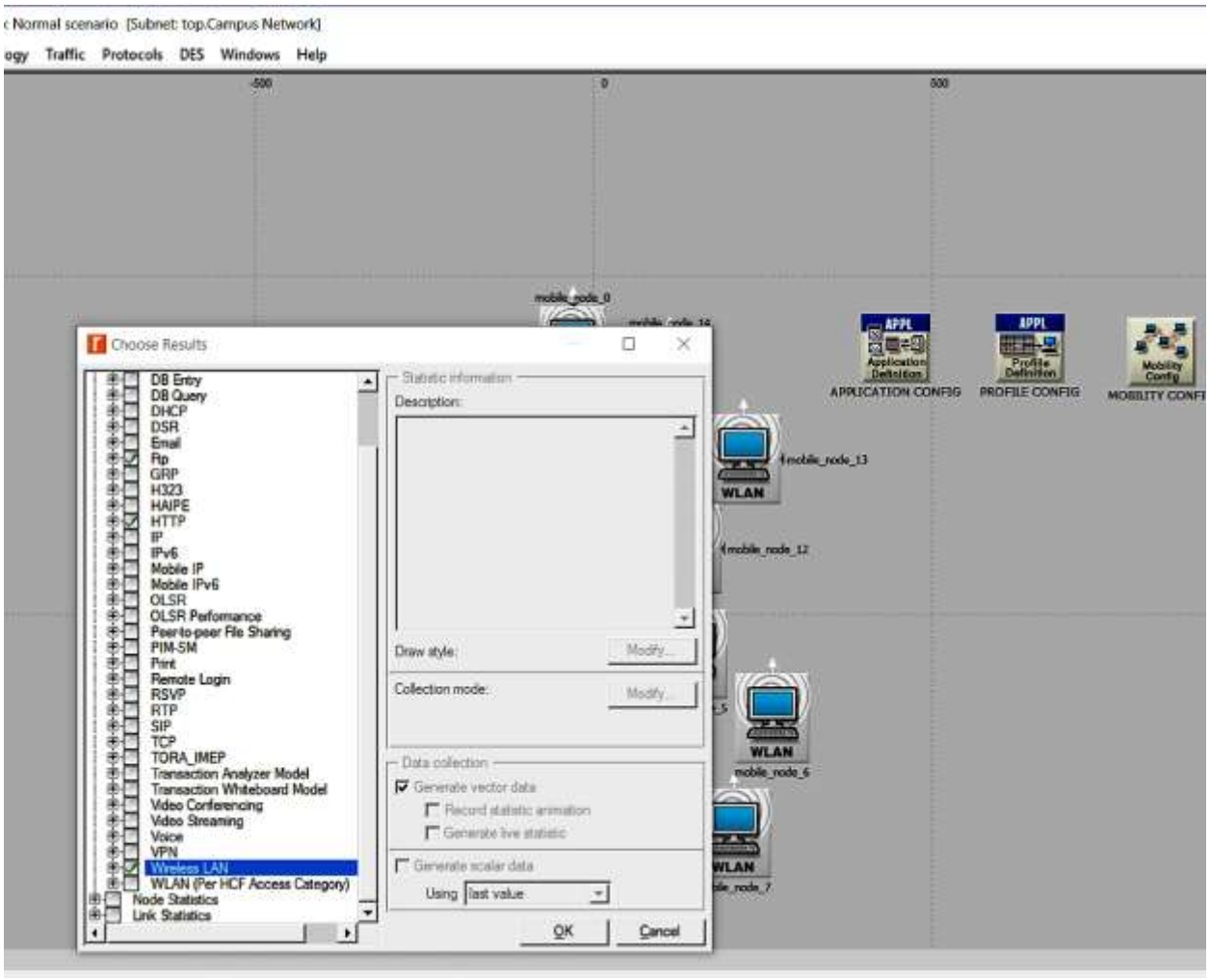

Normal scenario [Subnet: top.Campus Network]
ogy Traffic Protocols DES Windows Help
-500
0
500
Choose Results
DB Entry
DB Query
DHCP
DSR
Email
Rip
GRP
H323
HAIPE
HTTP
IP
IPv6
Mobile IP
Mobile IPv6
OLSR
OLSR Performance
Peer-to-peer File Sharing
PIM-SM
Print
Remote Login
RSVP
RTP
SIP
TCP
TORA_IMEP
Transaction Analyzer Model
Transaction Whiteboard Model
Video Conferencing
Video Streaming
Voice
VPN
Wireless LAN
WLAN (Per HCF Access Category)
Node Statistics
Link Statistics
Statistic information
Description:
Draw style:
Modify...
Collection mode:
Modify...
Data collection
Generate vector data
Record statistic animation
Generate live statistic
Generate scalar data
Using: last value
OK
Cancel
APPL
Application Definition
APPLICATION CONFIG
APPL
Profile Definition
PROFILE CONFIG
Mobility Config
MOBILITY CONFI
mobile_node_13
mobile_node_12
WLAN
mobile_node_6
WLAN

Figure 6.2:

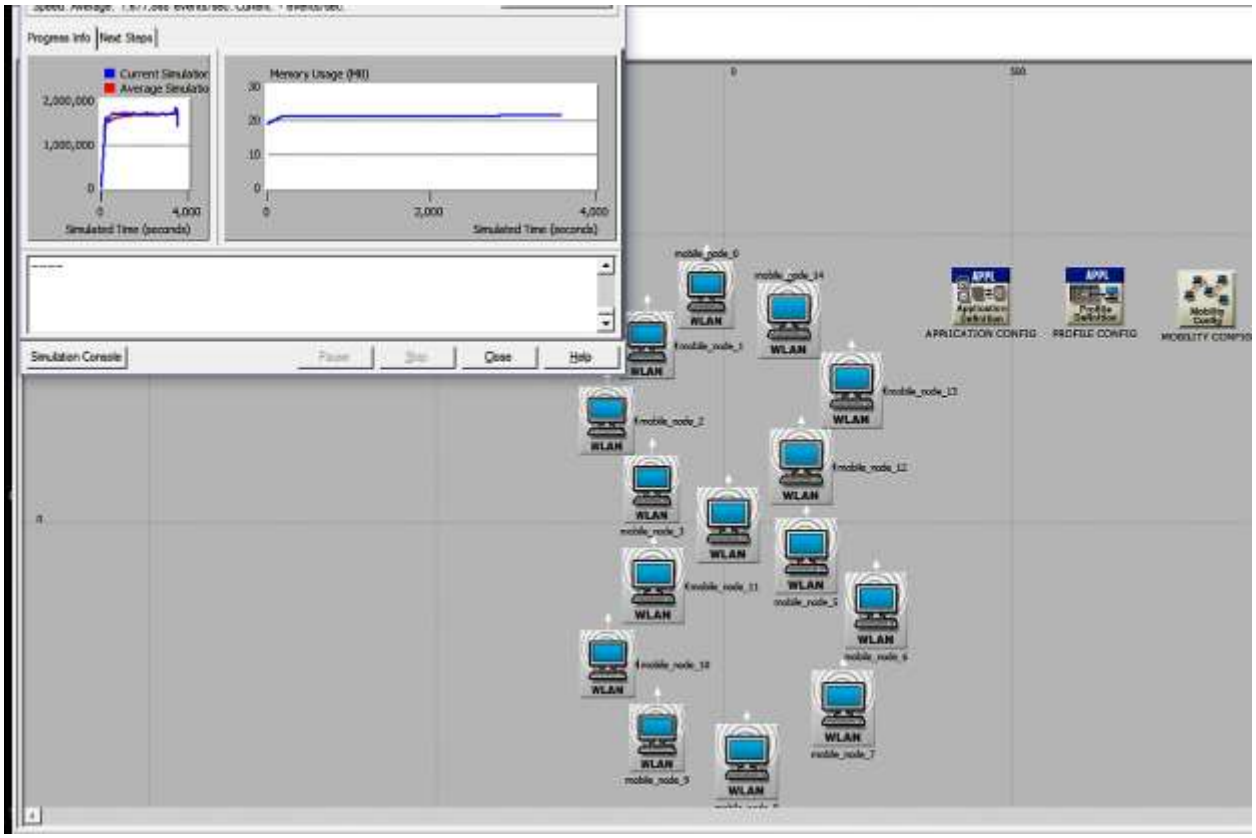

Progress Info
Next Steps
Current Simulator
Average Simulator
2,000,000
1,000,000
0
0
4,000
Simulated Time (seconds)
Memory Usage (MB)
30
20
10
0
0
2,000
4,000
Simulated Time (seconds)
Simulation Console
Pause
Stop
Close
Help
APPL
APPLICATION CONFIG
APPL
PROFILE CONFIG
MOBILITY CONFIG
WLAN

Figure 6.3

Chapter 7

Blackhole attack and changed configurations

Repeating the blackhole attack with change in some attributes and creating new scenario

1.Create the **new scenario** name **Blackhole Attack1**

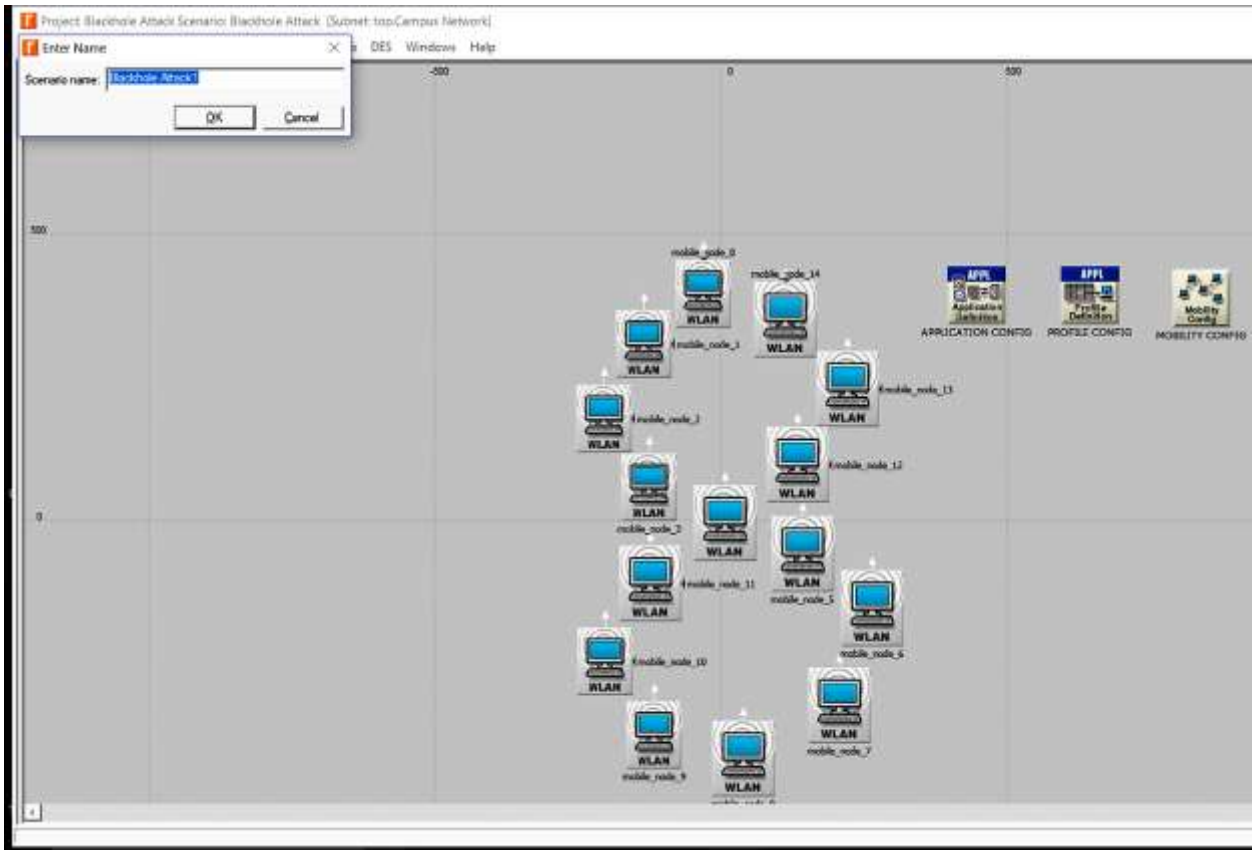


Figure 7.1

2.change the timeout buffer to 4

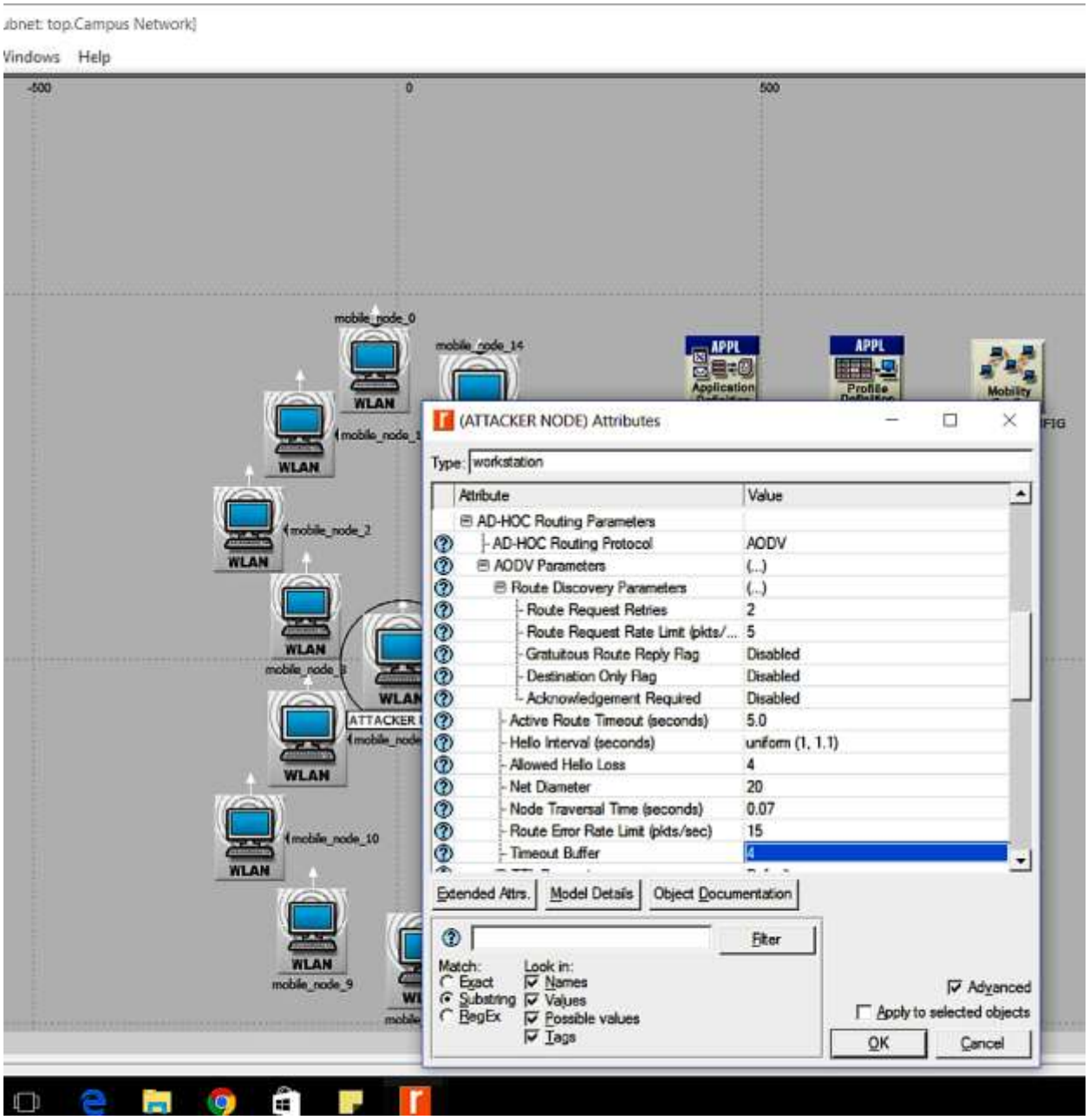


Figure 7.2

3)change long retry limit to 7

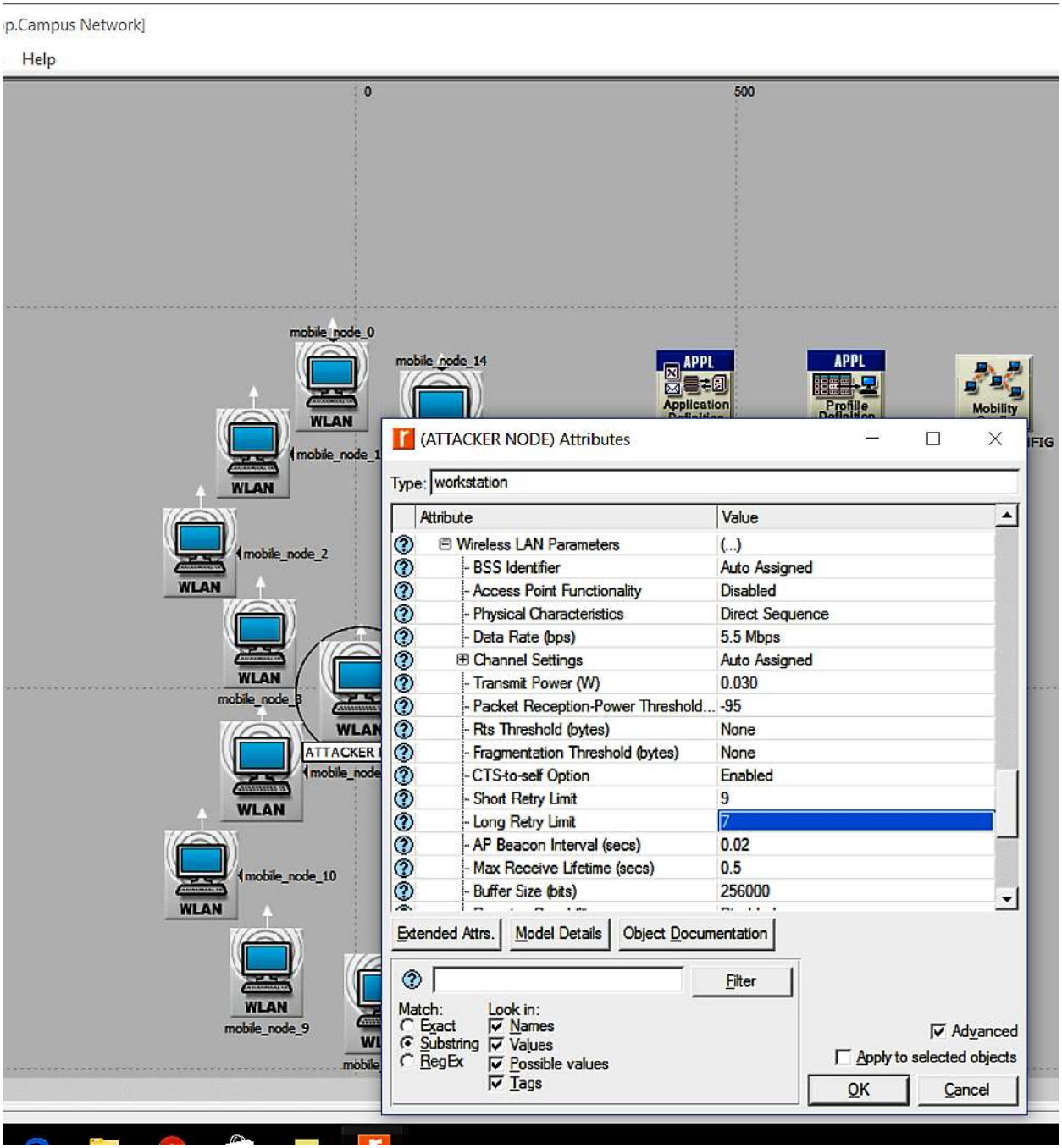


Figure 7.3

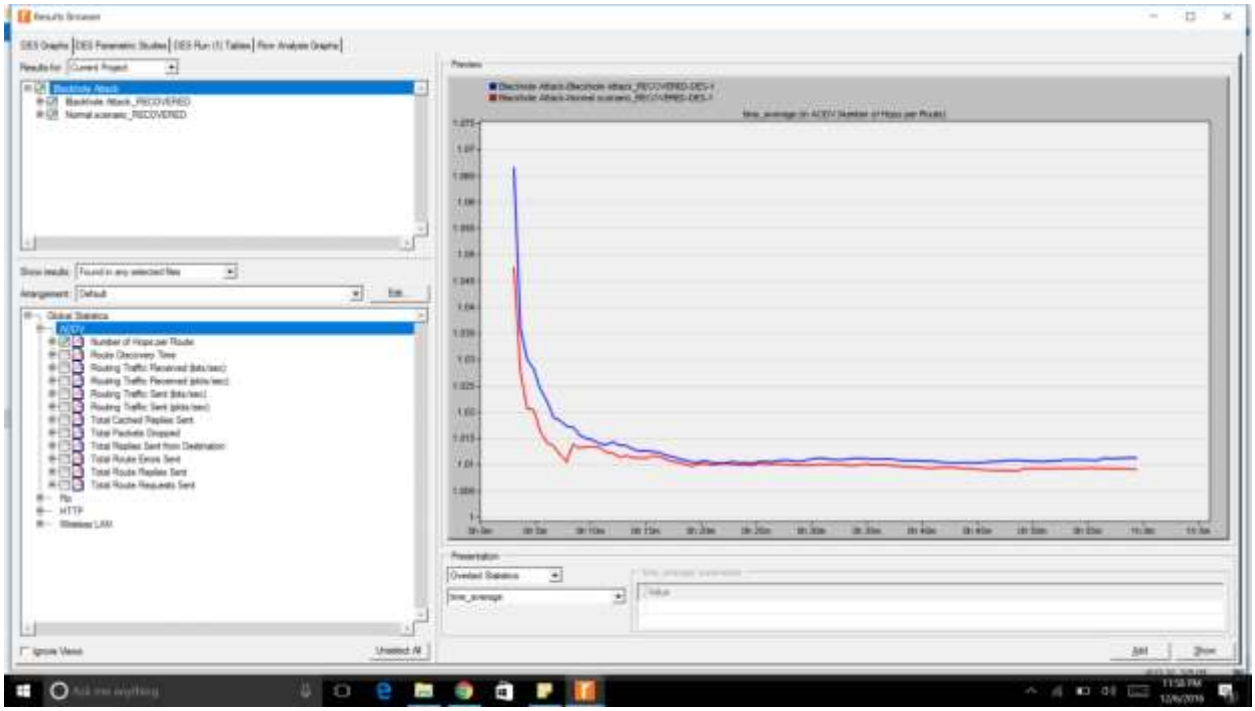
Chapter 8

Comparing the Results

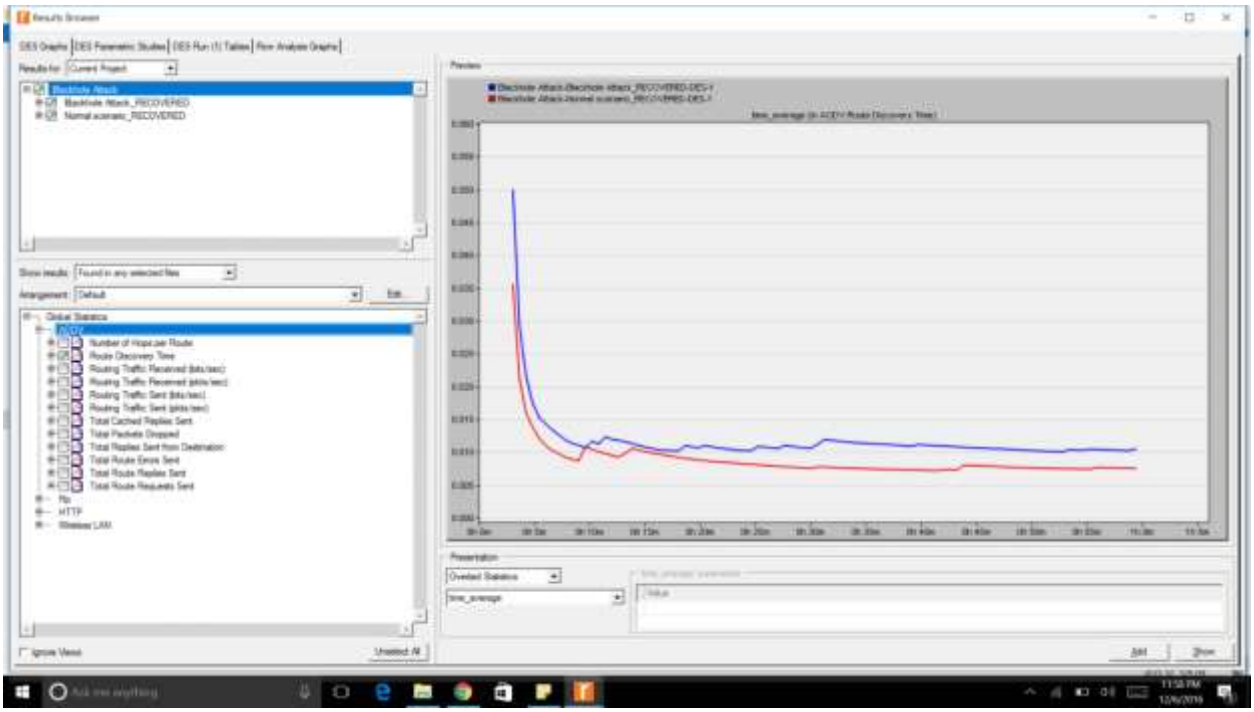
Let us now compare the results of both the scenarios **normal scenario** and **blackhole attack1**

Steps for comparison:

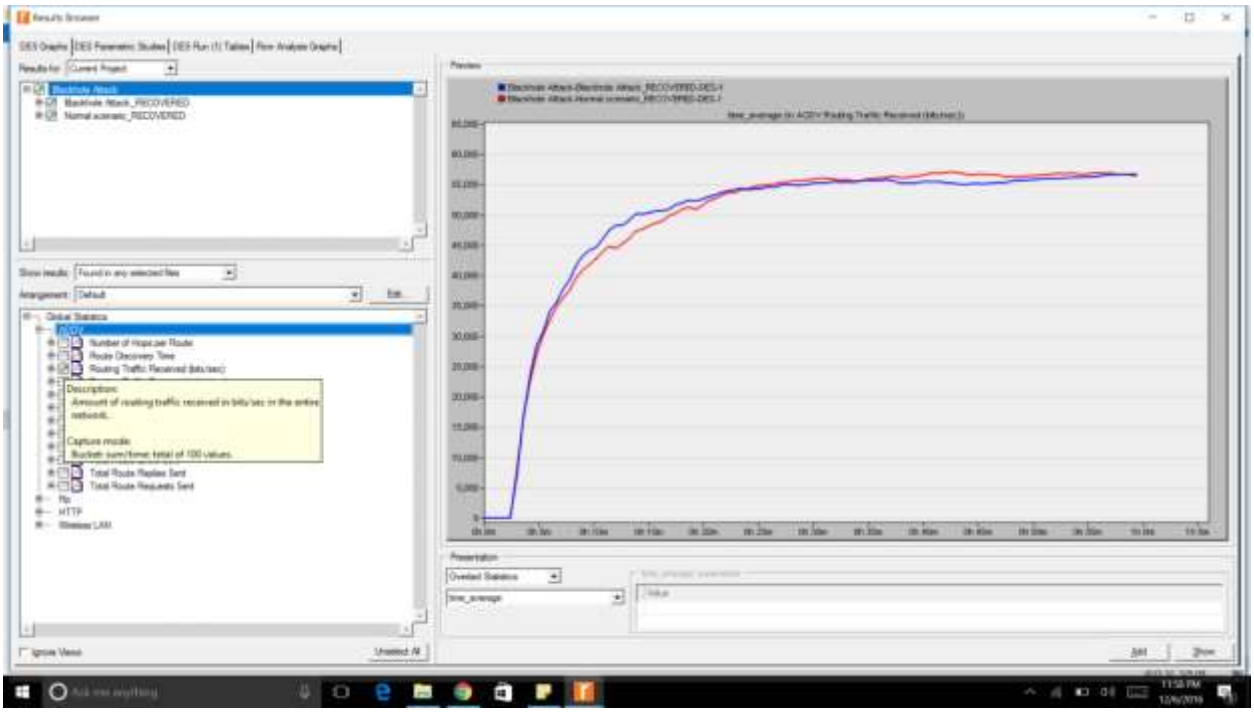
1) Open result browser -> select current project->check blackhole attack_RECOVERED and Normal scenario_RECOVERED
2) In global statistics under AODV check number of hops per route
3) In presentation select overlaid statistics. Also select time_avg. Click add
4) Select all the options in left corner one by one and generate graph of each
5)



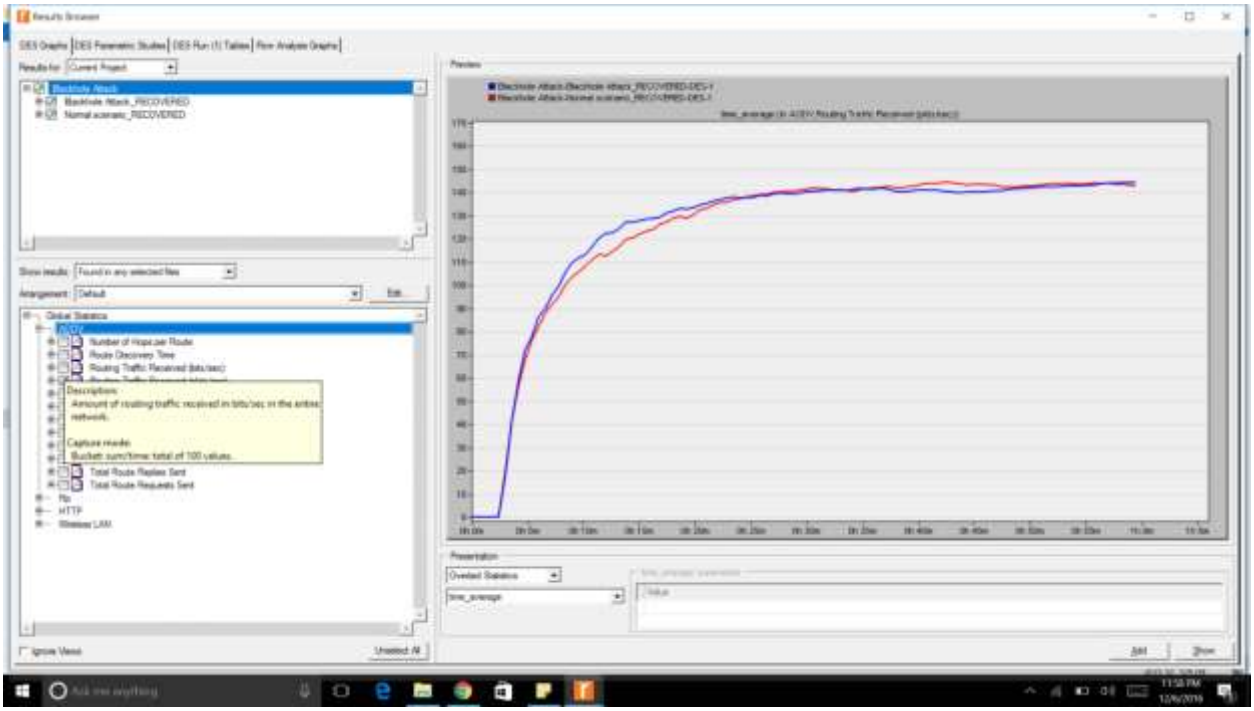
Graph 8.1:Number of Hops per route



Graph 8.2: Route Dicovery time

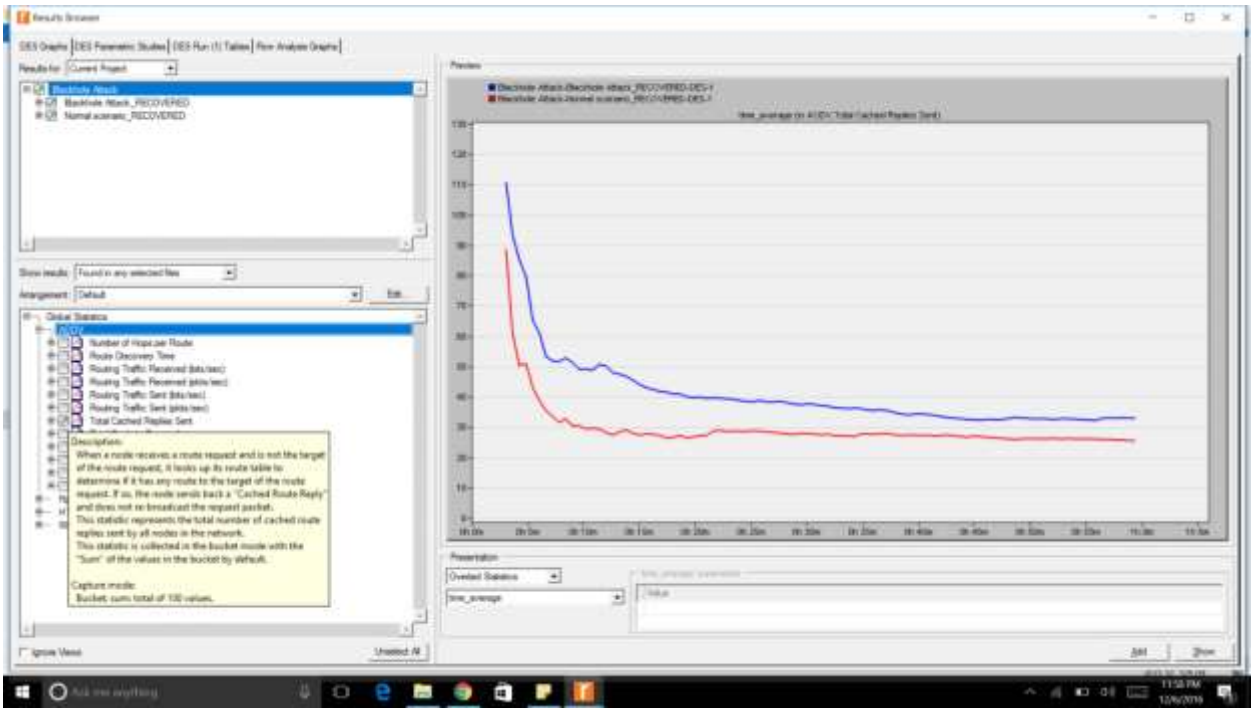


Graph 8.3: Routing traffic received(bits/sec) in entire network
Capture mode: Bucket : sum/time : total of 100 values



Graph 8.4: Routing traffic received(pkts/sec) in entire network

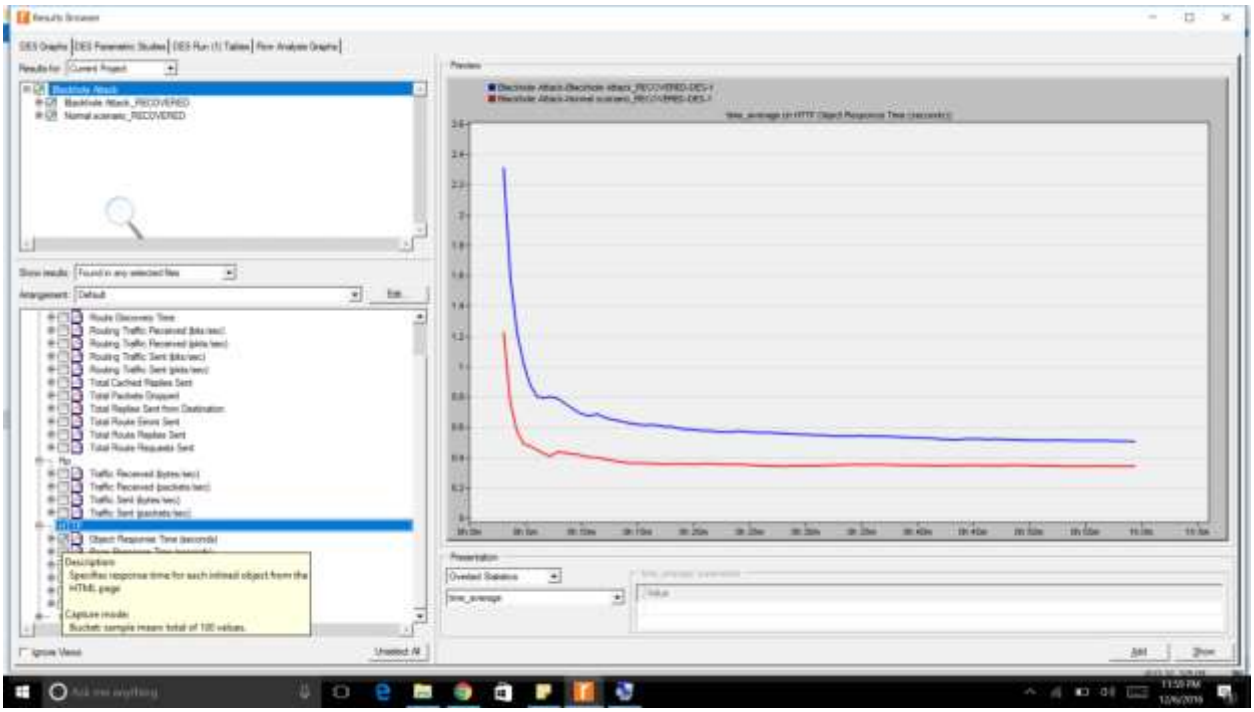
Capture mode: Bucket : sum/time : total of 100 values



Graph 8.5:Total cached replies sent

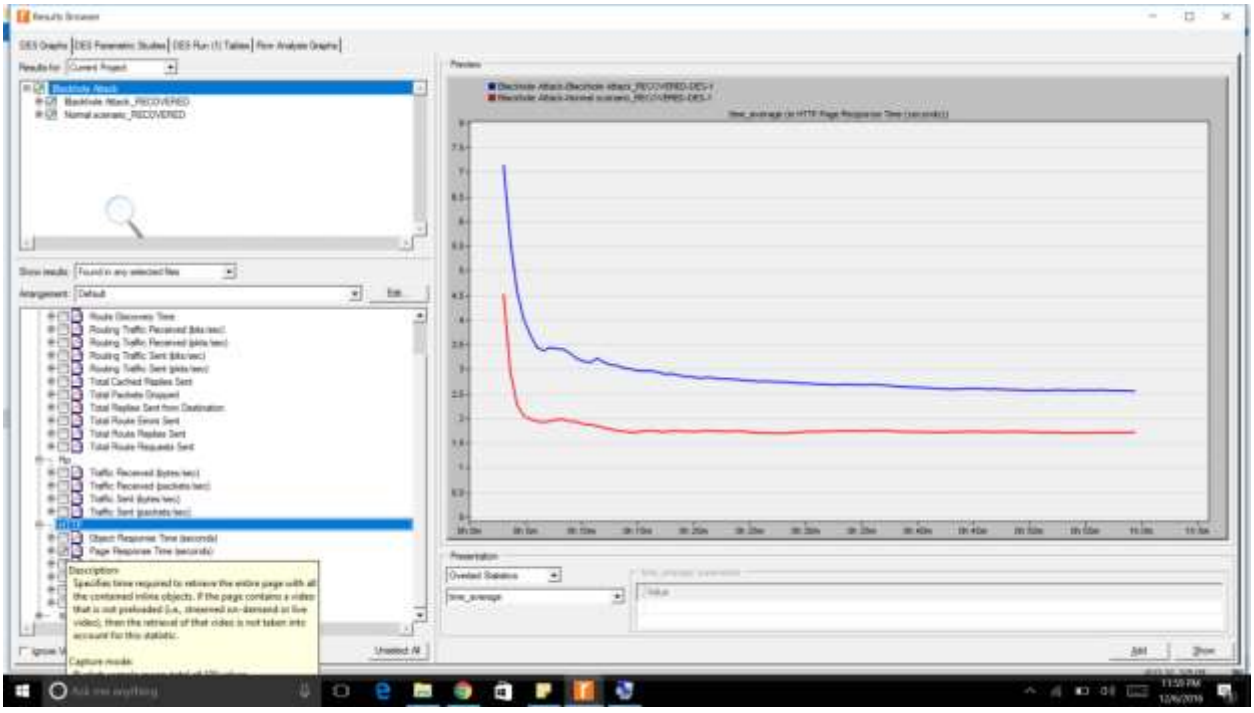
In above figure when a node receives a route request and if it is not the target of the route request it looks up its route table to determine if it has any route to the target of route request. If so the node sends back a “Catched route reply” and does not re-broadcast the request packet. This statistics represent the total number of catched route replies send by all nodes in the network.

Now go in http and select object response time(seconds)



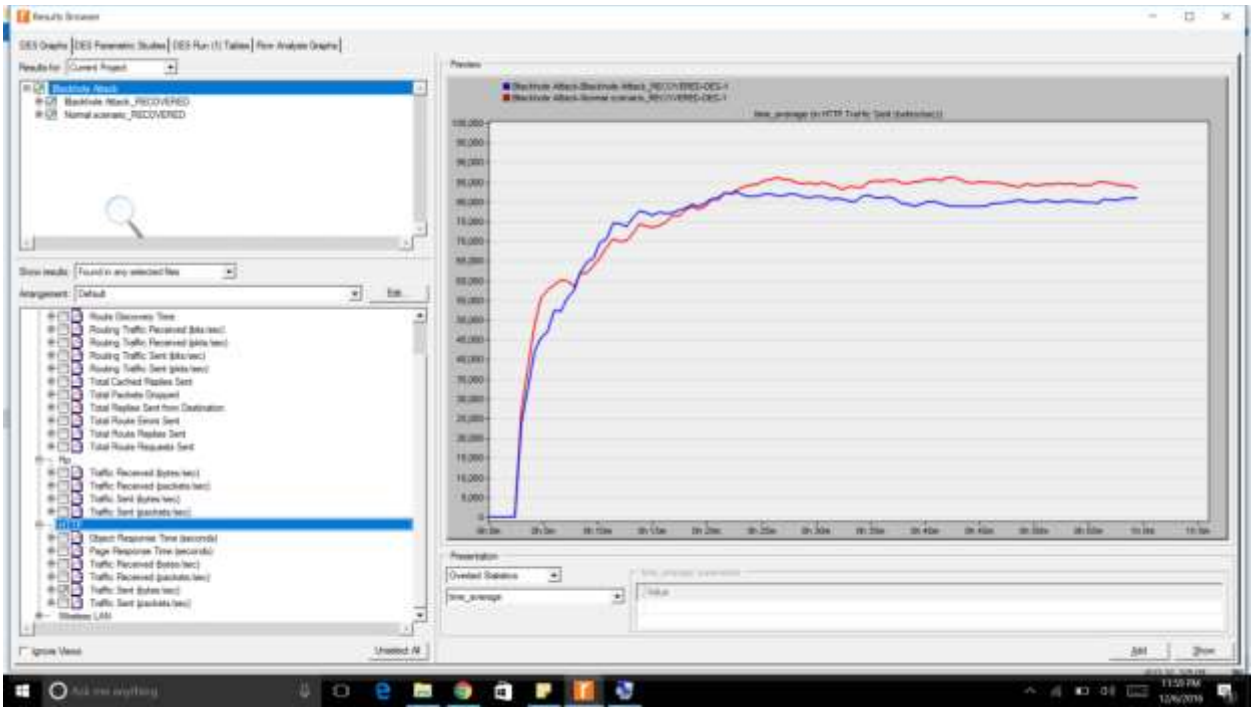
Graph 8.6:Response time(seconds)

Specifies response time for each inlined object from the HTML page

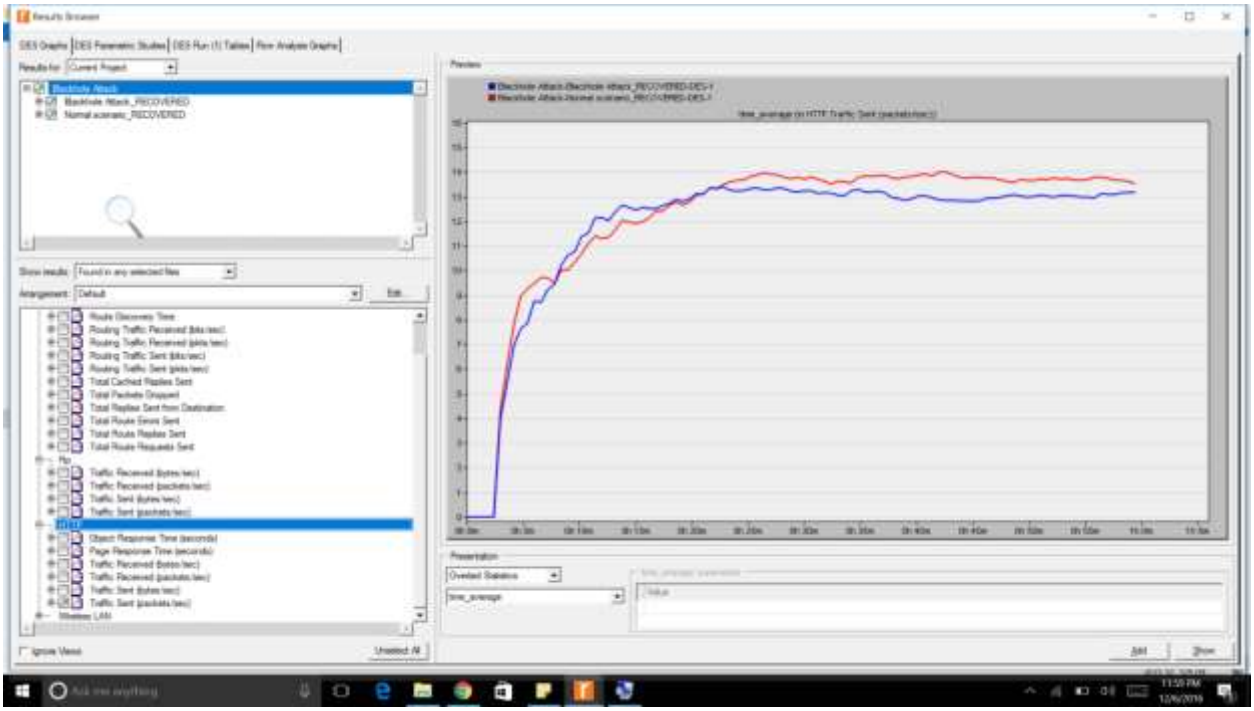


Graph 8.7: Page response time(seconds)

Specifies the time required to retrieve the entire page with all the contained inline objects. If the page contains a video that is not preloaded then the retrieval of that video is not taken into account.

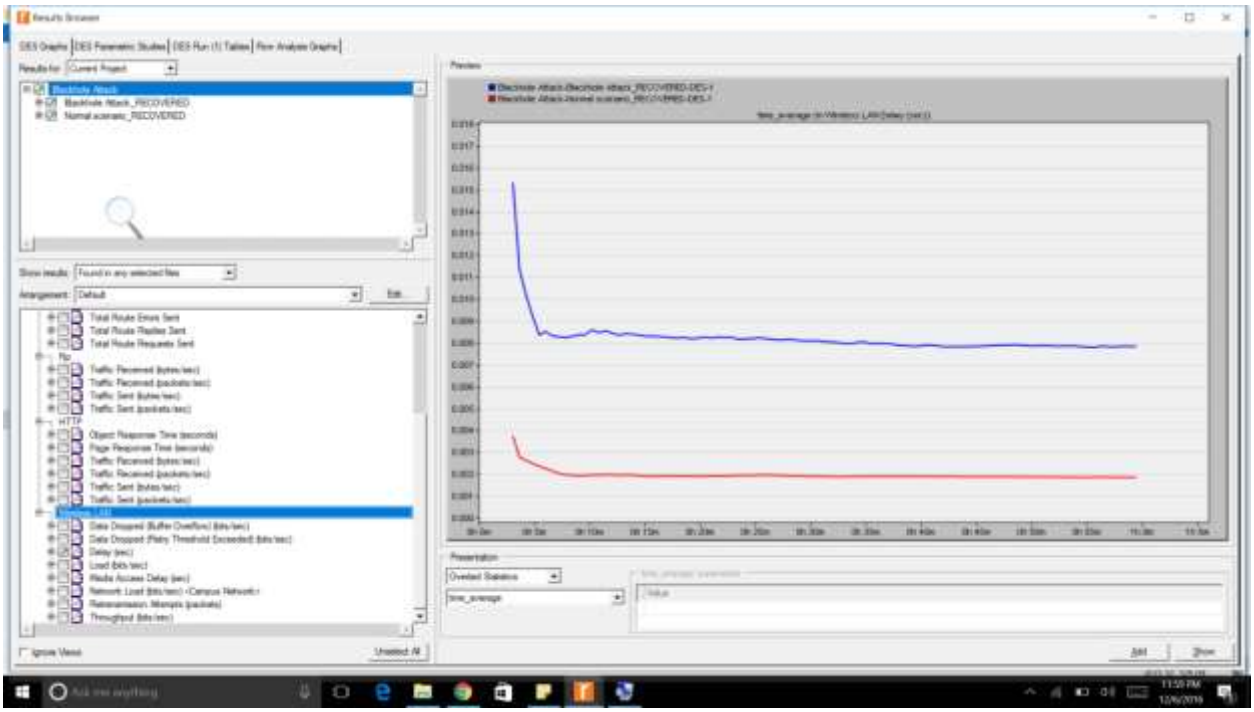


Graph 8.8:Traffic sent (bytes/sec)

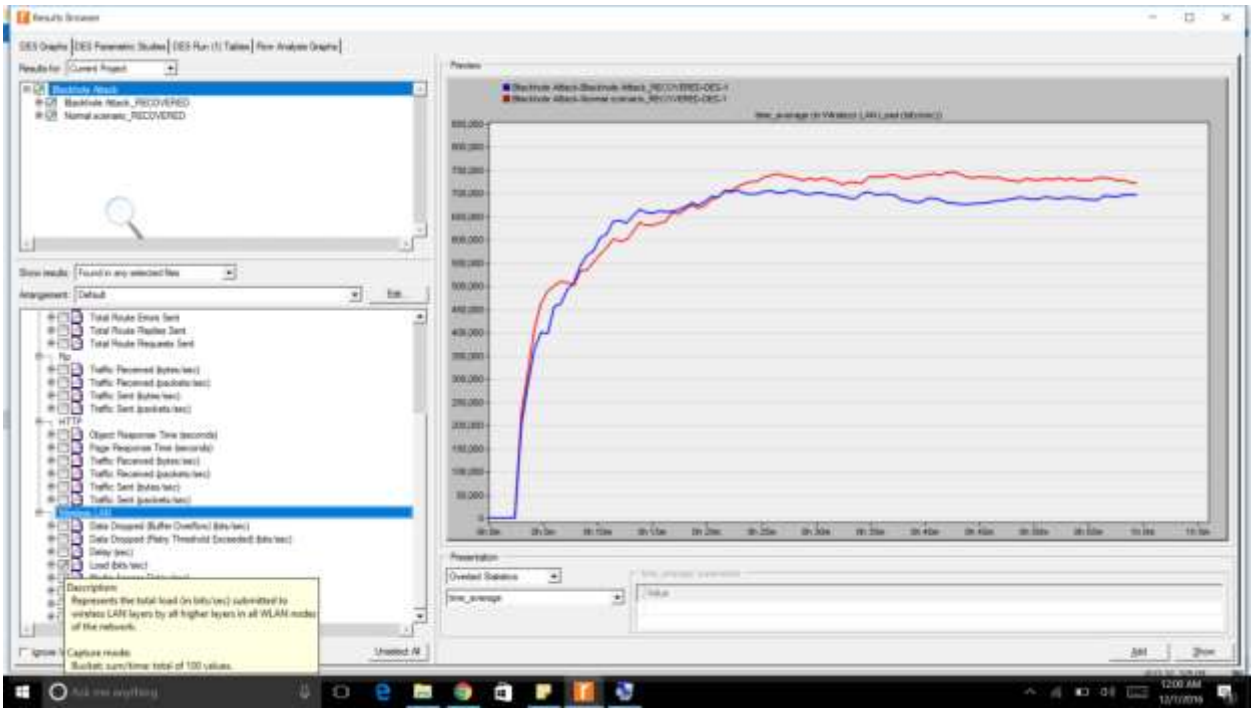


Graph 8.9: Traffic sent(pkts/sec)

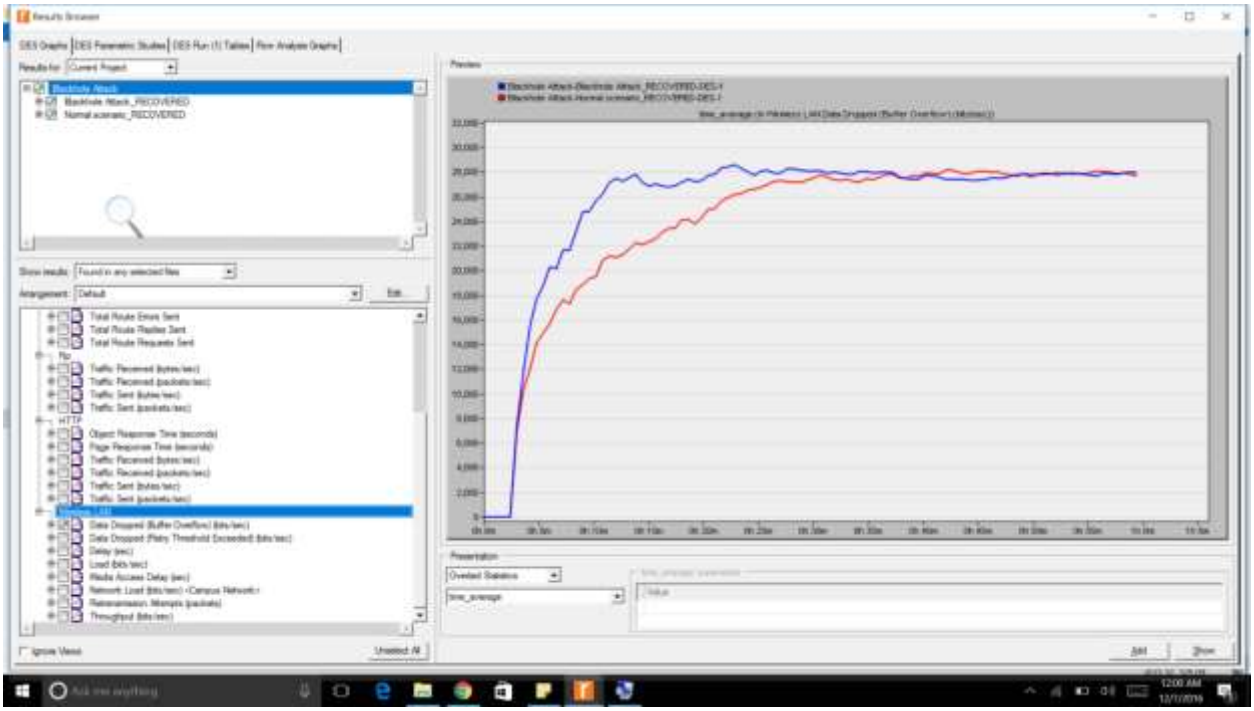
Graphs of Wireless LAN :



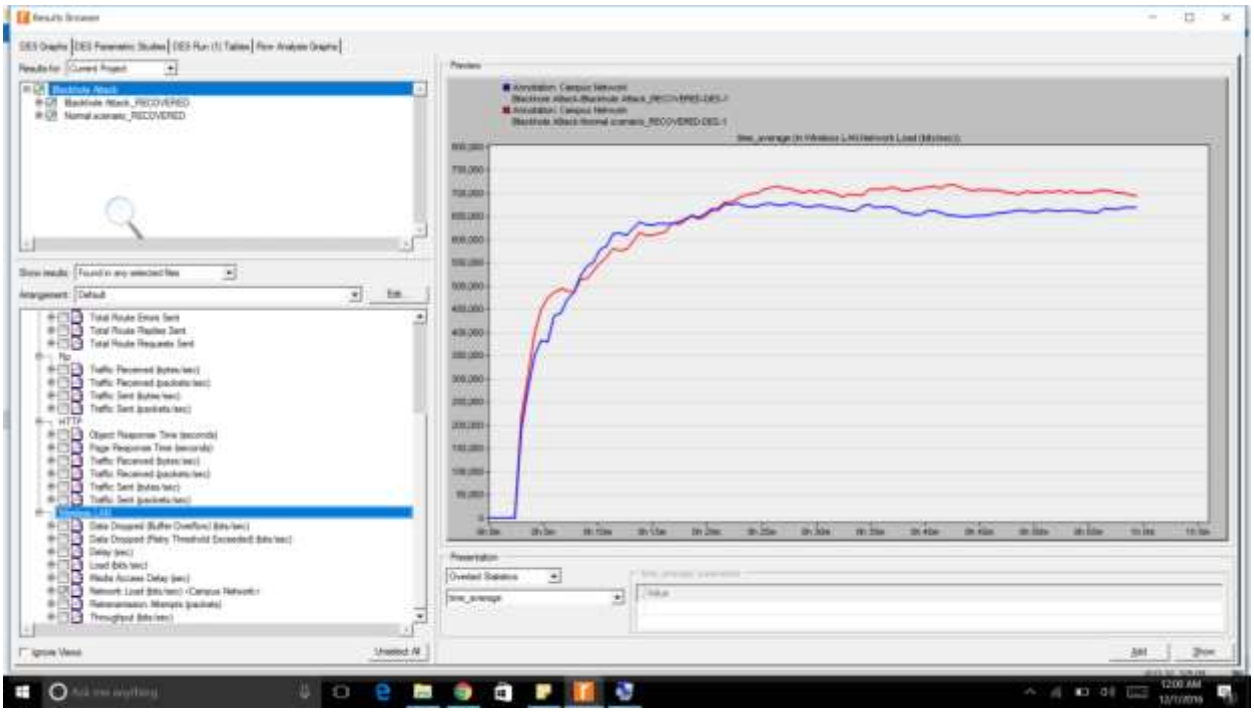
Graph 8.10: Delay(sec)



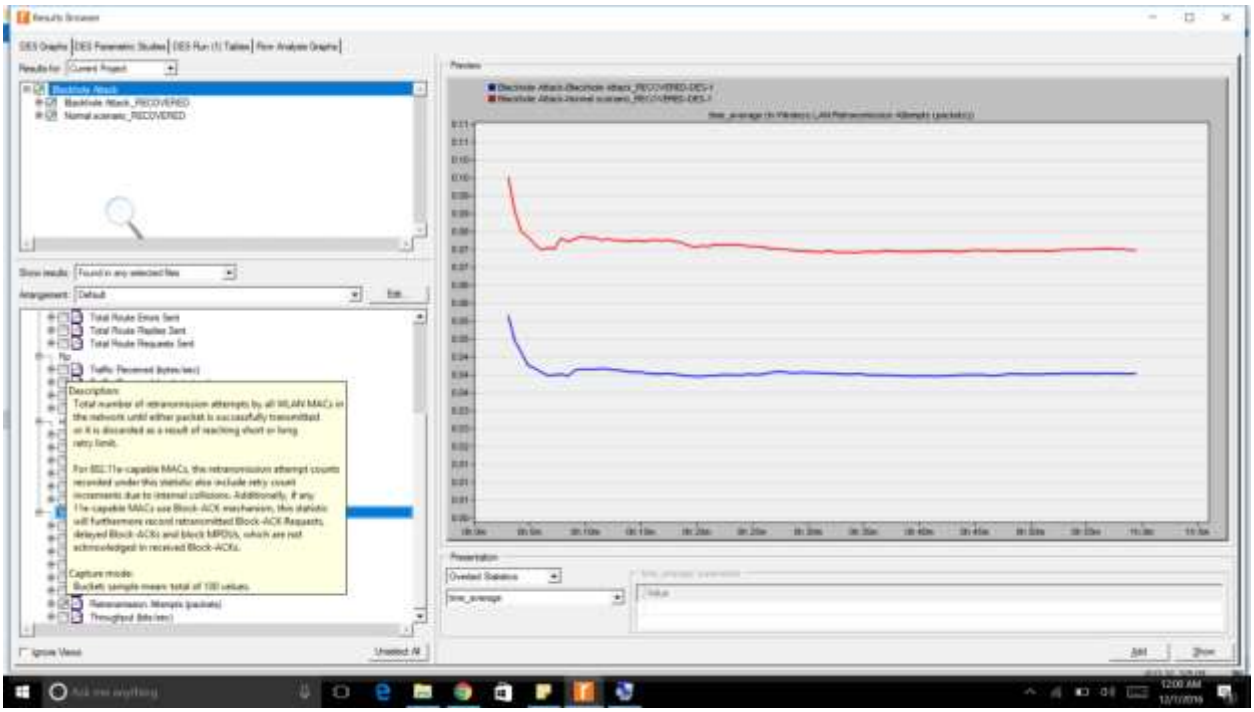
Graph 8.11: Load(bits/sec)



Graph 8.12: Data dropped(Buffer overflow)(bits/sec)

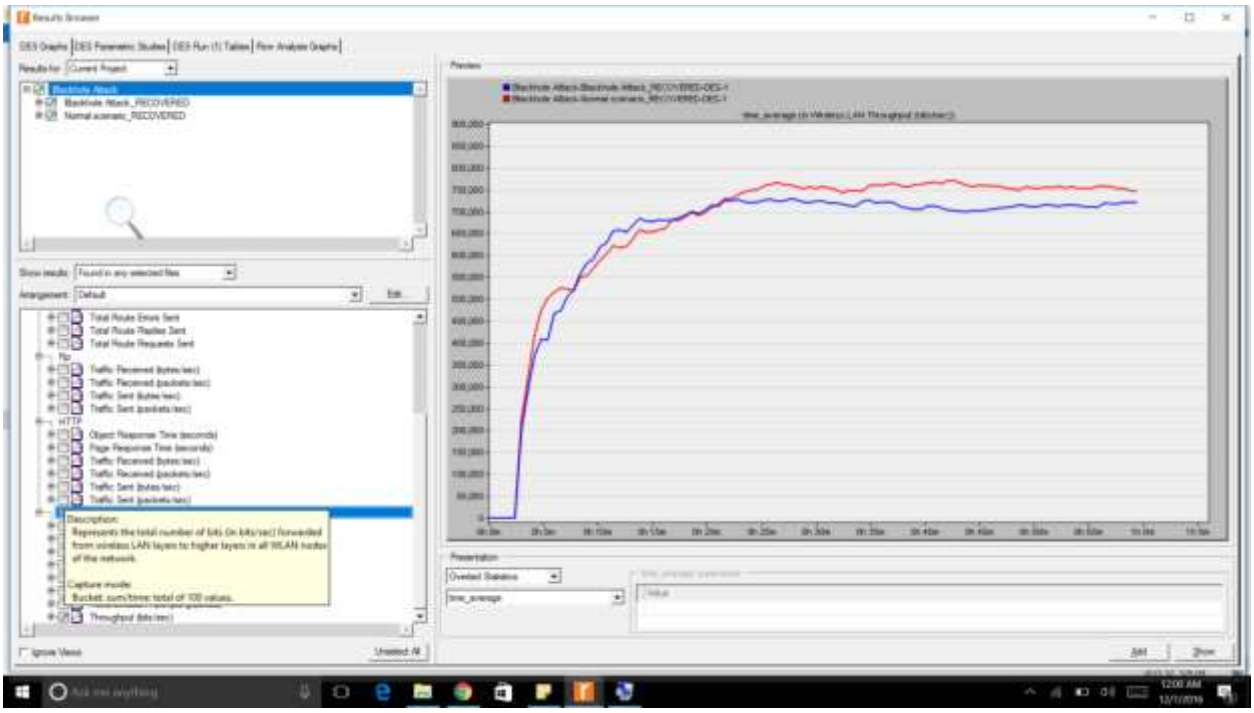


Graph 8.13: Network load (bits/sec)<Campus network>



Graph 8.14: Retransmission attempts(packets)

Total number of retransmission attempts by all WLAN MACs in the network until either packet is successfully transmitted or it is discarded as a result of reaching short or long retry limit.



Graph 8.15: Throughput(bits/sec)

Represents total number of bits forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network.

Chapter 9:

Prevention Scenario

Till now we have seen the blackhole attack and also the comparison between two scenarios of blackhole attack.Now let's discuss the prevention scenario of blackhole attack.

Steps for Prevention:

1)Create new scenario **Blackhole Attack Prevention**

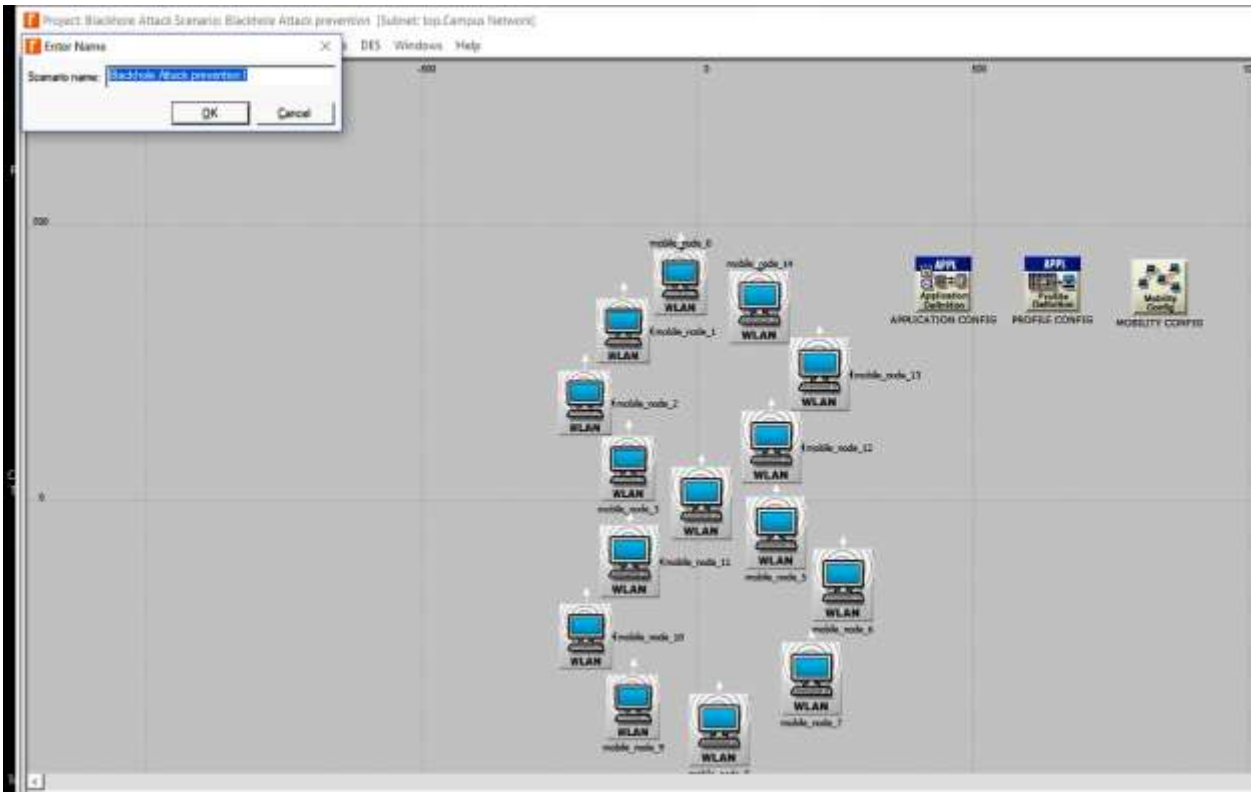


Figure 9.1

2)In attributes of nodes(workstation) under AODV parameters set active route timeout to 6 sec., Interval to uniform, Loss allowed-2, Net diameter- 43, Node traversal time (sec)-0.1, Route error rate limit(pkts/sec)-5, timeout buffer-6

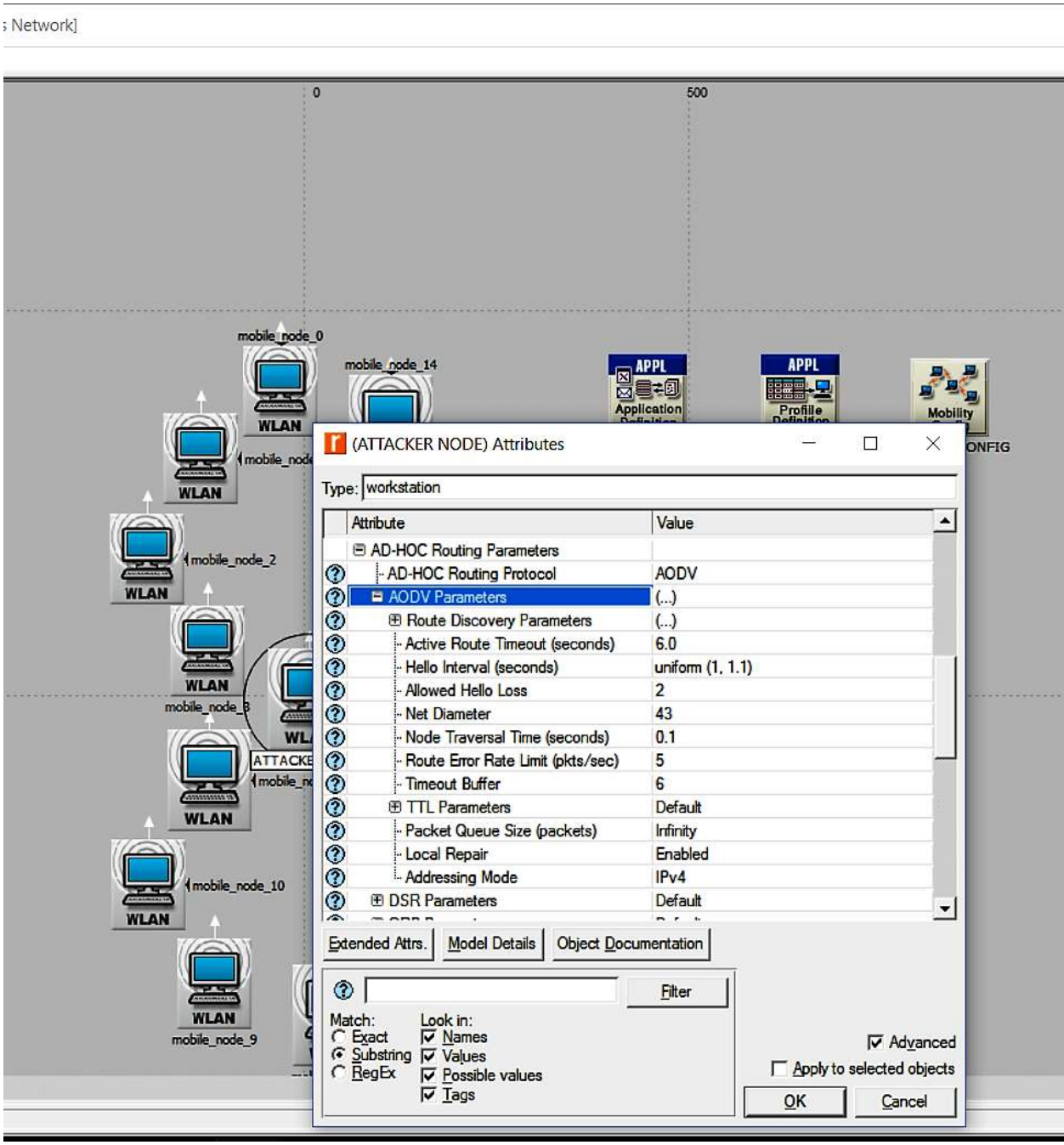

Network]
0
500
mobile_node_0
mobile_node_14
WLAN
APPL
Application
APPL
Profile
Mobility
ONFIG
mobile_node_2
mobile_node_10
mobile_node_9
ATTACKE
(ATTACKER NODE) Attributes
Type: workstation
Attribute
Value
AD-HOC Routing Parameters
AD-HOC Routing Protocol
AODV
AODV Parameters
(...)
Route Discovery Parameters
(...)
Active Route Timeout (seconds)
6.0
Hello Interval (seconds)
uniform (1, 1.1)
Allowed Hello Loss
2
Net Diameter
43
Node Traversal Time (seconds)
0.1
Route Error Rate Limit (pkts/sec)
5
Timeout Buffer
6
TTL Parameters
Default
Packet Queue Size (packets)
Infinity
Local Repair
Enabled
Addressing Mode
IPv4
DSR Parameters
Default
Extended Attrs.
Model Details
Object Documentation
Filter
Match:
Exact
Substring
RegEx
Look in:
Names
Values
Possible values
Tags
Advanced
Apply to selected objects
OK
Cancel

Figure 9.2

3.In nodes attributes under wireless LAN parameters set the physical characteristics as direct sequence and data rate to 2Mbps

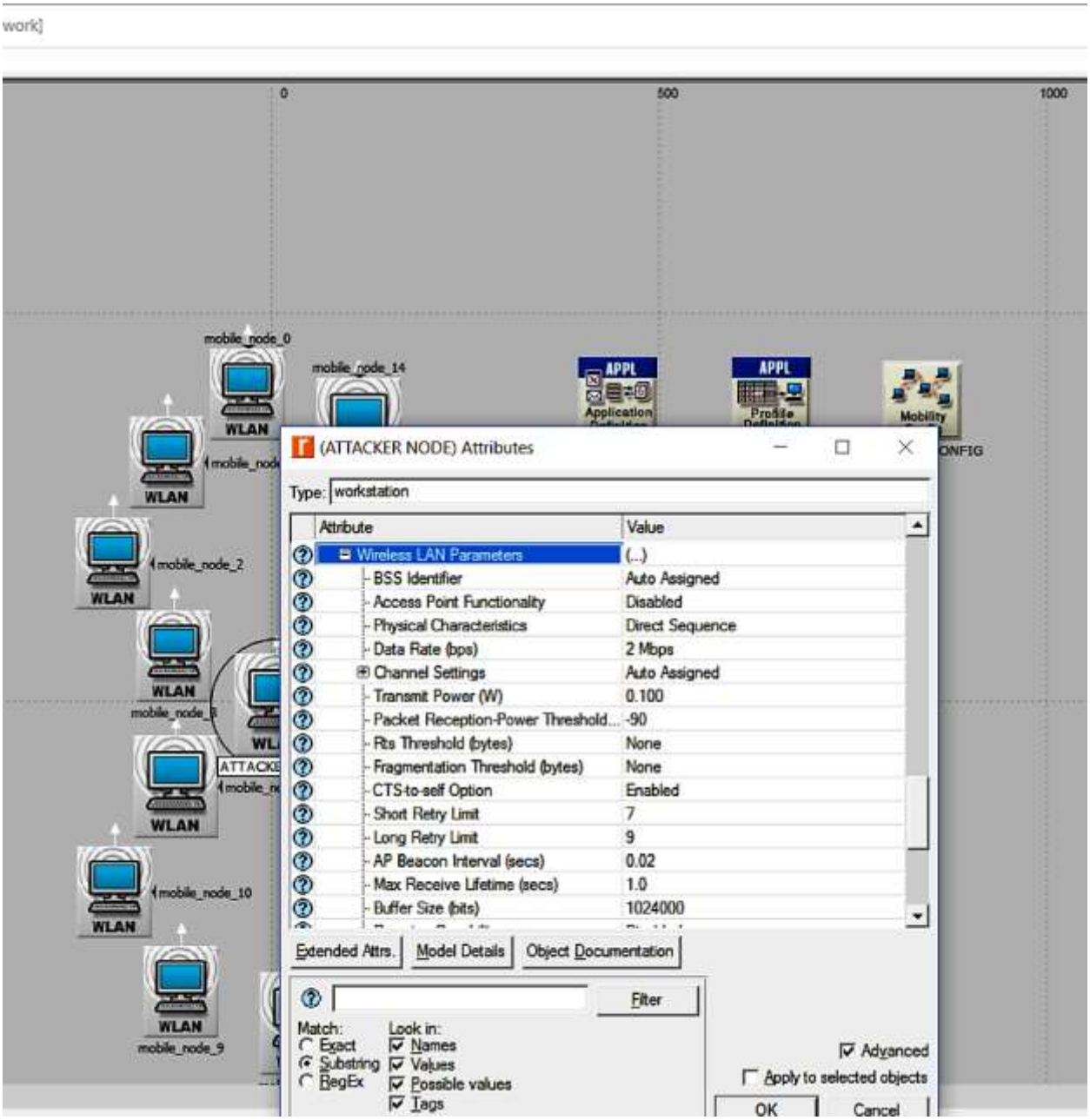


Figure 9.3

Chapter 10

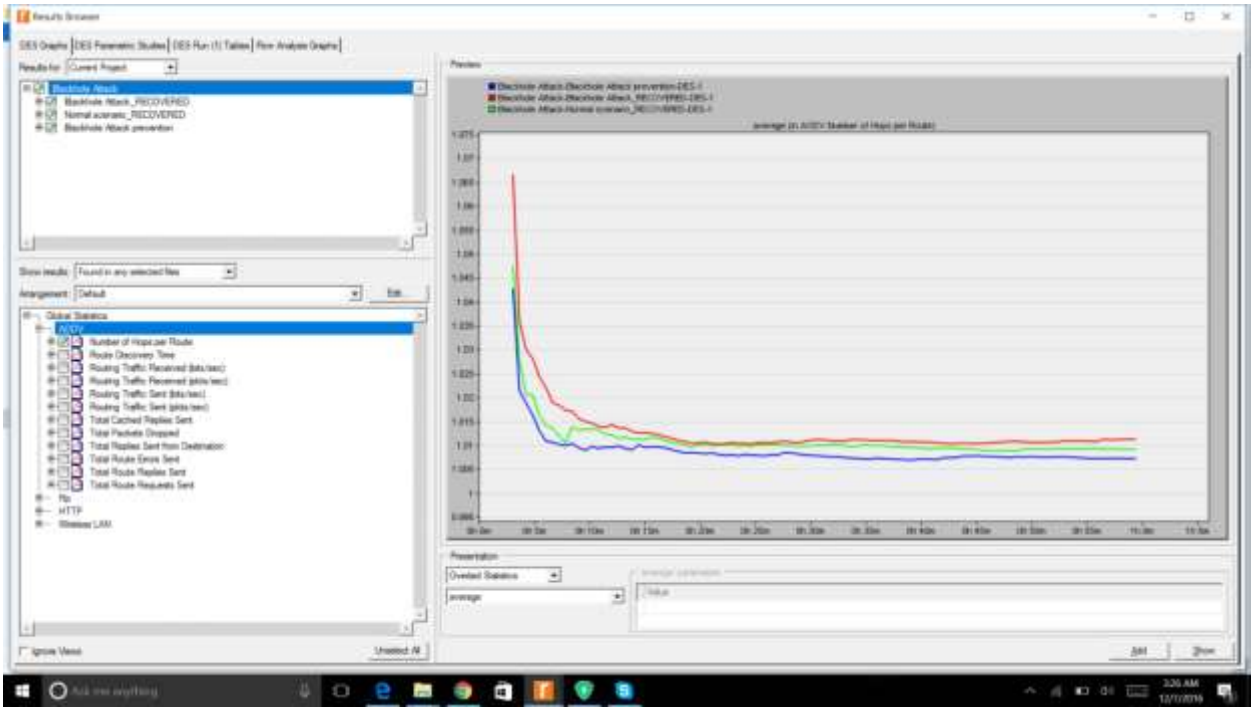
Comparing Scenarios

After creating the above prevention scenario let's do simulation to verify that Blackhole attack is successfully prevented

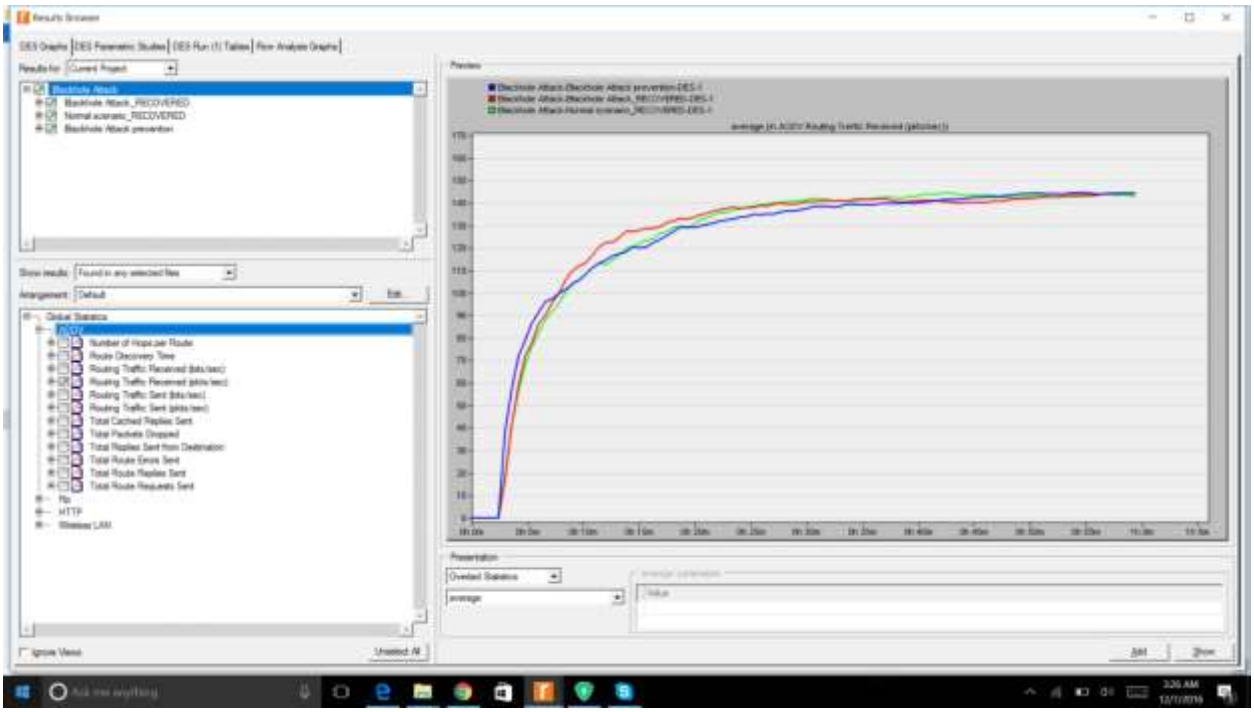
Steps for verification:

1. Go to results browser -> **DES graph**-> select current project->click on global statistics

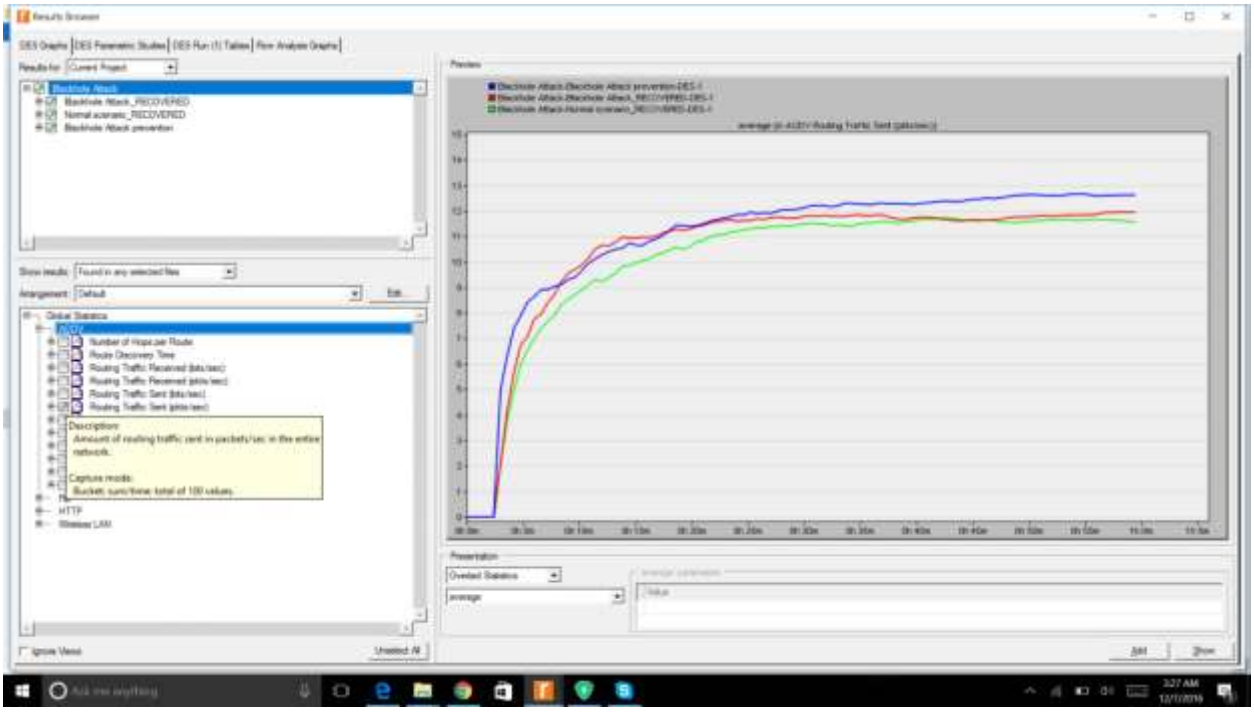
AODV protocol graphs:



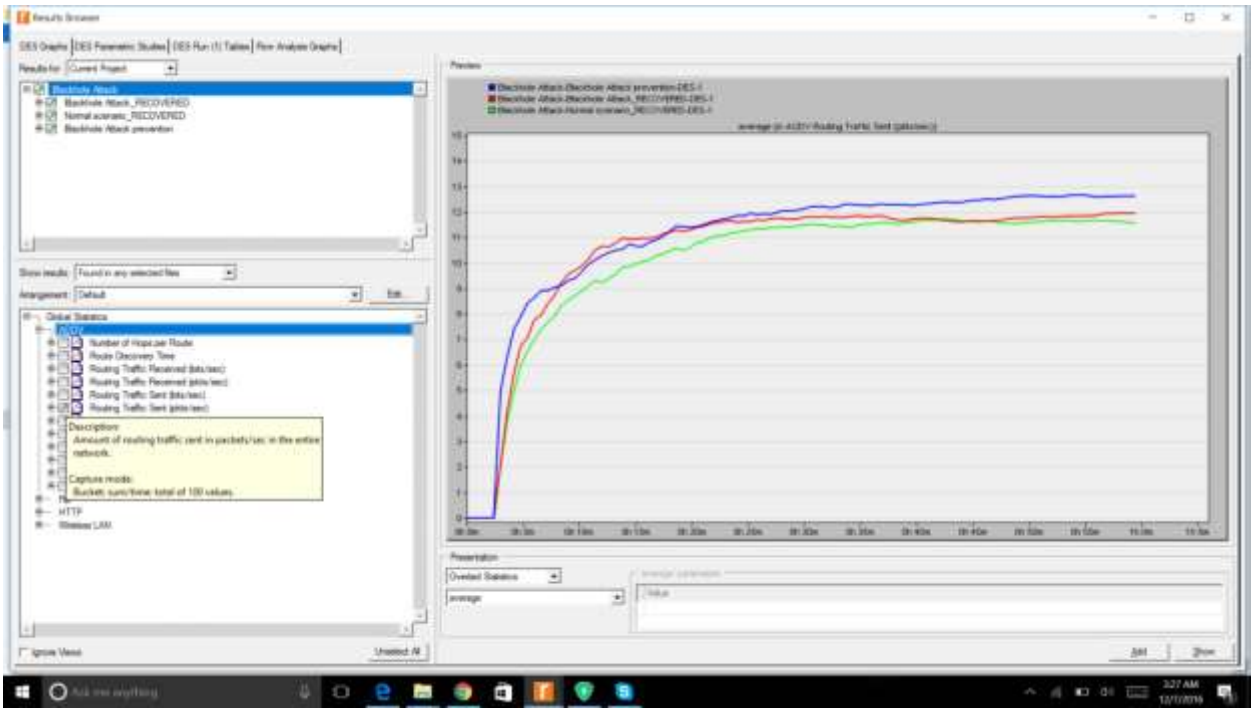
Graph 10.1: Number of Hops per route



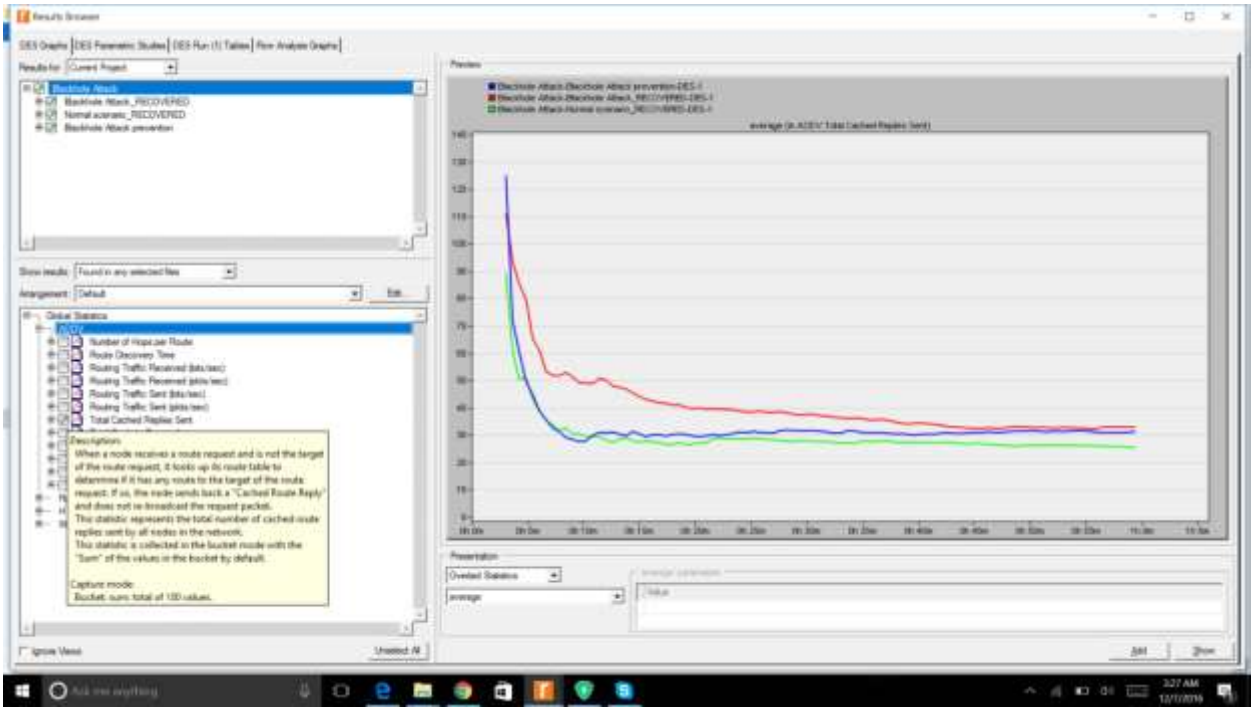
Graph 10.2:Routing traffic received (bits/sec)



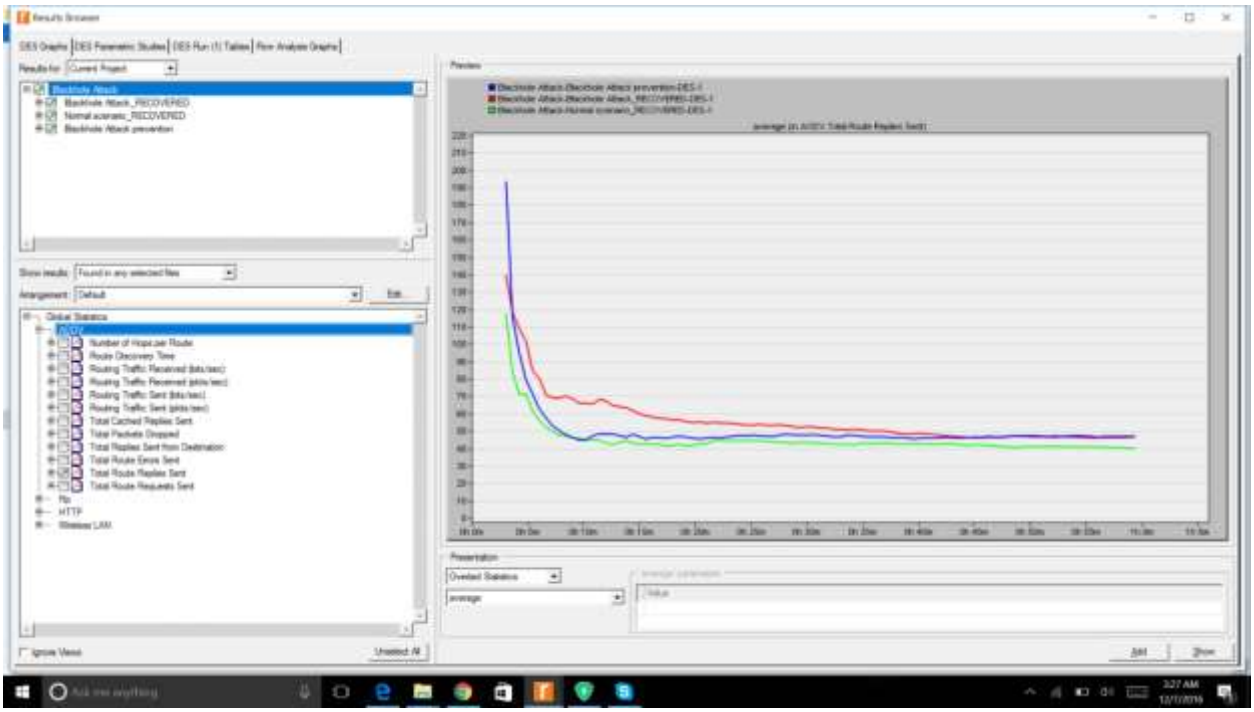
Graph 10.3: Routing traffic sent(pkts/sec)



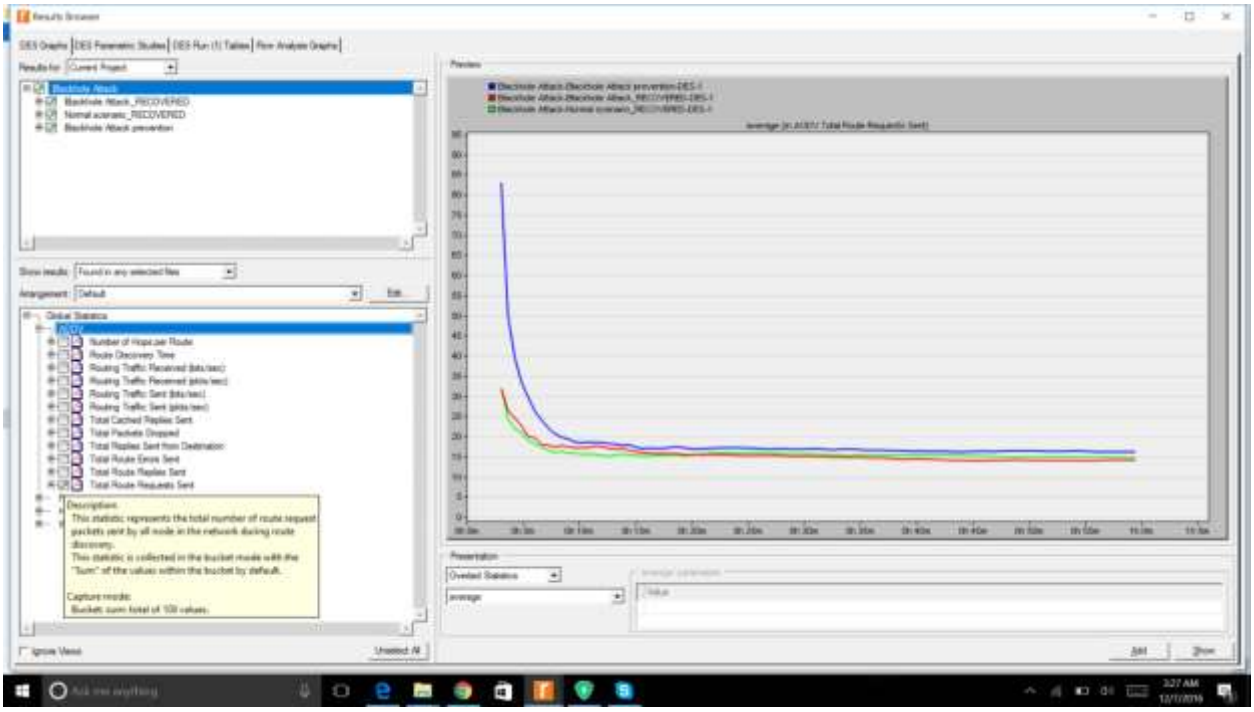
Graph 10.4:Routing traffic sent(pkts/sec)



Graph 10.5:Total catched replies sent

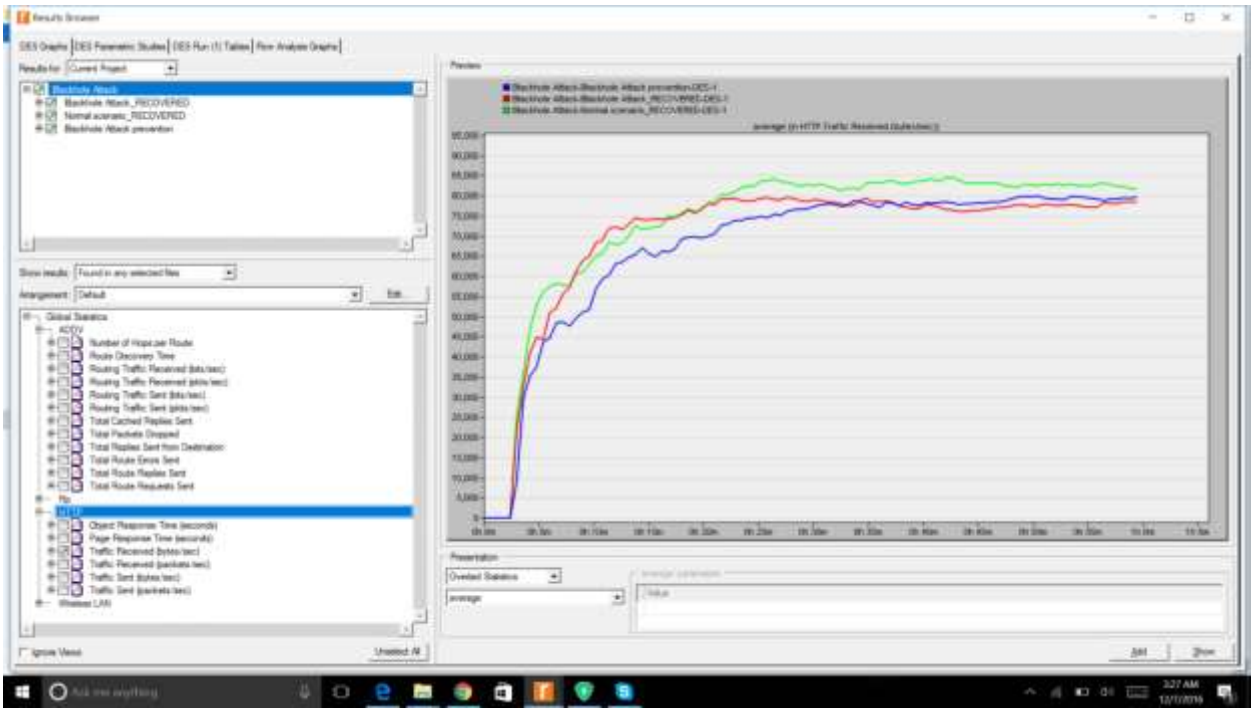


Graph 10.6: Total route replies sent

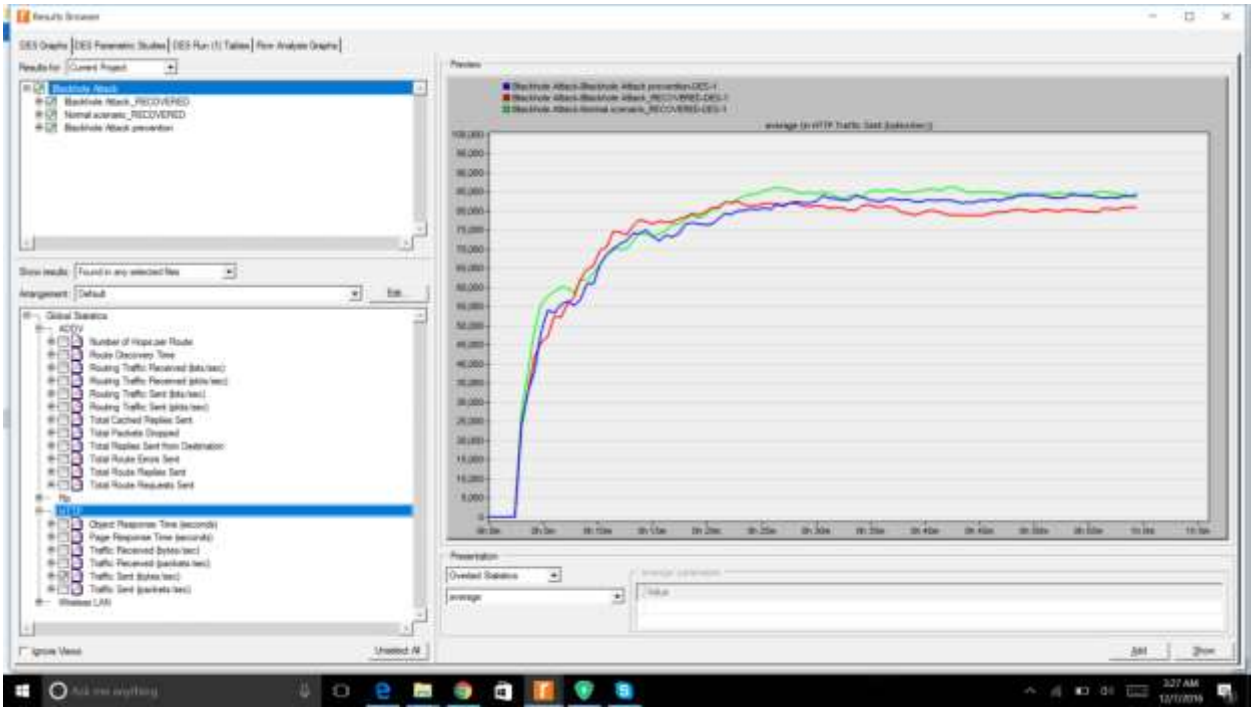


Graph 10.7:Total route requests sent

Http protocol :

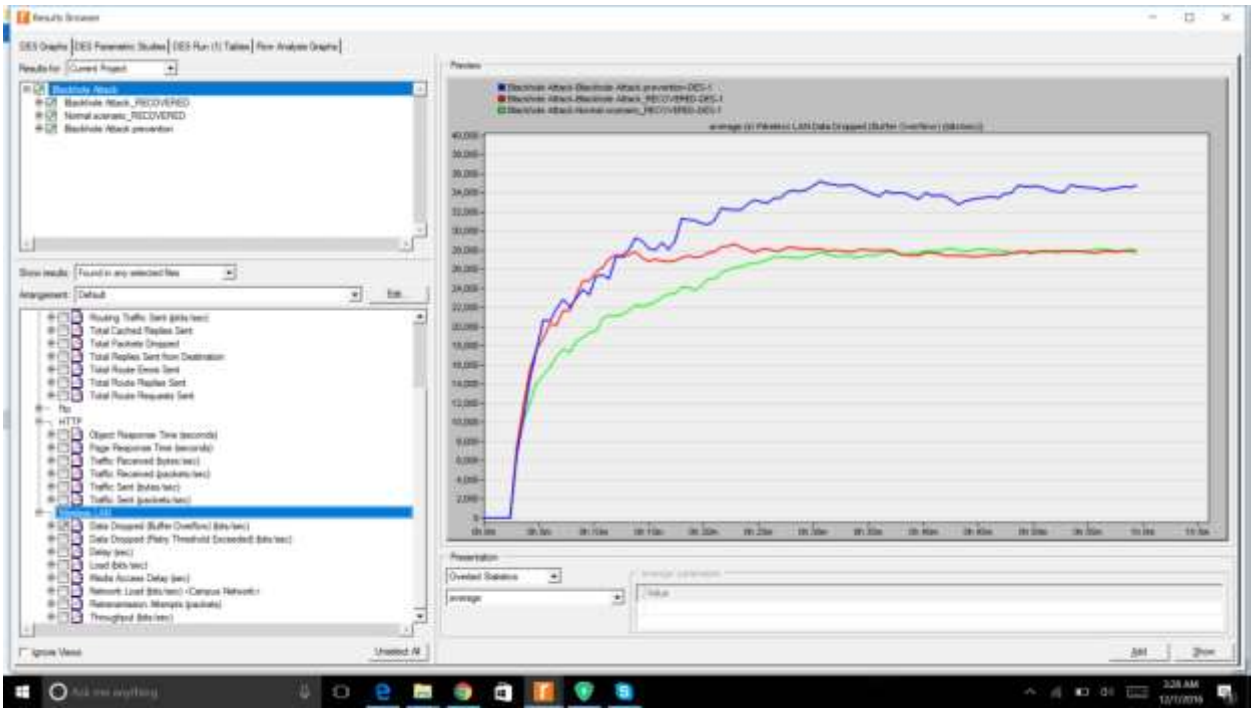


Graph 10.8: Traffic received(bytes/sec)

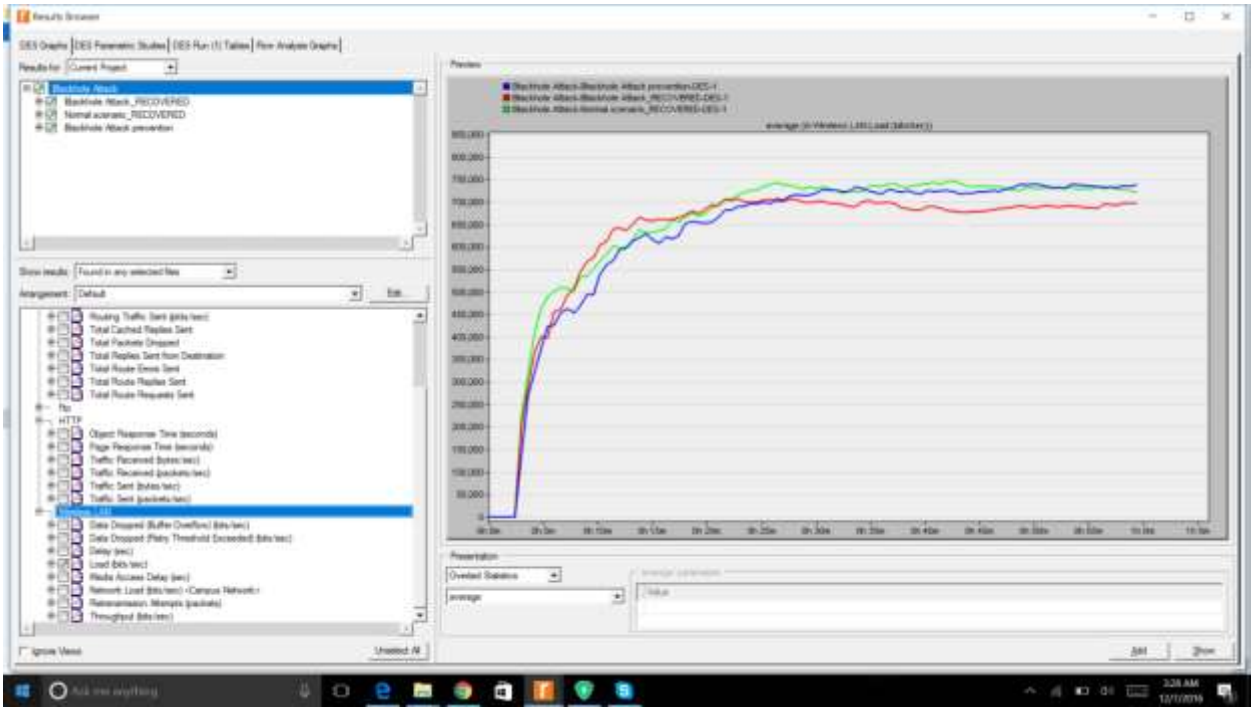


Graph 10.9:Traffic sent (bytes/sec)

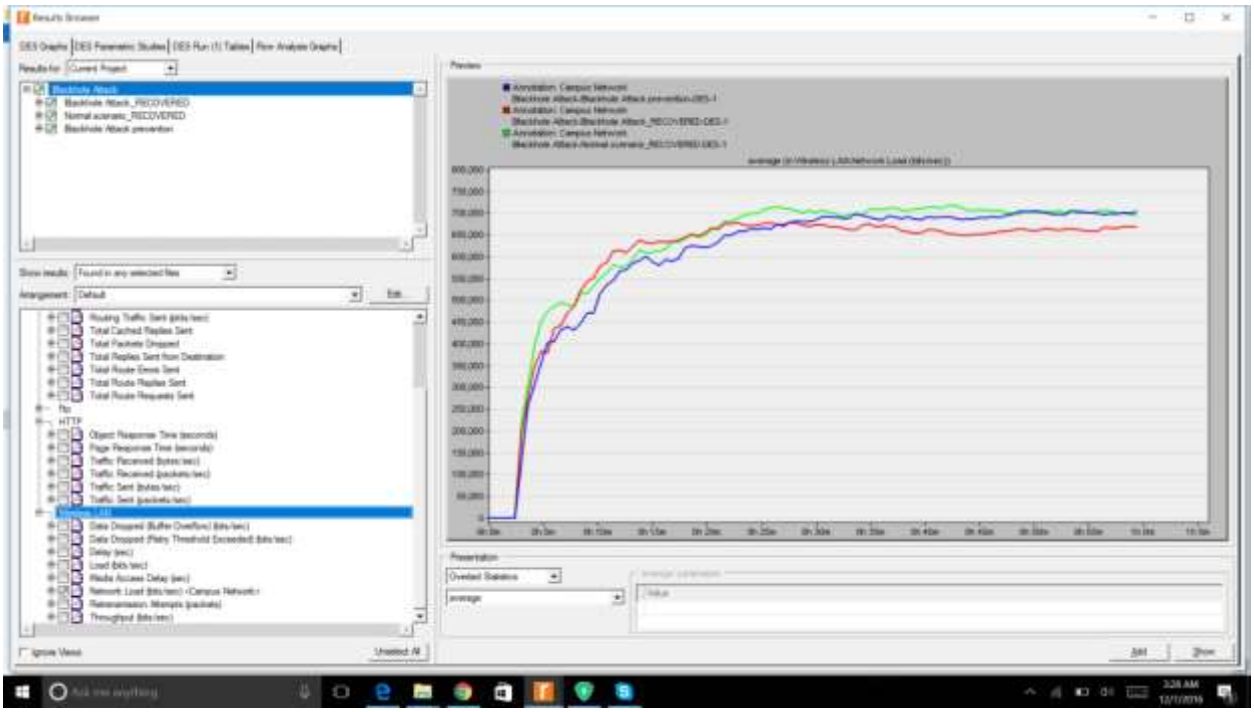
Wirless LAN protocol:



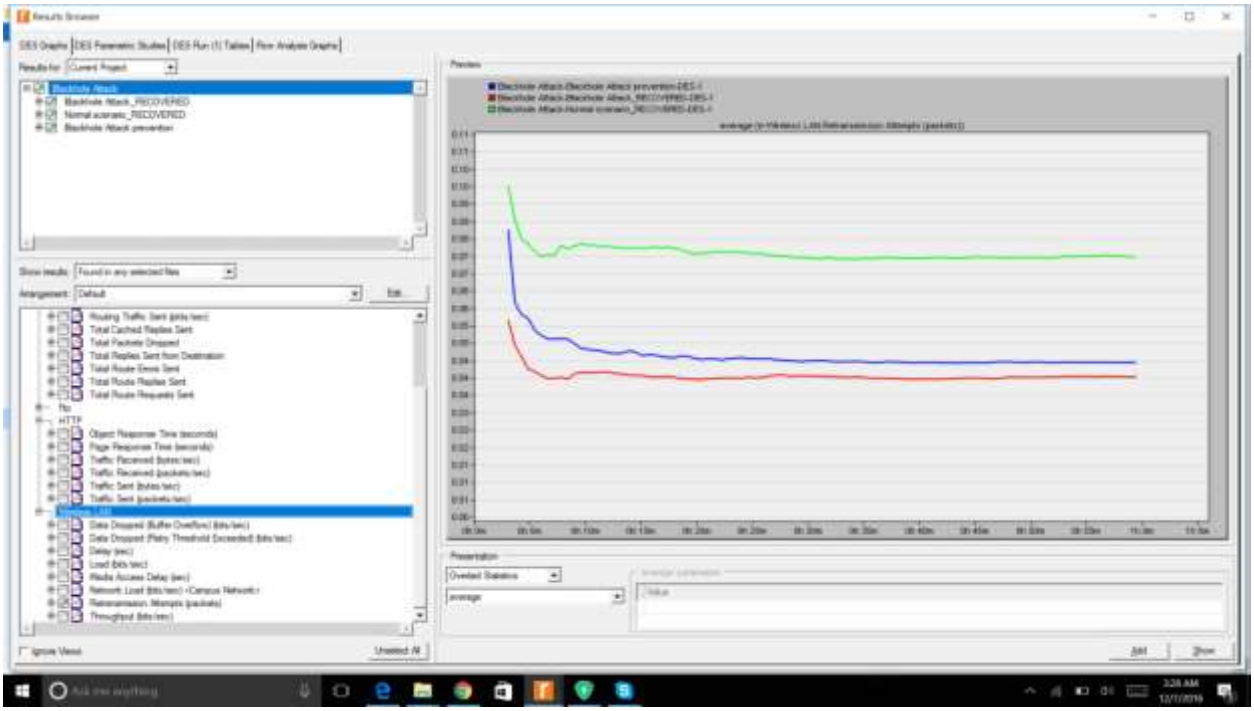
Graph 10.10: Data dropped(Buffer overflow)(bits/sec)



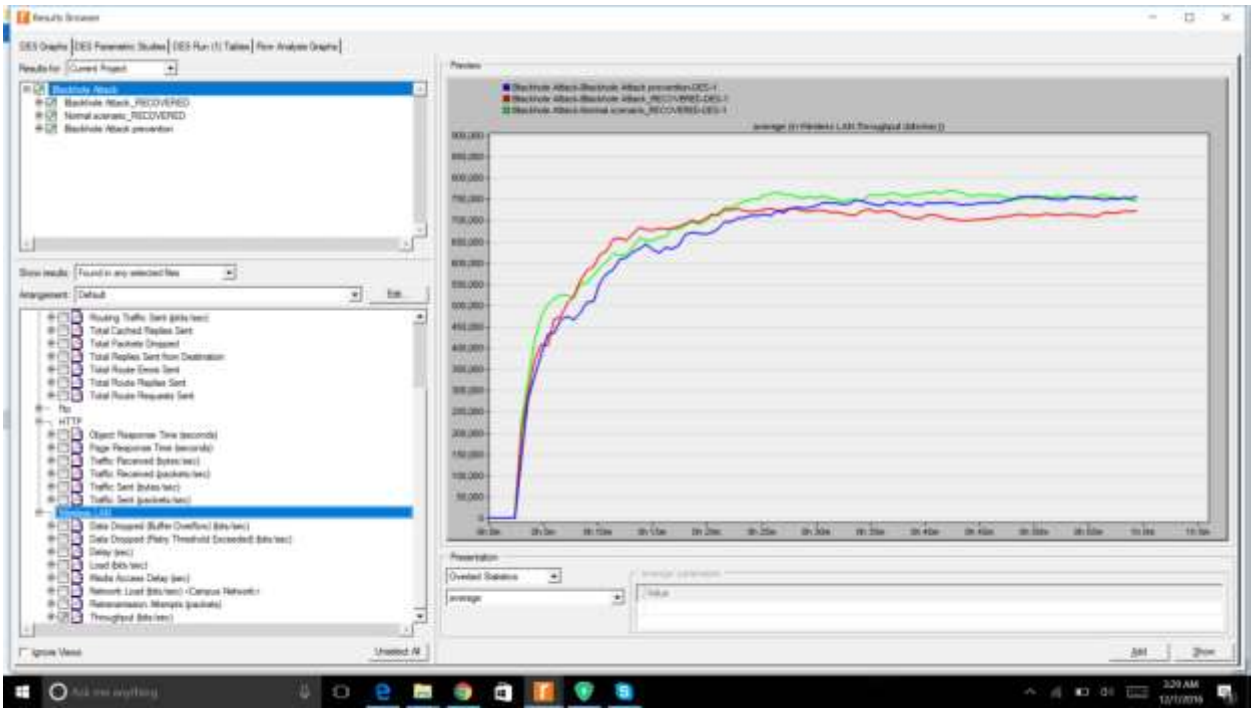
Graph 10.11: Load(bits/sec)



Graph 10.12: Network load(bits/sec)



Graph 10.13: Retransmission attempts(packets)



Graph 10.14:Throughput(bits/sec)

Conclusion:

From above scenario we come to know that when we make the changes with the attributes of all the protocols in order to prevent Blackhole attack, the changes led to decrease in delay of output scenario. The prevention scenarios is not only verified but also has given the better results than normal scenario.

References:

1) Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao. *Human-centric Computing and Information Sciences*2011 **|DOI:** 10.1186/2192-1962-1-4 © Tseng et al; licensee Springer. 2011 **Received:** 16 October 2011 **Accepted:** 22 November 2011 **Published:** 22 November 2011

   https://hcis-journal.springeropen.com/articles/10.1186/2192-1962-1-4

2) Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil Fault Tolerance Systems Group (GSTF), Instituto de las TIC Avanzadas (ITACA) Universidad Politécnica de Valencia, Campus de Vera s/n, E-46022, Valencia, Spain { jcruizg, jefrilo, ddandres, pgil}@disca.upv.es

   https://users.ece.cmu.edu/~koopman/dsn08/fastabs/dsn08fastabs_ruiz.pdf