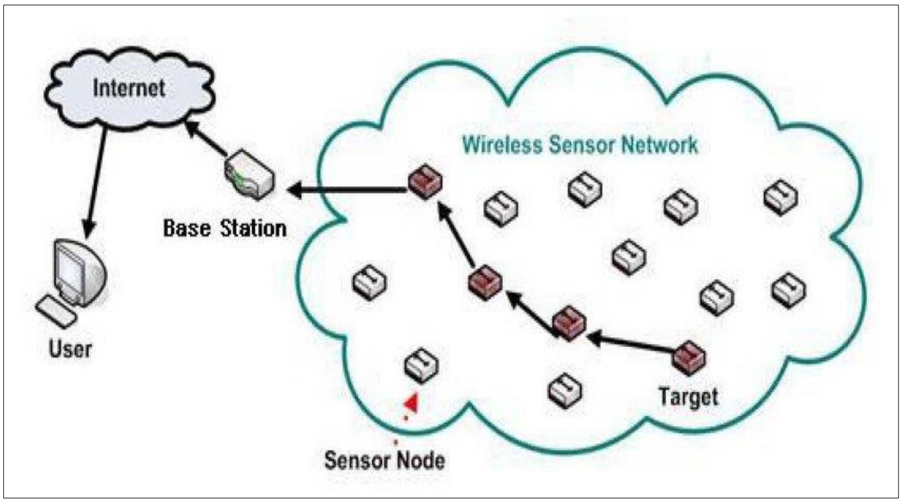
1. Introduction

1.1 Introduction to WSN

A Wireless Sensor Network (WSN) comprises of sovereign sensor devices that are used to supervise physical and environmental conditions like temperature and pressure. The WSN is built of hundreds and thousands of recognizing stations called nodes, where each node consists of one or more sensors having a radio transceiver, an internal/external antenna, a microcontroller and a battery. Wireless sensor networks are the systems that are used to communicate by sensing the behavioral changes and the sensing nodes will collect the data and it will get handled. After data handling, the data will be sent to the receiver.

The wireless sensor networks have to be fortified from network attacks especially at unfavorable situations because data can easily be obtained by the attackers. There are also some security protocols being implemented in sensor networks. There are some limitations in a wireless sensor network like they have limited storage capacity, limited capability of processing and limited energy to transmit data. These drawbacks can make wireless sensor network different from other networks. The imitation of the attacks is done in the NS2 simulator. By imitating, the performance of the network can be monitored.



1.1 Illustration of WSN

Constructing a wireless sensor network (WSN) has become important in all places. The sensor nodes collect the data and direct it to the center station for processing and then it is directed to the user via a wireless medium. A WSN has copious applications in many fields. They are employed in many places. A WSN is used in these applications to supervise the safeguarding, improving the throughput and enhance the defense and safety. For wide deployment, it is required that the sensors should be made smaller and easy on the pocket. There are also multifarious methods being proposed to safeguard the network from different manners of attacks.

Application of WSN

Wireless Sensor Networks (WSNs) have a wide range of applications across various domains due to their ability to monitor, collect, and transmit data from remote or harsh environments. Some common applications of WSNs include:

1. Environmental Monitoring:

- Weather forecasting and climate monitoring.
- Air quality and pollution control.
- Forest fire detection and management.
- Water quality and flood monitoring.

2. Agriculture:

- Soil moisture and nutrient level monitoring.
- Crop health and growth tracking.
- Pest and disease detection.
- Livestock tracking and management.
- 3. Healthcare:
- Remote patient monitoring.
- Elderly and disabled patient care.
- Medication adherence tracking.
- Fall detection for the elderly.

4. Industrial Automation:

- Equipment and machinery health monitoring.
- Real-time inventory and supply chain management.
- Process control and optimization.
- Energy management and conservation.

5. Smart Cities:

- Traffic management and control.
- Smart street lighting.
- Waste management and bin status monitoring.
- Noise and pollution monitoring.

6. Military and Defense:

- Battlefield surveillance and reconnaissance.
- Intrusion detection and perimeter security.
- Asset tracking and logistics.
- Unmanned aerial vehicle (UAV) coordination.

7. Disaster Management:

- Earthquake and tsunami early warning systems.
- Search and rescue operations.
- Landslide and avalanche monitoring.
- Wildfire detection and management.

8. Wildlife Monitoring:

- Animal tracking and behavior analysis.
- Biodiversity conservation.
- Poaching detection.
- Habitat and ecosystem monitoring.

9. Structural Health Monitoring:

- Monitoring the condition of buildings, bridges, and infrastructure.
- Detecting and predicting structural failures.
- Preventive maintenance and repair.

10. Home Automation:

- Smart home devices and appliances control.
- Security and surveillance systems.
- Energy-efficient HVAC and lighting systems.
- Home healthcare and well-being monitoring.

11. Retail and Logistics:

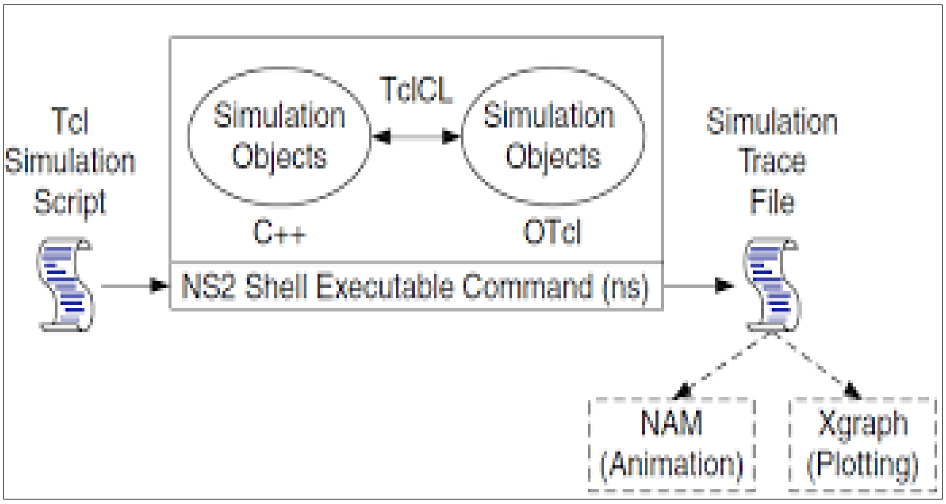
- Inventory tracking and management.
- Supply chain optimization.
- Customer behavior analysis.
- RFID-based product tracking.

12. Oil and Gas:

- Monitoring of pipelines and well sites.
- Gas leak detection.
- Environmental impact assessment.
- Remote valve control.

1.2 Introduction to Network Simulator

Using the network simulator NS2, the attacks in the WSN can be replicated. NS2 makes a replica of a real time network. It is a time-based event driven simulator. The code can be written in such a way that at a particular time, what particular event can happen. The data transfer between the nodes and the attacks can be shown. It has become one of the most widely used open-source simulators. It is a free simulation tool that can be available online. The simulator consists of a wide variety of applications, protocols like TCP, UDP and many network parameters. It runs on various platforms like UNIX, Mac and windows platforms. This NS2 tool allows to develop a model design for wireless sensor network connection between nodes in the network. Based on the network attacks like denial of service, Sybil attacks the network security can be tested. These attacks can be created in the network and the security level of the wireless sensor network can be tested to ensure secure data transmission between the nodes in the network. Figure 1.3 shows the basic architecture of NS2 Simulator. It is provided with a command „ns" to execute the code written in NS2. The name of the Tcl simulation script is passed as an input argument. After executing a simulation trace file is created which can be used to create animation or to plot graph. NS2 Simulator consists of two languages namely C++ and OTcl (Object oriented Tool Command Language). C++ does the internal mechanism i.e., back end and OTcl deals with the front end. The simulation trace file engendered after execution can be used to create animation in a network animator or to plot a graph. The information in the network animator can blogged in data format in nam trace file.



1.2 Basic Architecture of NS2

1.3 Necessity

A WSN has multifarious applications in many fields. It is employed in many places. Ensuring the security in a WSN is of great concern. Because of the constraints in the network, it is susceptible to many attacks. The major attacks include denial of service, Sybil etc. These attacks decrease the performance and efficiency of the network. The attacks are studied in detail and are replicated in a simulator. The characteristics of the attack and the nature of the attack can be known. By simulating, the behavior of the network and the performance can be scrutinized. The network simulated is closer to real time network. By understanding the attacks, proper procedures can be taken in order to detect and prevent them. A simulator holds good for replicating the real time network. By understanding all the problems in the design phase, itself, one can be able to construct a more efficient network.

A network simulator is a software program that can predict the performance of a computer network or a wireless communication network. Since communication networks have become too complex for traditional analytical methods to provide an accurate understanding of system behavior, network simulators are used. In simulators, the computer network is modeled with devices, links, applications, etc., and the network performance is reported. Simulators come with support for the most popular technologies and networks in use today such as 5G, Internet of Things (IoT), Wireless LANs, mobile ad hoc networks, wireless sensor networks, vehicular ad hoc networks, cognitive radio networks, LTE etc.

Network emulation allows users to introduce real devices and applications into a test network (simulated) that alters packet flow in such a way as to mimic the behavior of a live network. Live traffic can pass through the simulator and be affected by objects within the simulation.

The typical methodology is that real packets from a live application are sent to the emulation server (where the virtual network is simulated). The real packet gets 'modulated' into a simulation packet. The simulation packet gets demodulated into a real packet after experiencing effects of loss, errors, delay, jitter etc., thereby transferring these network effects into the real packet. Thus it is as-if the real packet flowed through a real network but in reality it flowed through the simulated network. Emulation is widely used in the design stage for validating communication networks prior to deployment.

1.4 Objectives

It has several objectives, including:

1. **Network Protocol Research and Development:** NS-2 is designed to provide a platform for researchers to design, develop, and evaluate various networking protocols and algorithms. It allows researchers to simulate and test their ideas in a controlled and repeatable environment before implementing them in real-world networks.

2. **Performance Evaluation:** NS-2 enables the performance evaluation of network protocols, algorithms, and configurations under various network conditions. Researchers can analyze parameters such as throughput, latency, packet loss, and scalability to understand how different network designs perform.

3. **Educational Tool:** NS-2 serves as an educational tool in academic settings. It helps students and researchers understand the principles of network protocols, routing algorithms, and network behavior through simulation and experimentation.

4. **Network Modeling:** NS-2 provides a platform to model and simulate a wide range of network topologies, including wired and wireless networks. Users can create complex network scenarios to study the behavior of different network components.

5. **Customization and Extensibility:** NS-2 is designed to be highly customizable and extensible. Users can create custom network models, implement new protocols, and modify existing ones to suit their research needs.

6. **Simulate Real-World Scenarios:** NS-2 allows researchers to simulate real-world networking scenarios, such as mobile ad-hoc networks (MANETs), wireless sensor networks (WSNs), and internet protocols like TCP/IP, providing a flexible environment for different research areas.

7. **Code Validation:** Researchers can validate their implementations against established protocols and standards by comparing the results of their simulations with those of known reference implementations.

8. **Debugging and Testing:** NS-2 offers debugging tools and the ability to trace events and analyze simulation results, helping researchers identify and address issues in their network designs and protocols.

9. **Open Source and Community Support:** NS-2 is open-source software, which encourages a collaborative community of users and developers to contribute, share, and enhance the tool's capabilities. This open nature promotes innovation and the development of new features.

10. **Cross-Platform Compatibility:** NS-2 is designed to work on multiple operating systems, making it accessible to a broad user base regardless of the platform they are using.

1.5 Theme of Mini Project

The theme of a mini project on "Detection of Attacks in Network" focuses on developing and implementing techniques to identify and mitigate malicious activities and security threats within computer networks. This is a critical area in cyber security and network management, and it offers numerous opportunities for research and practical applications. Here's an outline of key aspects and potential subtopics for such a project:

Introduction to network security

1 Provide an overview of the importance of network security.

2 Explain the significance of detecting and preventing network attacks.

Types of different network attacks

1 Discuss common network attacks such as DoS attacks, malware infections, Wormwhole attack, Sybil attack, Blackhole attack etc.

2 Explain the characteristics and goals of each attack type.

Case Studies and Tools

1 Provide examples of real-world network attack incidents and how they were detected.

2 Introduce popular NS2 tool and their features.

Challenges and Limitations

1 Address the challenges in network attack detection, such as false positives and false negatives.
2 Discuss evasion techniques used by attackers to bypass detection systems.

Project Implementation

1 Develop a network attack detection system or prototype.
2 Use open-source tools or programming languages for implementation.

Conclusion and Future Work

1 Summarize the project's findings and the importance of network attack detection.
2 Suggest areas for future research and improvement.

References

1 Cite academic papers, books, and online resources that were used for the project.
2 Research Papers.

2. LITERATURE SURVEY

Sr. No.	Paper Title	Author	Abstract	Conclusion	Publication Date
1.	Replication of attacks in a wireless sensor network using NS2	Tejaswi Singh, Aatish Gandotra	Wireless Sensor Network (WSN) comprises of sovereign sensor devices that are used to supervise physical and environmental conditions like temperature and pressure. The WSN is built of hundreds and thousands of recognizing stations called nodes, where each node consists of one or more sensors having a radio transceiver, an internal/external antenna, a microcontroller and a battery. Wireless sensor networks are the systems that are used to communicate by sensing the behavioral changes and the sensing nodes will collect the data and it will get handled.	WSN's are of huge demand. The request for wireless sensor networks is increasing rapidly, because the growth of using WSN has increased.	Oct-2015
2.	Survey on Network Stimulators	D. Krishna Chaitanya, Dr. Arindam Ghosh	Simulation software plays a vital role in real world implementation. Practically hardware setup of network topologies is very costly and strenuous to modify often. Hence various simulators act as the prototype of the real system.	The paper presents comparative study and the brief description of various Network Stimulators.	Jan-2011

3.	Analysis of Deniel-of-Service attacks on Wireless Sensor Network	Ronit Patel	Evaluation of Wireless Sensor Networks (WSN) for performance evaluation is a popular research area and a wealth of literature exists in this area. Denial-of-Service (DoS) attacks are recognized as one of the most serious threats due to the resource's constraint Property in WSN.	This paper presented the simulation study of a wireless sensor network to analyze the Denial-of-service attack.	Oct-2018
4.	A Wormhole Attack Detection and Prevention Technique in NS2	Amin Karami, Arish Siddiqui	A WSN has multifarious applications in many fields. It is employed in many places. Ensuring the security in a WSN is of great concern. Because of the constraints in the network, it is susceptible to many attacks. The major attacks include wormhole attack.	Over the years, wireless sensor networks have gained much popu- larity, because of its operating nature in day to day use in wireless channels. Wormhole attack can significantly degrade network per- formance	Sep-2017
5.	Blackhole Attack Detection and Prevention Mechanism Using NS2 Simulation	Ashwini V. Jatt, V.J.K. Kishor Sonti	A blackhole attack is a type of security threat in wireless ad-hoc networks and mobile ad-hoc networks (MANETs). In this attack, a malicious node in the network, known as the "blackhole," falsely advertises itself as having the shortest path to a destination node and then drops or absorbs all data packets sent to it without	In this paper, technique for detection and removal of blackhole attacker has been presented.	Nov-2019

			forwarding them to the intended recipient. This malicious behavior can disrupt network communication and compromise data integrity and availability. Blackhole attacks can have serious consequences in scenarios where network nodes rely on each other to route data.		

2.1 Table for Literature Survey

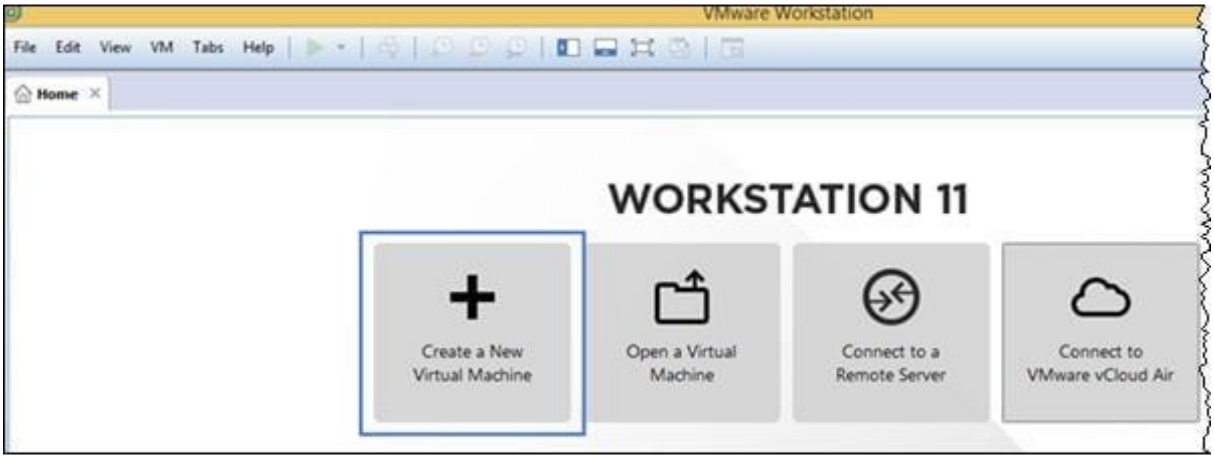
Steps to Install and Configure VMWare

1) Download the VMWare workstation. The setup is around 307 MB.

2) Install VMWare on your machine. Setup is simple and requires clicking the Next button a couple of times.

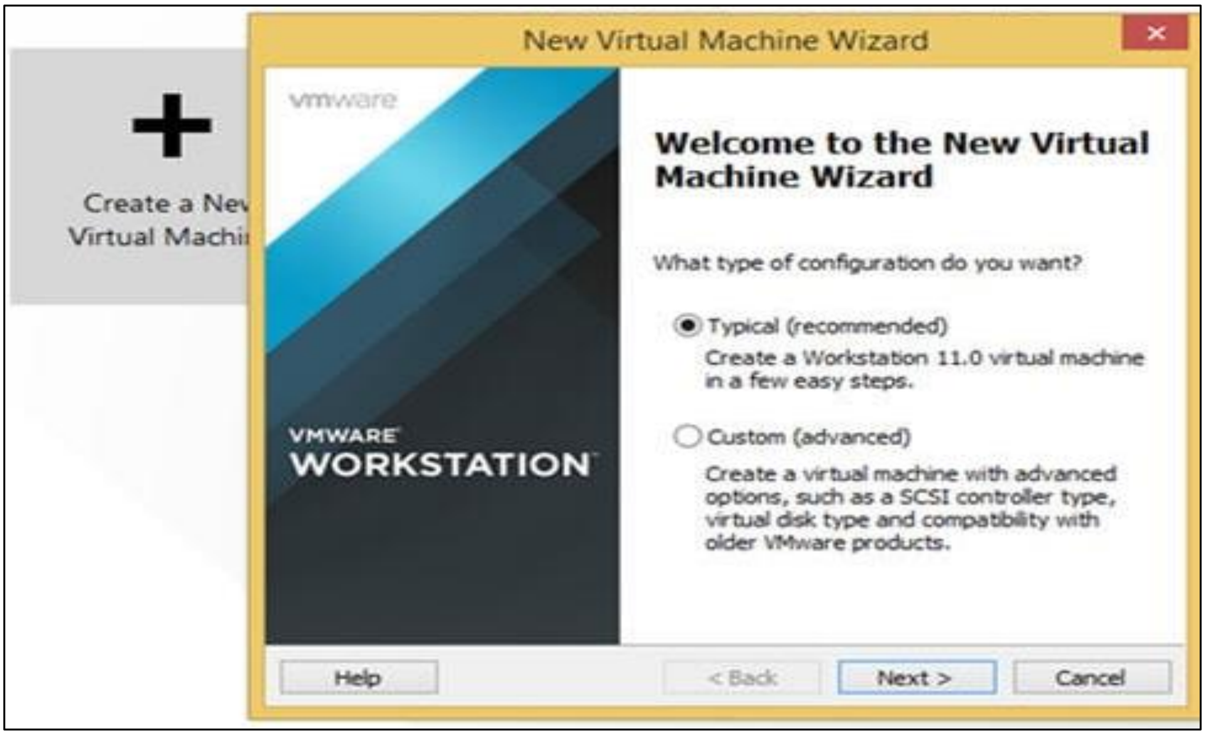
3) After installation open the VMWare workstation using either the start menu or shortcut created on the desktop.

4) Click on "Create a New Virtual Machine".


VMware Workstation
File Edit View VM Tabs Help
Home
WORKSTATION 11
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
Connect to VMware vCloud Air

2.1 VMWare Station

5) With default "Typical" selected, click on the Next button.


New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

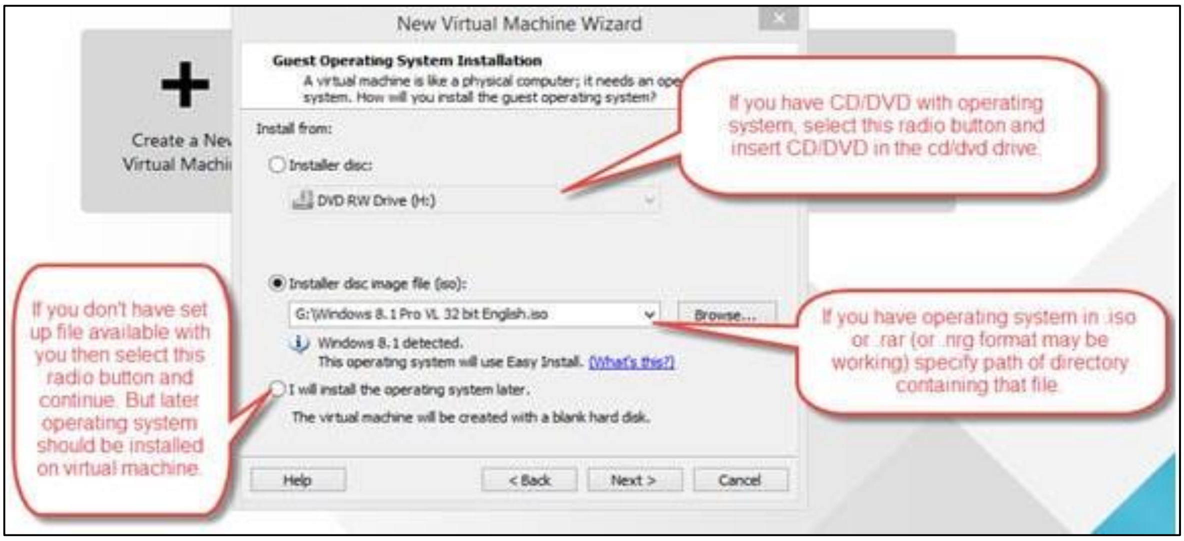
What type of configuration do you want?

● Typical (recommended)
Create a Workstation 11.0 virtual machine in a few easy steps.

○ Custom (advanced)
Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

2.2 VMWare Wizard

6) Specify the path of the operating system setup file.



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an ope system. How will you install the guest operating system?

Install from:

○ Installer disc:

DVD RW Drive (H:)

● Installer disc image file (iso):

G:\Windows 8.1 Pro VL 32 bit English.iso

Windows 8.1 detected.
This operating system will use Easy Install. (What's this?)

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

If you have CD/DVD with operating system, select this radio button and insert CD/DVD in the cd/dvd drive.

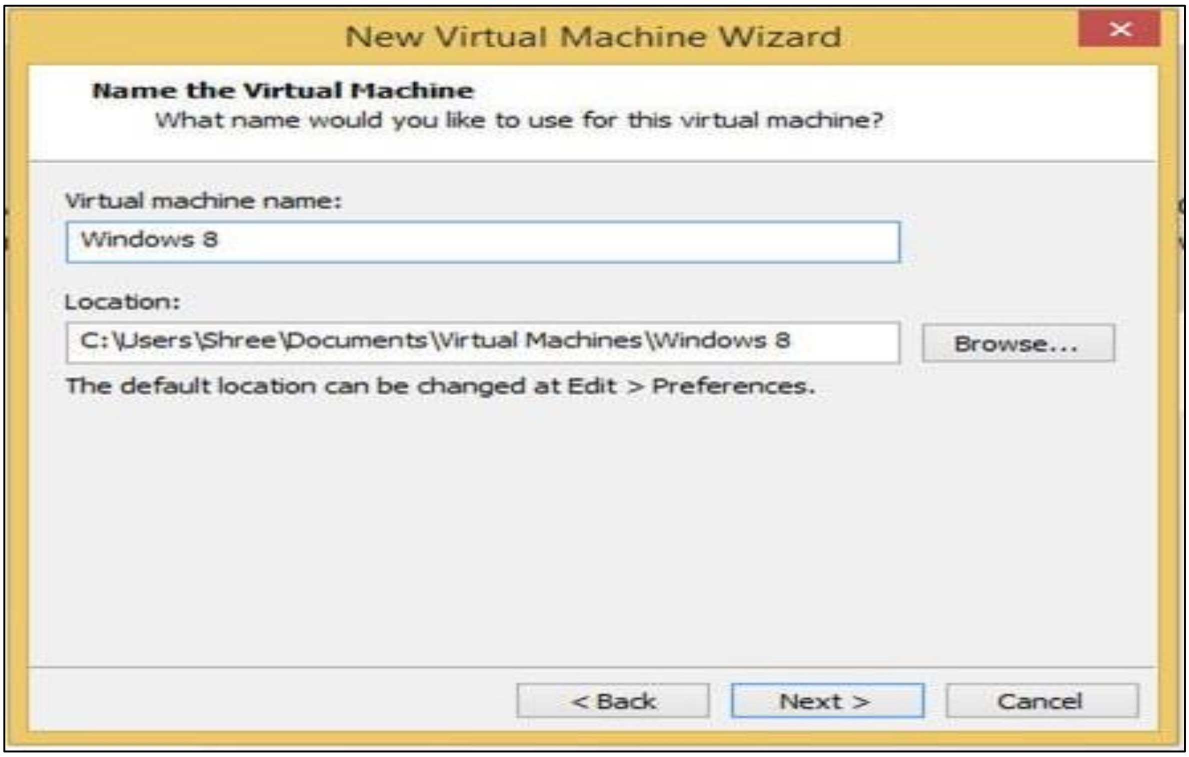
If you have operating system in .iso or .rar (or .nrg format may be working) specify path of directory containing that file

If you don't have set up file available with you then select this radio button and continue. But later operating system should be installed on virtual machine.

2.3 OS Setup

7) In the Next step you need to specify the key or serial number of the operating system. If you are using the trial version then that part can be skipped.

8) Enter the name for the virtual machine and specify a path to the directory where you want to create your virtual machine. It is recommended that the drive you're selecting to install a virtual machine should have sufficient space.



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

Windows 8

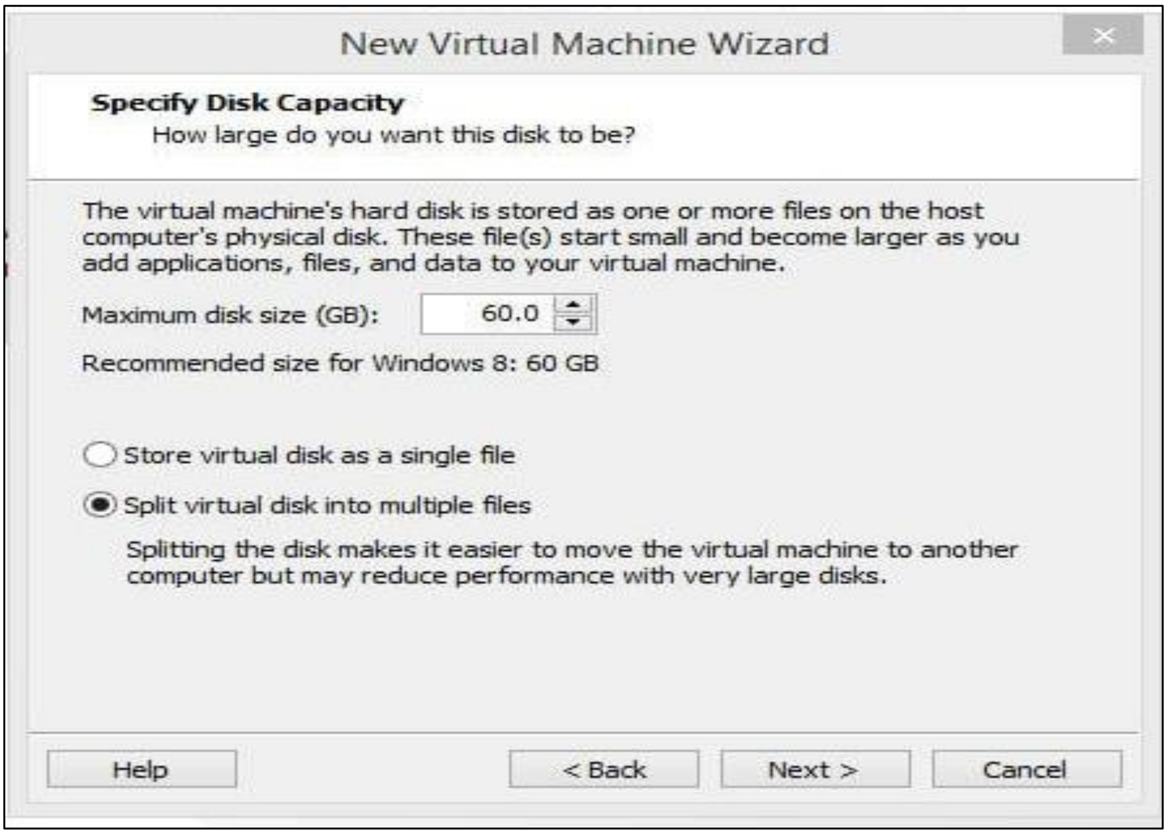
Location:

C:\Users\Shree\Documents\Virtual Machines\Windows 8

The default location can be changed at Edit > Preferences.

2.4 New VM Wizard

9) Specify the amount of disk space you want to allocate for a virtual machine. Allocate disk space according to the size of software you are going to install on the virtual machine.



New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 60.0

Recommended size for Windows 8: 60 GB

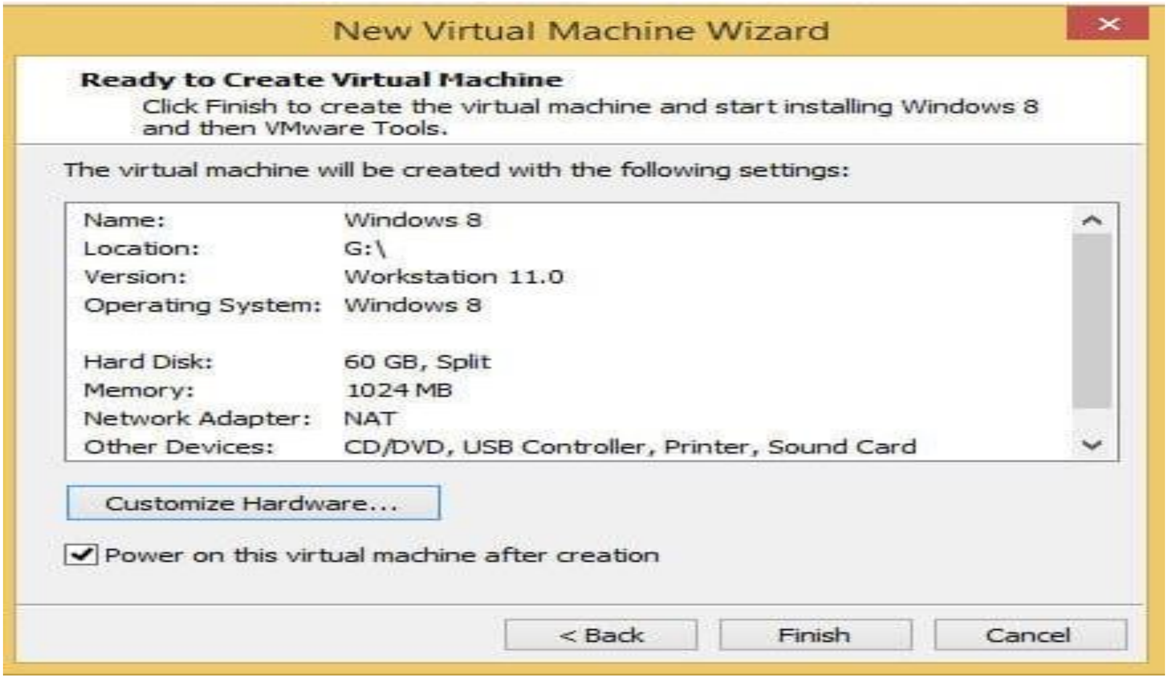
○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

2.5 Disk Management

10) On the next screen it will show the configuration you selected for a virtual machine.



New Virtual Machine Wizard

Ready to Create Virtual Machine
Click Finish to create the virtual machine and start installing Windows 8 and then VMware Tools.

The virtual machine will be created with the following settings:

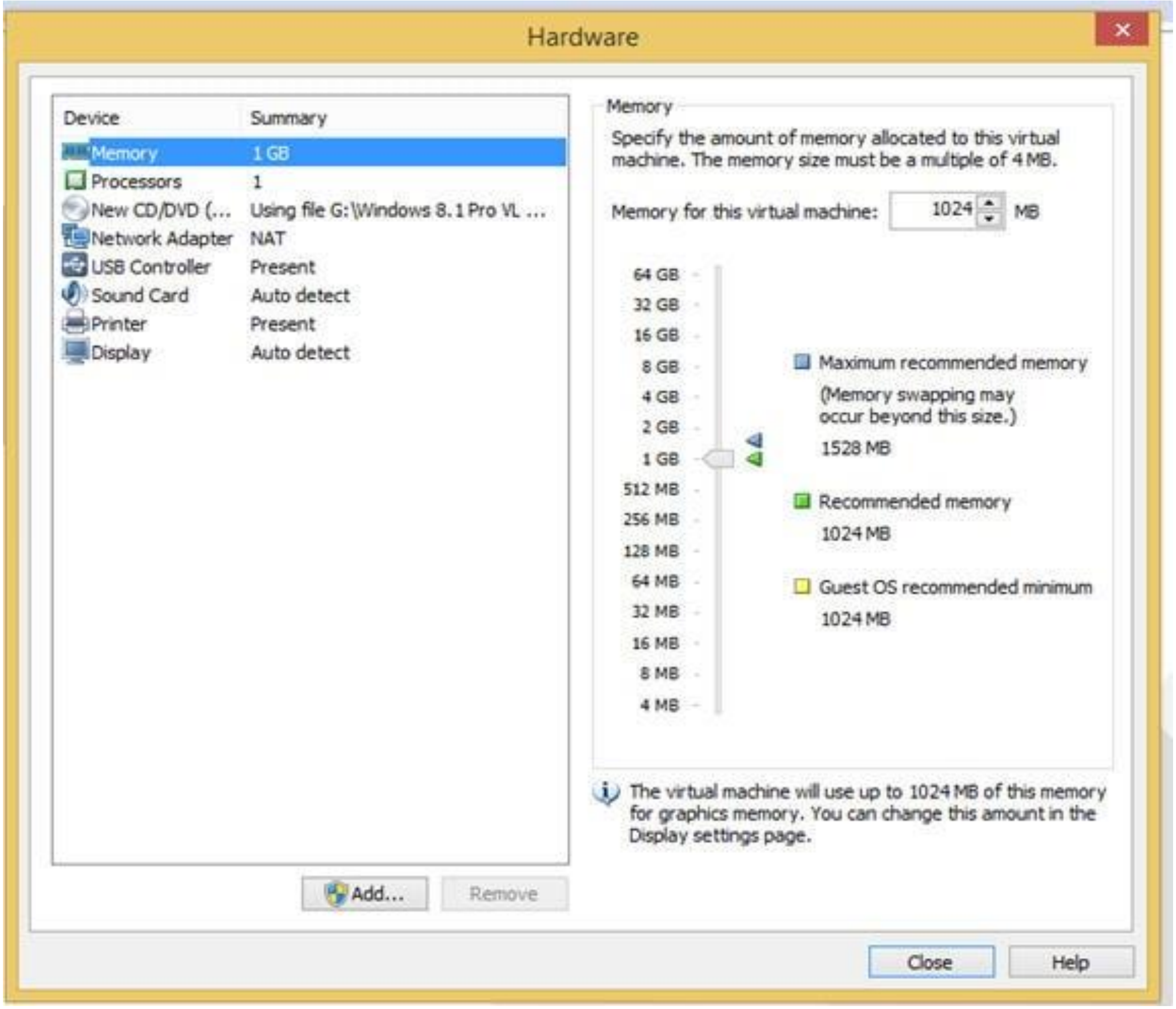
```
Name:               Windows 8
Location:           G:\
Version:            Workstation 11.0
Operating System:   Windows 8

Hard Disk:          60 GB, Split
Memory:             1024 MB
Network Adapter:    NAT
Other Devices:      CD/DVD, USB Controller, Printer, Sound Card
```

☑ Power on this virtual machine after creation

2.6 Ready to Create VM

11) It will allocate Hardware according to the default settings but you can change it by using Customize Hardware button on the screen above.

You can specify what amount of RAM a processor has to be allocated for a virtual machine. Do not allocate complete RAM or complete Processor for a virtual machine. Also, do not allocate very little RAM or processor. Leave the default settings or allocate them in such a way that your application should be able to run on the virtual machine. Else it will result in a slow virtual machine.



Device	Summary
Memory	1 GB
Processors	1
New CD/DVD (...	Using file G:\Windows 8.1 Pro VL ...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 1024 MB

■ Maximum recommended memory
(Memory swapping may occur beyond this size.)
1528 MB

🟩 Recommended memory
1024 MB

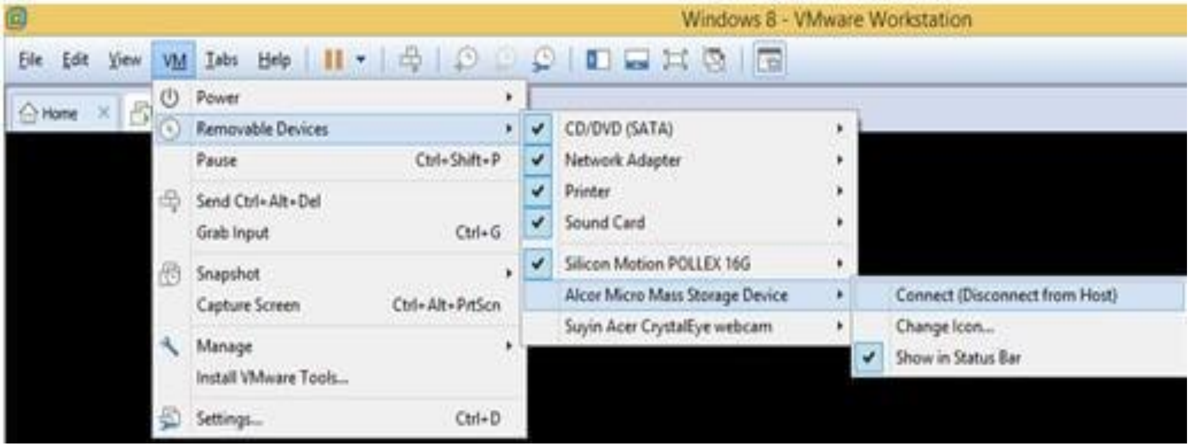
□ Guest OS recommended minimum
1024 MB

The virtual machine will use up to 1024 MB of this memory for graphics memory. You can change this amount in the Display settings page.

2.7 Hardware Selection

12) Click on the Finish button to create the virtual machine at the specified location and with specified resources.

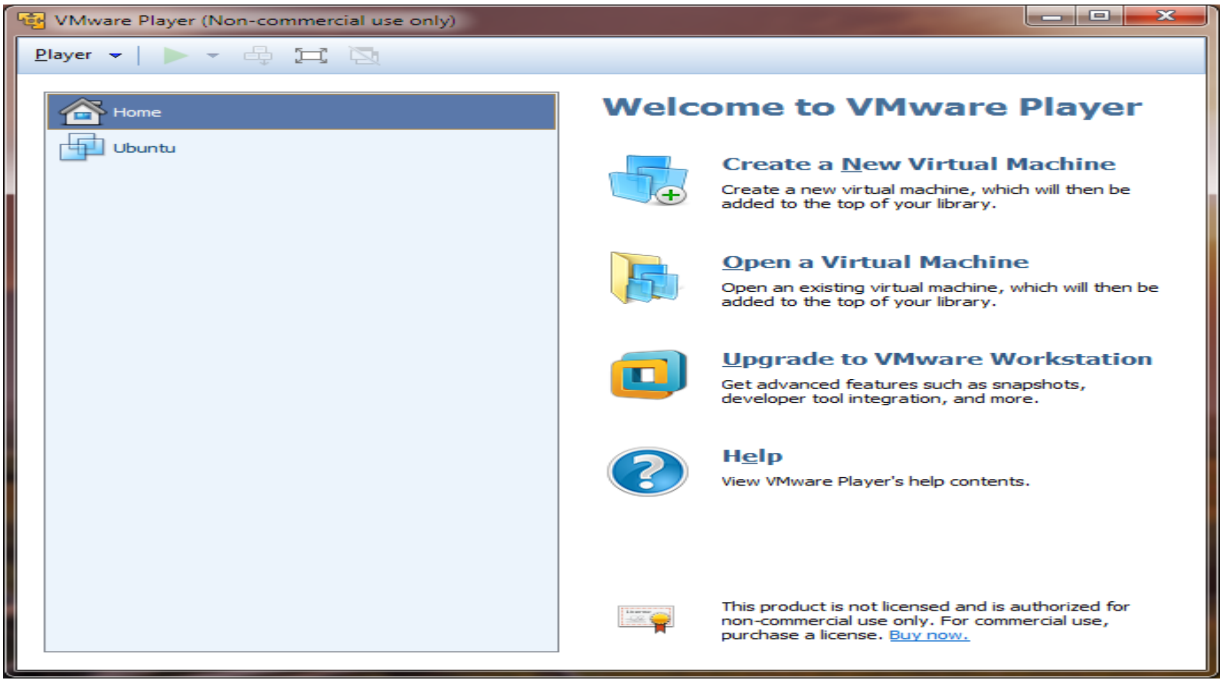
If you have specified a valid file (.iso, .rar., .nrg) for the operating system it will take standard time to complete the operating system set up on the virtual machine, and then it will be ready to use your regular OS.



2.8 Display of VM Tools

Steps to Install Ubuntu Operating System in VMWare

Step1 Open VMware Player



Welcome to VMware Player

Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

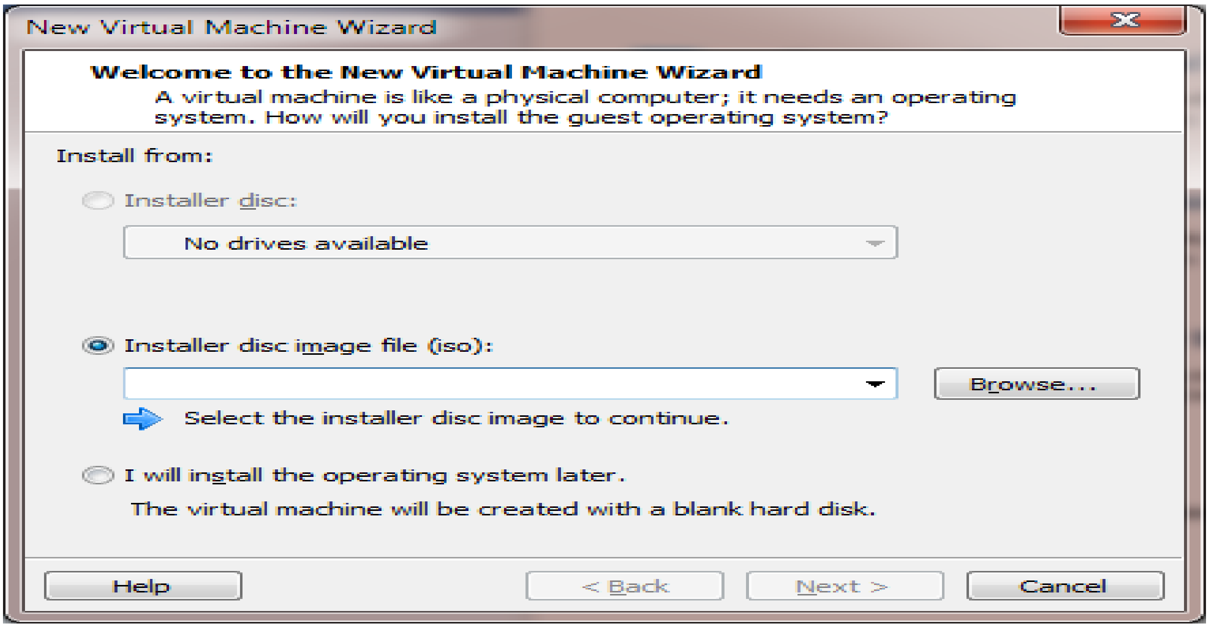
Upgrade to VMware Workstation
Get advanced features such as snapshots, developer tool integration, and more.

Help
View VMware Player's help contents.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

2.9 How to install Ubuntu

Step 2 Click on "Browse" to select installer disc image



Welcome to the New Virtual Machine Wizard
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:
No drives available

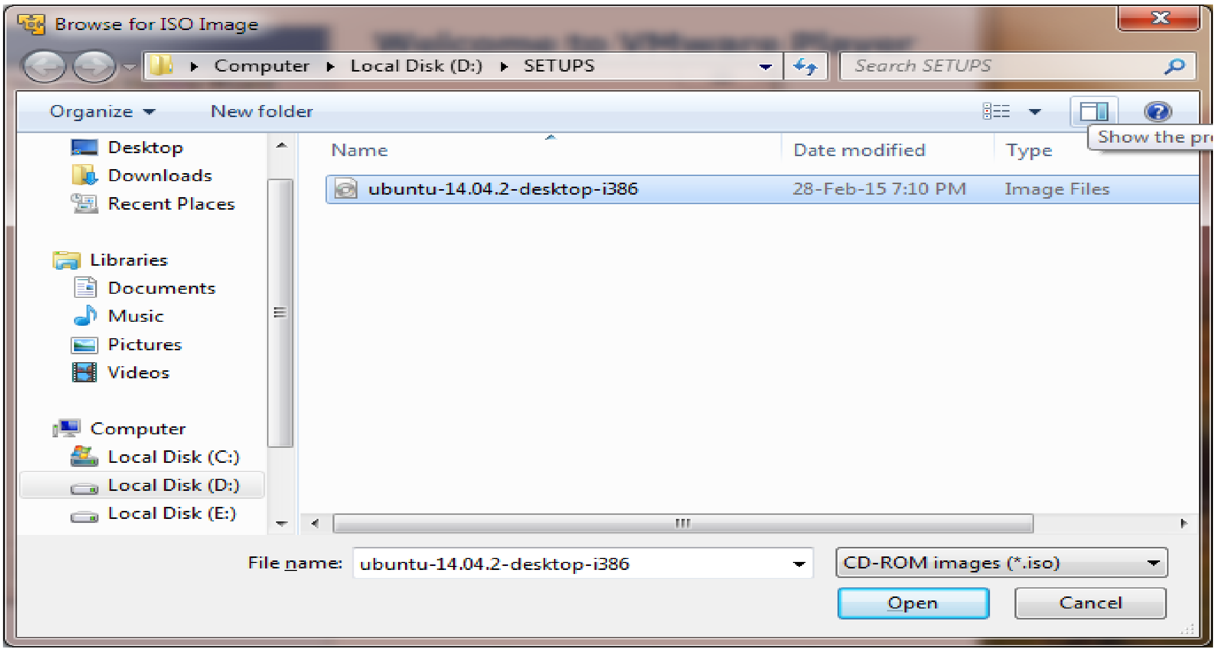
● Installer disc image file (iso):

Select the installer disc image to continue.

○ I will install the operating system later.
The virtual machine will be created with a blank hard disk.

2.10 Browse

Step 3 After selecting the disc image click “Open”



Browse for ISO Image

Computer ▸ Local Disk (D:) ▸ SETUPS

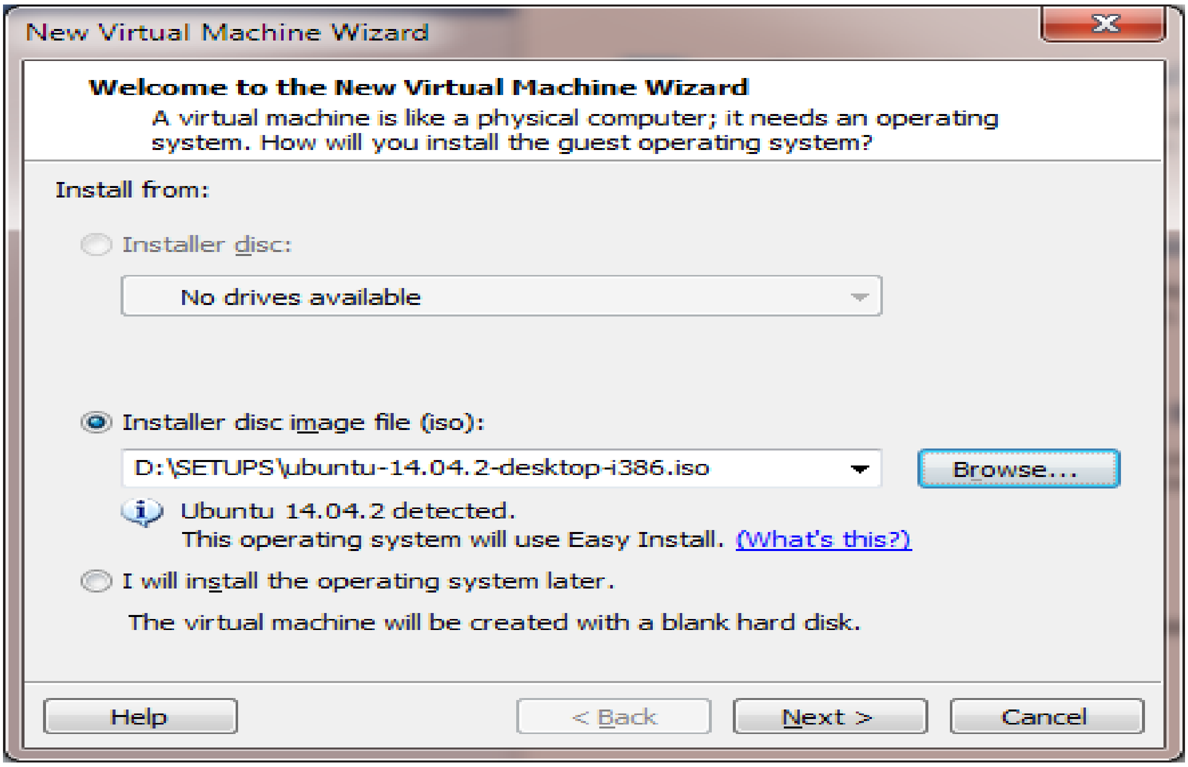
Name	Date modified	Type
ubuntu-14.04.2-desktop-i386	28-Feb-15 7:10 PM	Image Files

File name: ubuntu-14.04.2-desktop-i386

CD-ROM images (*.iso)

2.11 Disk Image

Step 4 Click “Next”



New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

● Installer disc image file (iso):

D:\SETUPS\ubuntu-14.04.2-desktop-i386.iso

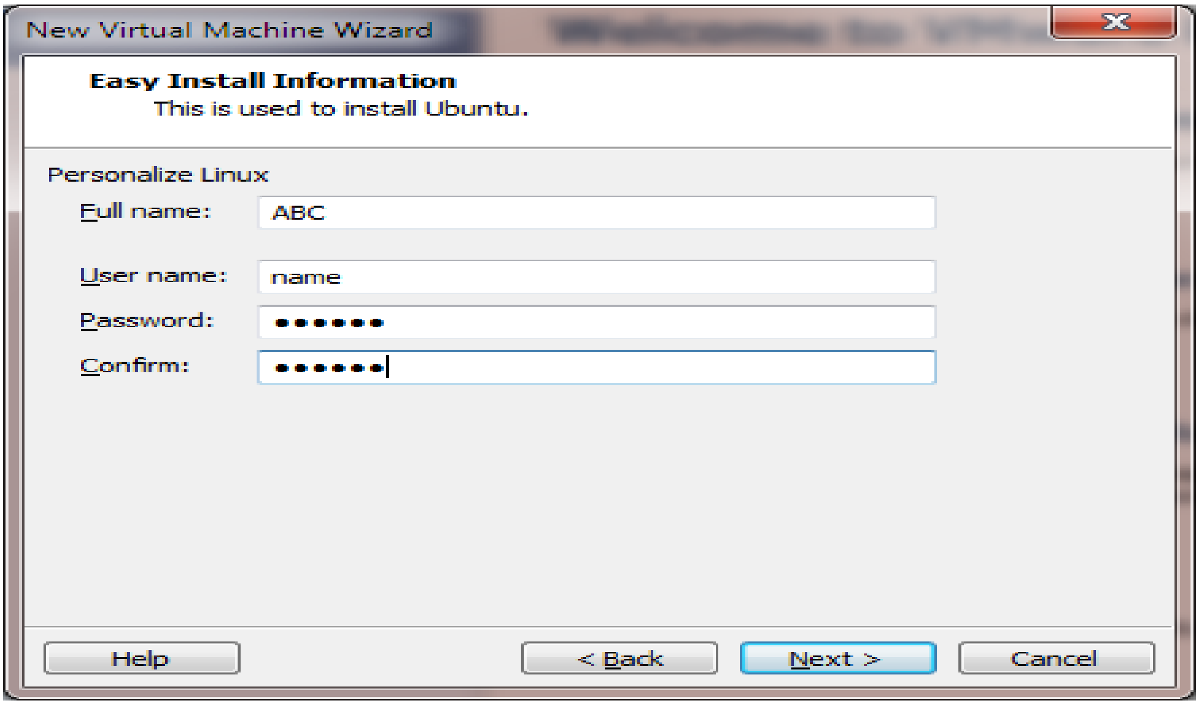
Ubuntu 14.04.2 detected.
This operating system will use Easy Install. (What's this?)

○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

2.12 Installer Disc Image

Step 5 Enter all the details and click "Next"



Easy Install Information
This is used to install Ubuntu.

Personalize Linux

Full name: ABC

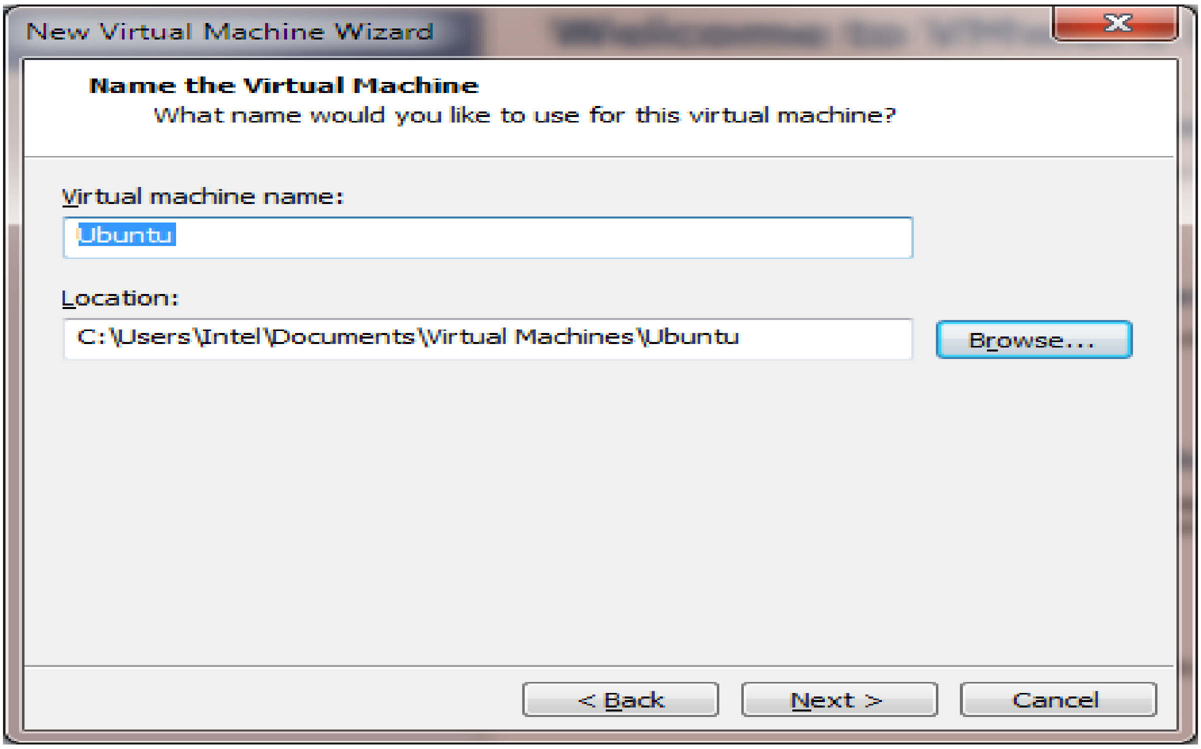
User name: name

Password: ●●●●●●

Confirm: ●●●●●●

2.13 Easy Install Information

Step 6 Supply machine name and Click "Next"



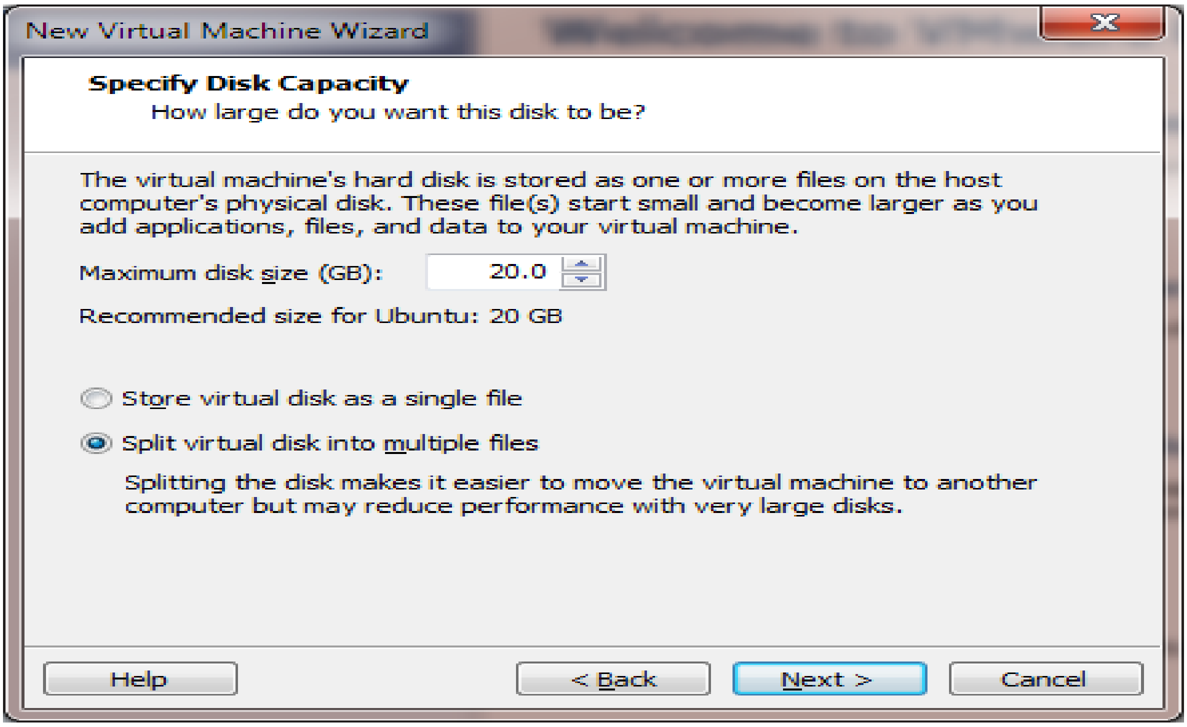
Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name: Ubuntu

Location: C:\Users\Intel\Documents\Virtual Machines\Ubuntu

2.14 Naming the VM

Step 7 Specify disk capacity and Click “Next”



Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 20.0

Recommended size for Ubuntu: 20 GB

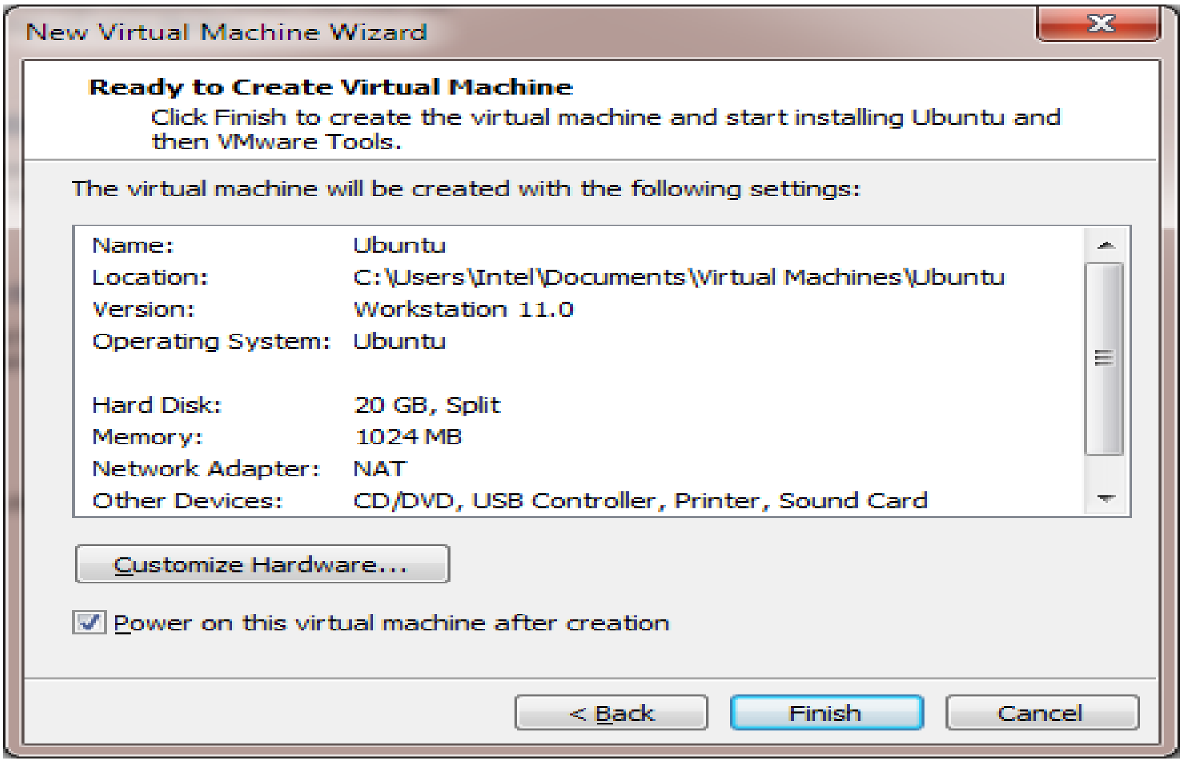
○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

2.15 Disk Capacity

Step 8 Click “Finish”



Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing Ubuntu and then VMware Tools.

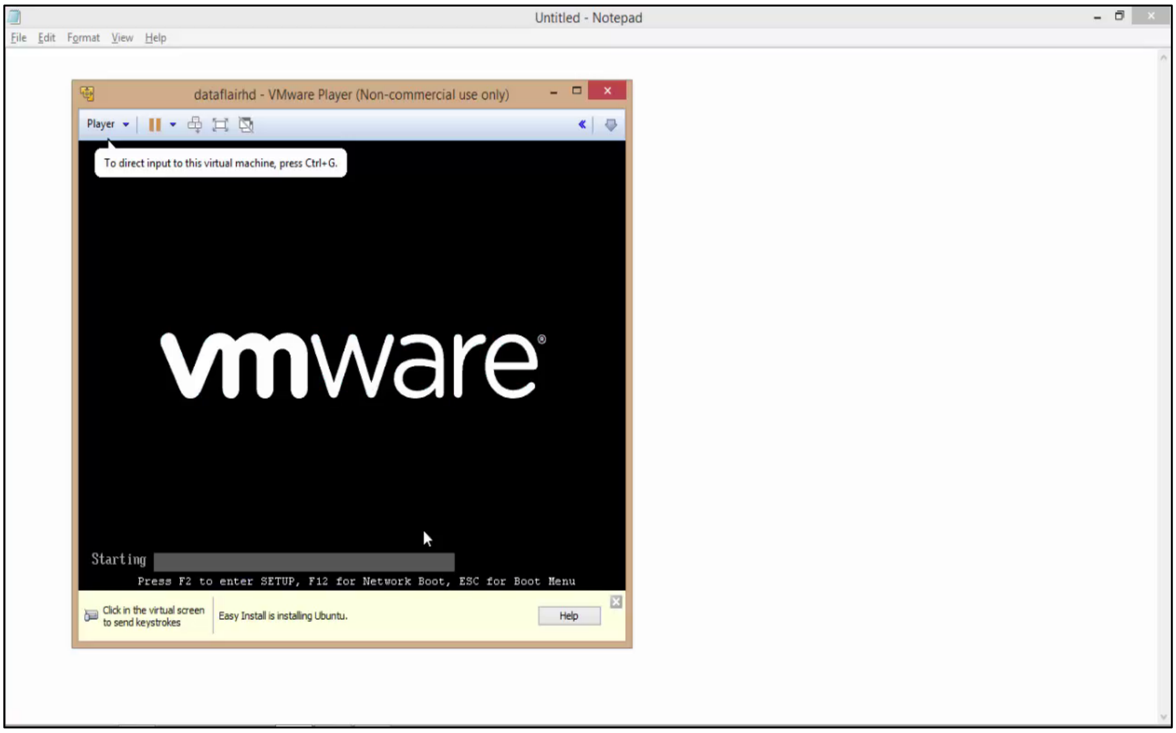
The virtual machine will be created with the following settings:

Name:	Ubuntu
Location:	C:\Users\Intel\Documents\Virtual Machines\Ubuntu
Version:	Workstation 11.0
Operating System:	Ubuntu
Hard Disk:	20 GB, Split
Memory:	1024 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

☑ Power on this virtual machine after creation

2.16 Ready to Create Virtual Machine

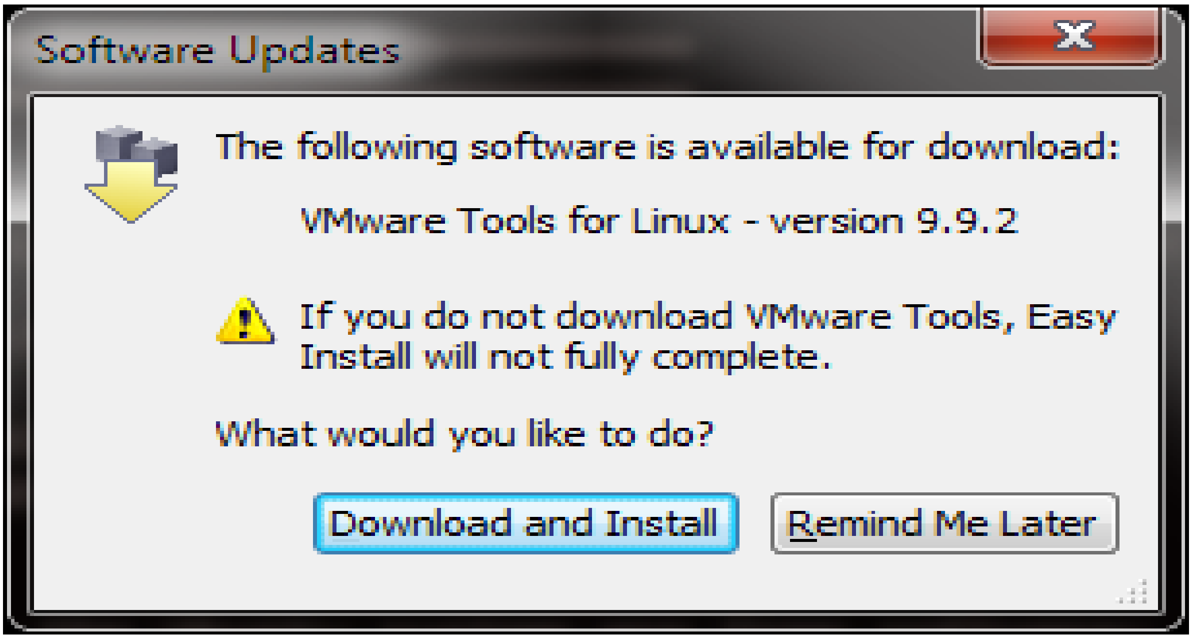
Step 9 Now installation procedure will start and below screen will get displayed



Untitled - Notepad
File Edit Format View Help
dataflairhd - VMware Player (Non-commercial use only)
Player
To direct input to this virtual machine, press Ctrl+G.
vmware
Starting
Press F2 to enter SETUP, F12 for Network Boot, ESC for Boot Menu
Click in the virtual screen to send keystrokes
Easy Install is installing Ubuntu.
Help

2.17 Starting Installation

Step 10



Software Updates

The following software is available for download:

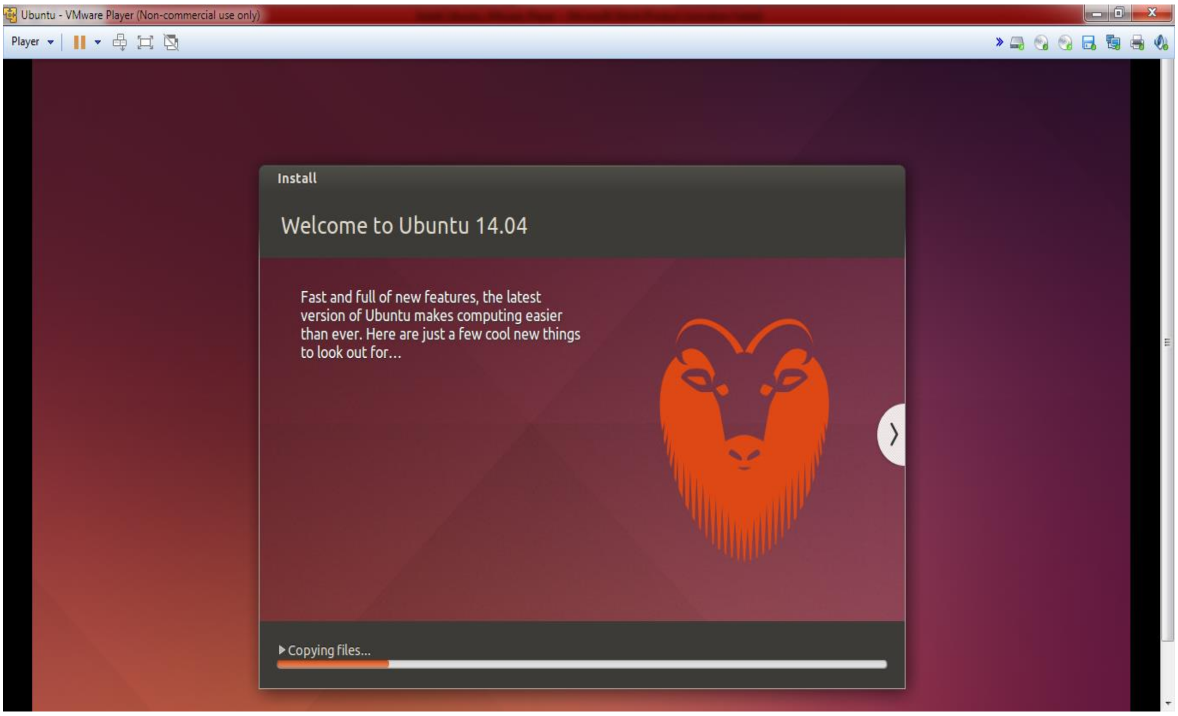
VMware Tools for Linux - version 9.9.2

If you do not download VMware Tools, Easy Install will not fully complete.

What would you like to do?

2.18 Installation of Ubuntu OS – Software Update

Step.11 Installation of Ubuntu OS on VMware Player



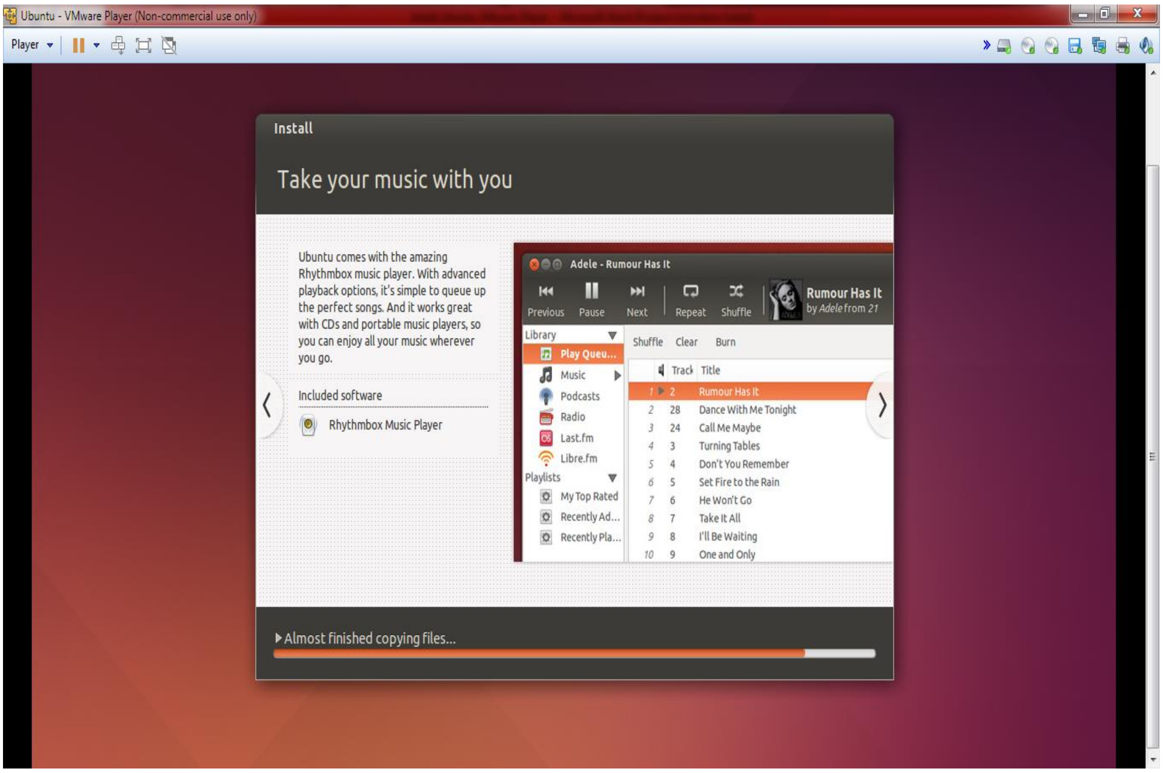
Install

Welcome to Ubuntu 14.04

Fast and full of new features, the latest version of Ubuntu makes computing easier than ever. Here are just a few cool new things to look out for…

▸ Copying files...

2.19 Ubuntu Installation Process



Install

Take your music with you

Ubuntu comes with the amazing Rhythmbox music player. With advanced playback options, it's simple to queue up the perfect songs. And it works great with CDs and portable music players, so you can enjoy all your music wherever you go.

Included software

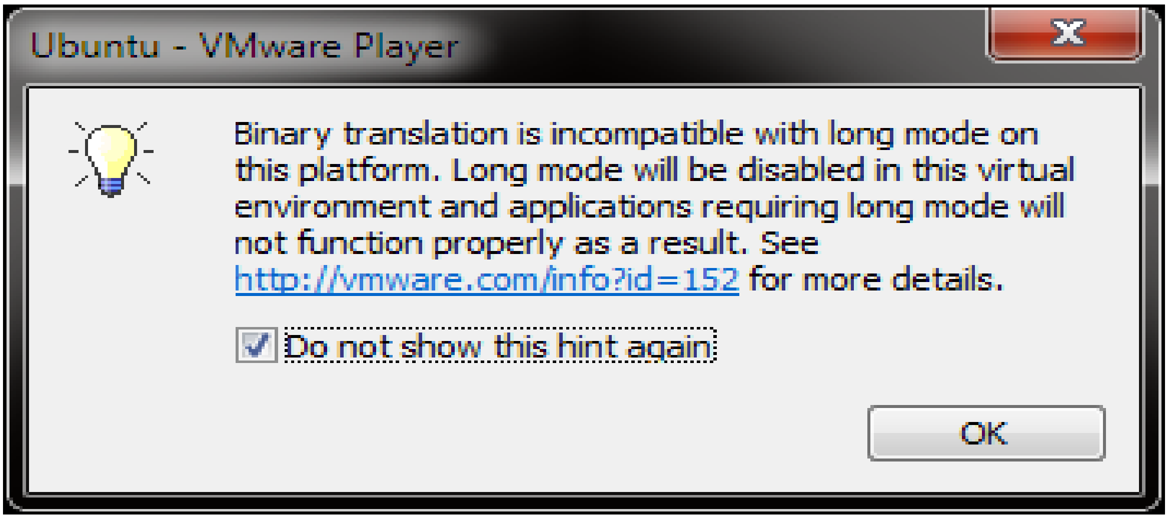
Rhythmbox Music Player

	Track	Title
1	2	Rumour Has It
2	28	Dance With Me Tonight
3	24	Call Me Maybe
4	3	Turning Tables
5	4	Don't You Remember
6	5	Set Fire to the Rain
7	6	He Won't Go
8	7	Take It All
9	8	I'll Be Waiting
10	9	One and Only

▸ Almost finished copying files...

2.20 Ubuntu OS Installation Finishing

Step 12 After completion of installation procedure the following message gets displayed. Check the message and click “OK”



Ubuntu - VMware Player

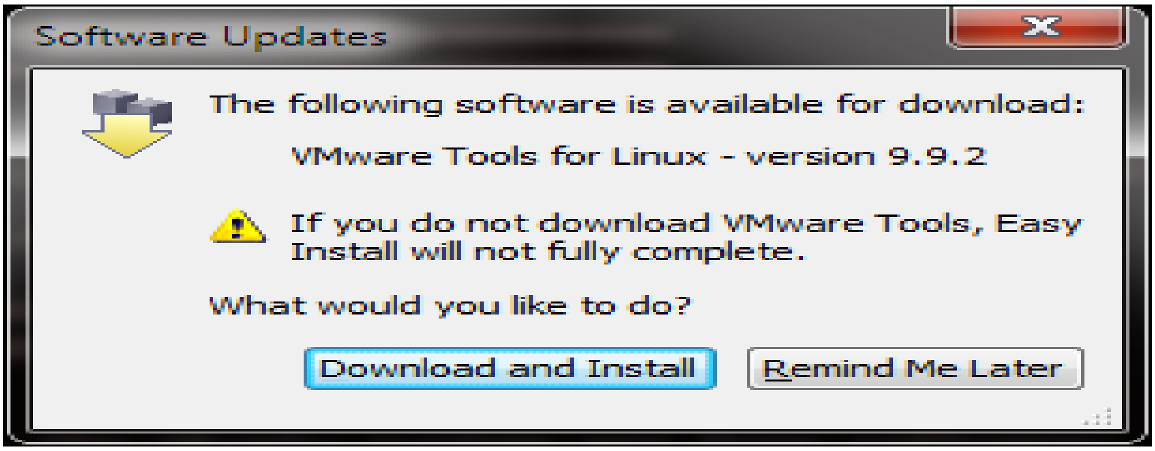
Binary translation is incompatible with long mode on this platform. Long mode will be disabled in this virtual environment and applications requiring long mode will not function properly as a result. See http://vmware.com/info?id=152 for more details.

☑ Do not show this hint again

2.21 Message

Step 13 If on completion of installation procedure if you get the following screen

Click Download and Install



Software Updates

The following software is available for download:

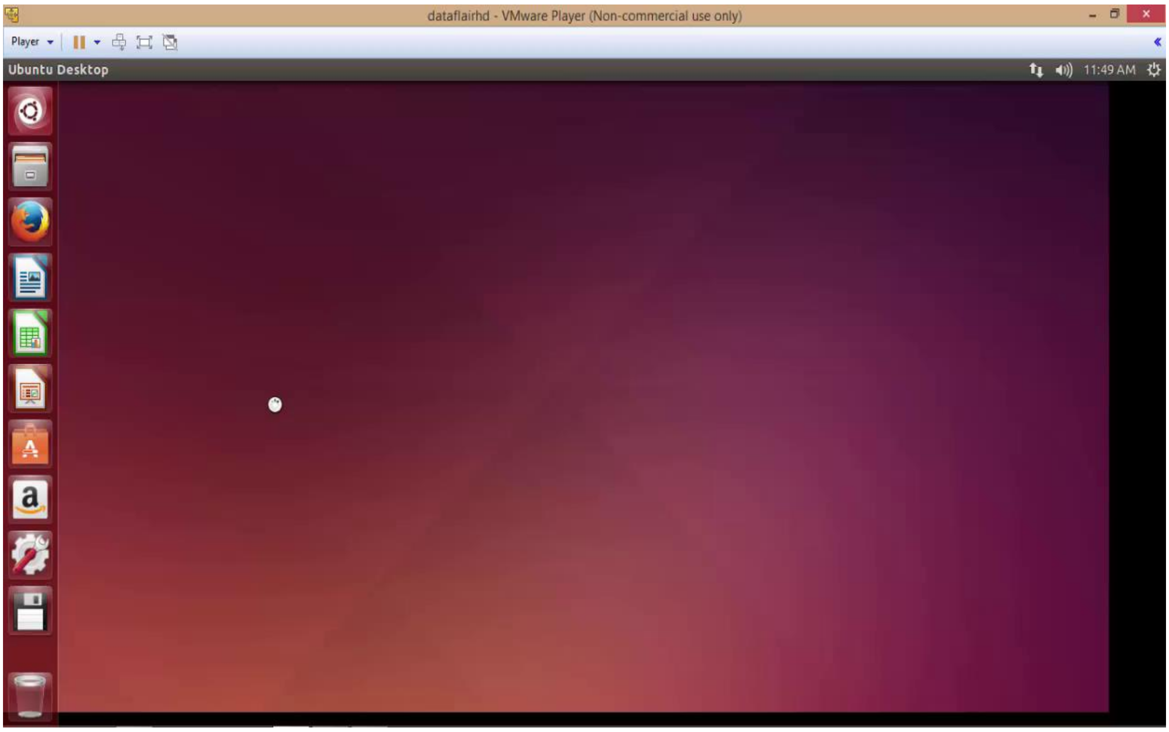
VMware Tools for Linux - version 9.9.2

If you do not download VMware Tools, Easy Install will not fully complete.

What would you like to do?

2.22 Software Update

Step 14 After downloading VMware tools your Ubuntu desktop will get displayed.



2.23 Ubuntu Desktop

Installation of NS2

Step 1 Open terminal/command window and type the following commands one-by-one:

```
sudo apt-get update
sudo apt-get install ns2
sudo apt-get install nam
sudo apt-get install tcl
```

Note: Type administrator password when prompted.

Note: If you see any error/warning messages like file is locked or unable to obtain a lock, etc., just restart the system and try the commands again.

Step 2 Type the command “nam” at the terminal to see the NAM window. If you are unable to see the NAM window, then do the following process:

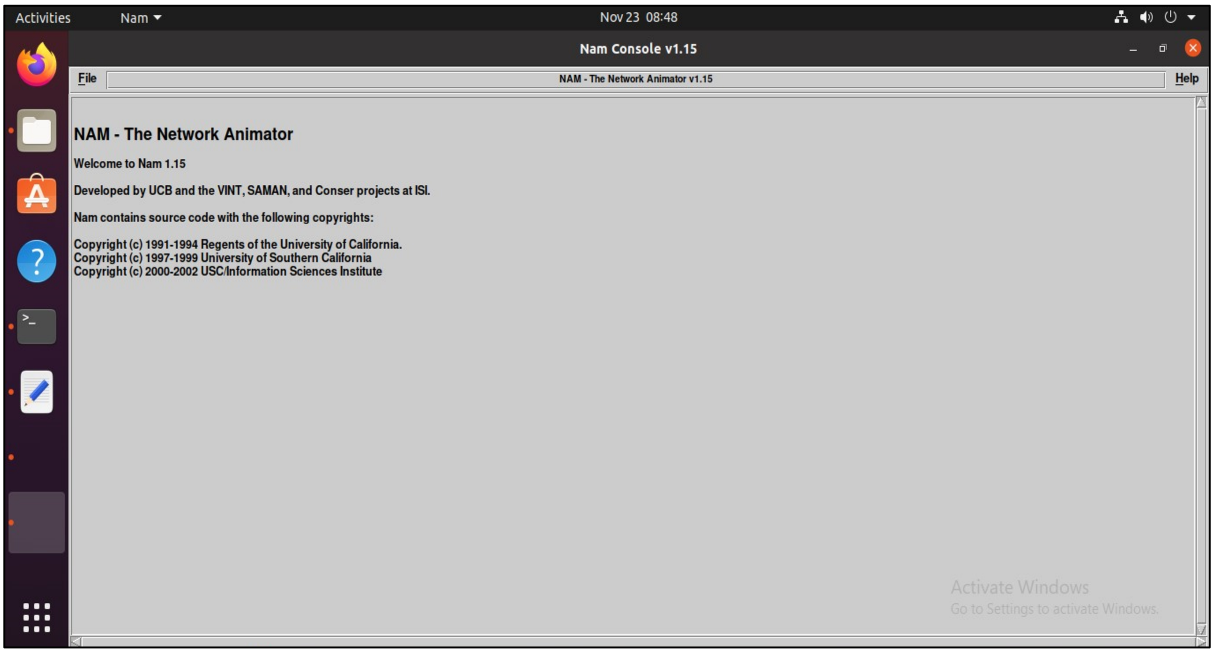
Type the command “sudo dpkg –install nam version”

Now you can work with both ns and nam on your system.

Step 3 Save the following NS2 script in a file named with .tcl extension

Step 4 Run the script using the following command:

Eg: ns ex2.tcl


Activities
Nam
Nov 23 08:48
Nam Console v1.15
File
NAM - The Network Animator v1.15
Help
Activate Windows
Go to Settings to activate Windows.

NAM - The Network Animator

Welcome to Nam 1.15

Developed by UCB and the VINT, SAMAN, and Conser projects at ISI.

Nam contains source code with the following copyrights:

Copyright (c) 1991-1994 Regents of the University of California.
Copyright (c) 1997-1999 University of Southern California
Copyright (c) 2000-2002 USC/Information Sciences Institute

2.24 NAM Software

3. System Development

3.1 Requirement Specification

1. Functional Requirement

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Sybil Attack is a type of attack seen in peer-to-peer networks in which a node in the network operates multiple identities actively at the same time and undermines the authority/power in reputation systems. The main aim of this attack is to gain the majority of influence in the network to carry out illegal (with respect to rules and laws set in the network) actions in the system.

The Blackhole attack works by blocking network traffic from a host or container. It drops Internet Protocol (IP) packets at the transport layer by using traffic policing features built into the Linux Kernel and the Windows Filtering Platform for Windows hosts.

A wormhole receives a message at its "origin end" and transmits it at its "destination end." Note that the designation of wormhole ends as origin and destination is dependent on the context. We also assume a wormhole is passive (i.e., it does not send a message without receiving an inbound message) and static (i.e., it does not change its location).

2. Non-Functional Requirement

Requirements (NFRs) are system qualities that guide the design of the solution and Nonfunctional often serve as constraints across the relevant backlogs. As opposed to functional requirements, which specify how a system responds to specific inputs, nonfunctional requirements are used to specify various system qualities and attributes, such as:

1. Performance: Fast system and it should respond to requests

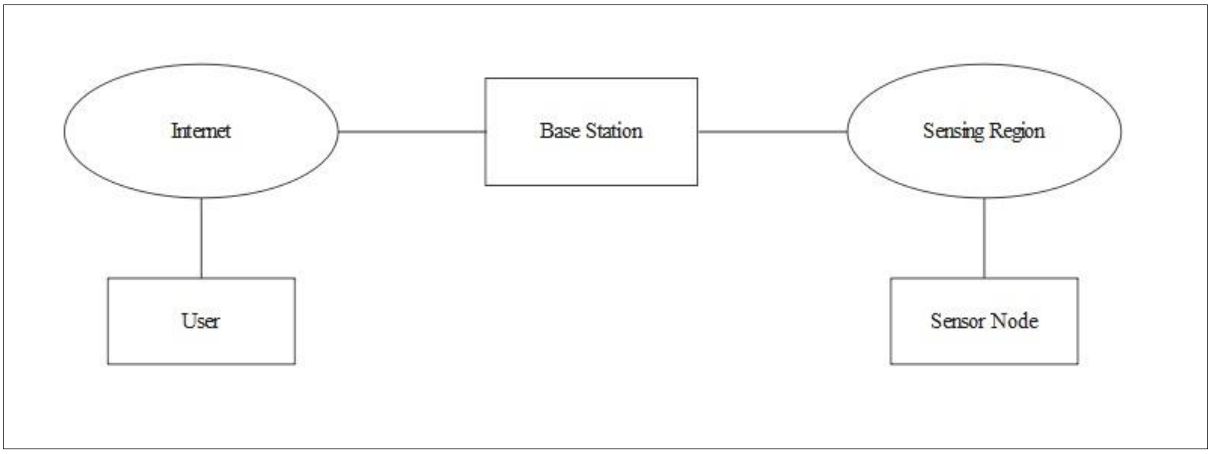
2. Scalability: System can handle an increase in users or workload

3. Security: System should protect against malicious attacks and unauthorized access.

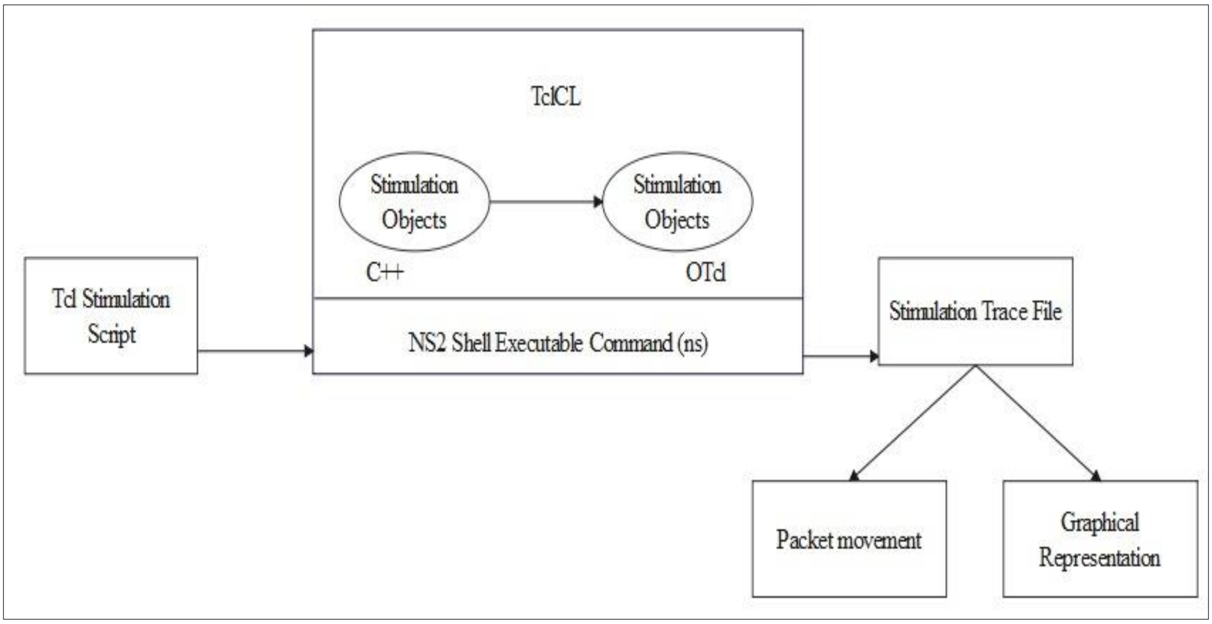
4. Usability: Using NS2 it is easy to detect the system attacks.

5. Maintainability: System is easy to maintain the malicious attacks.

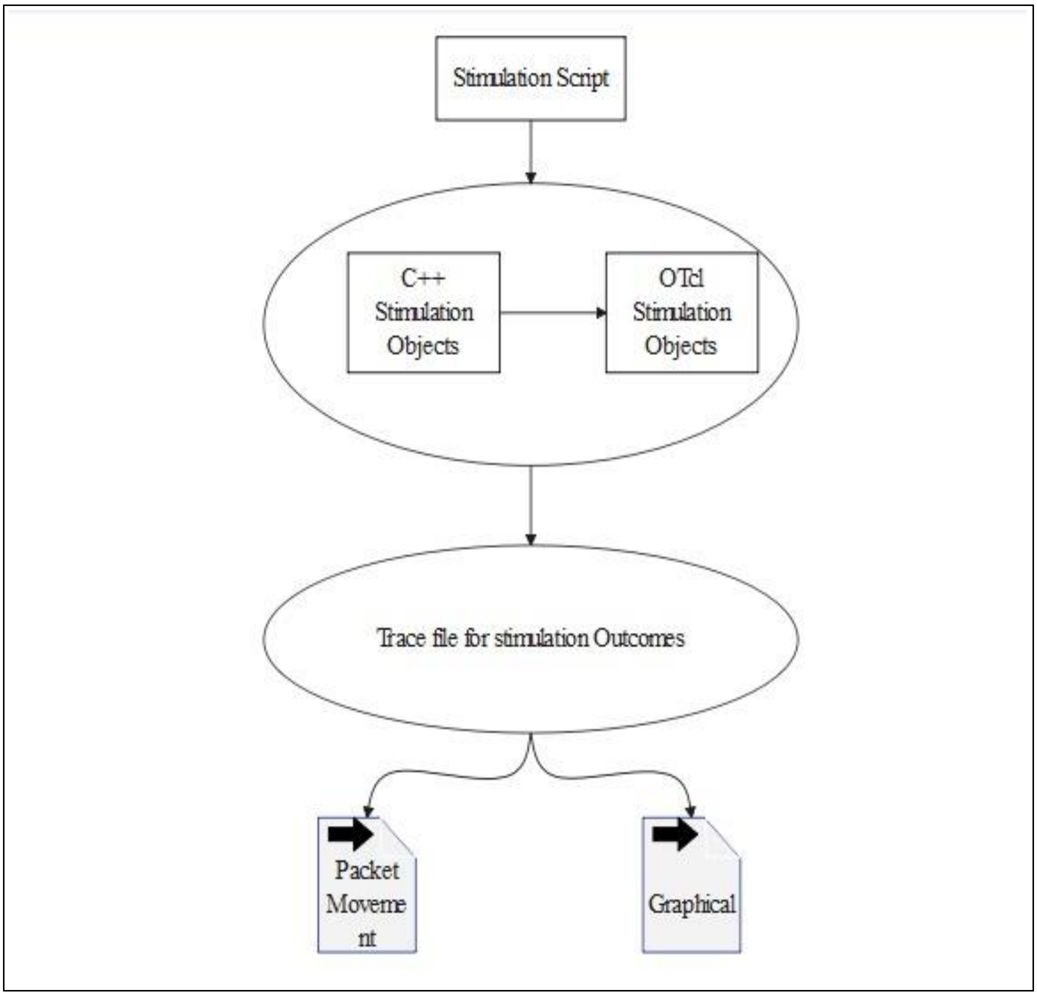
3.2 Data Flow Diagram



3.1 DFD Level 0 for WSN

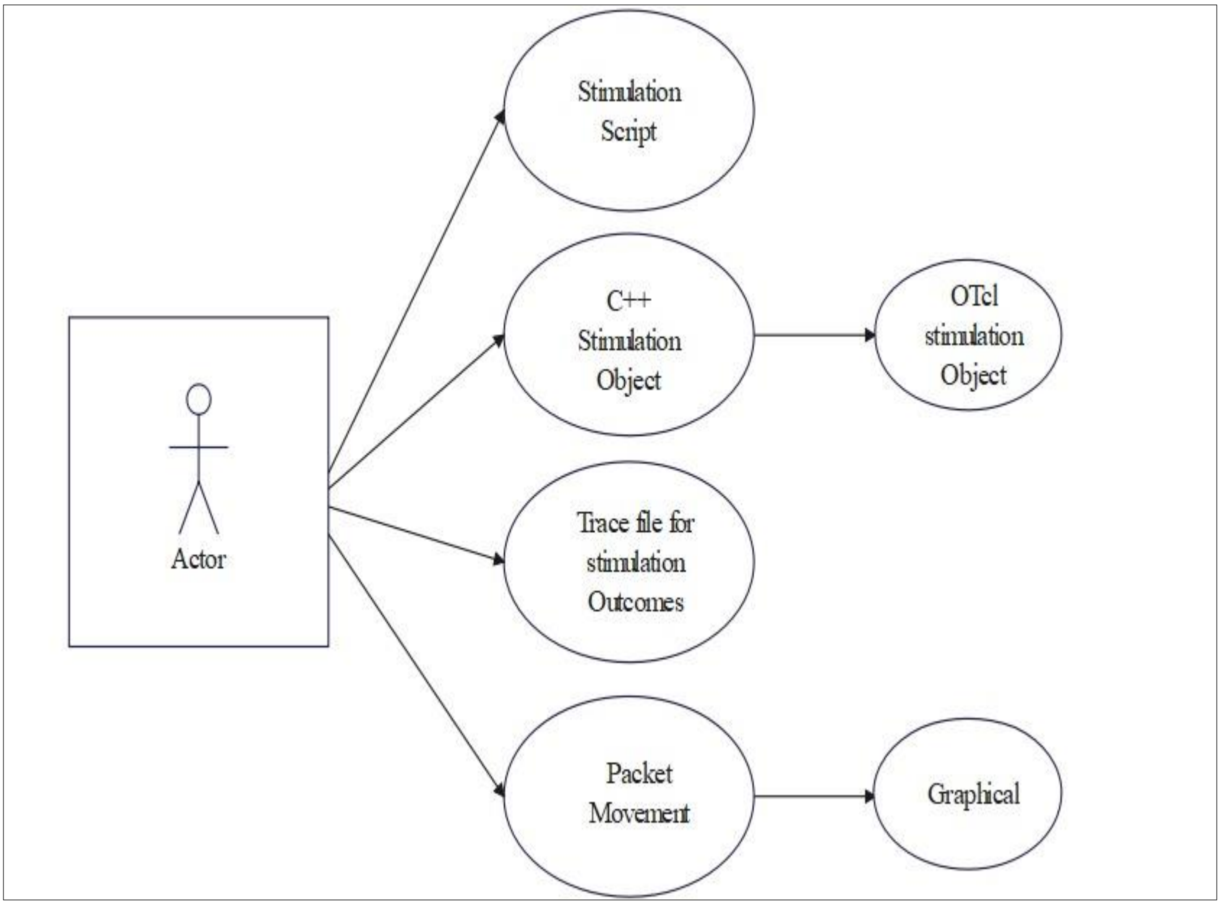


3.2 DFD Level 0 for NS2



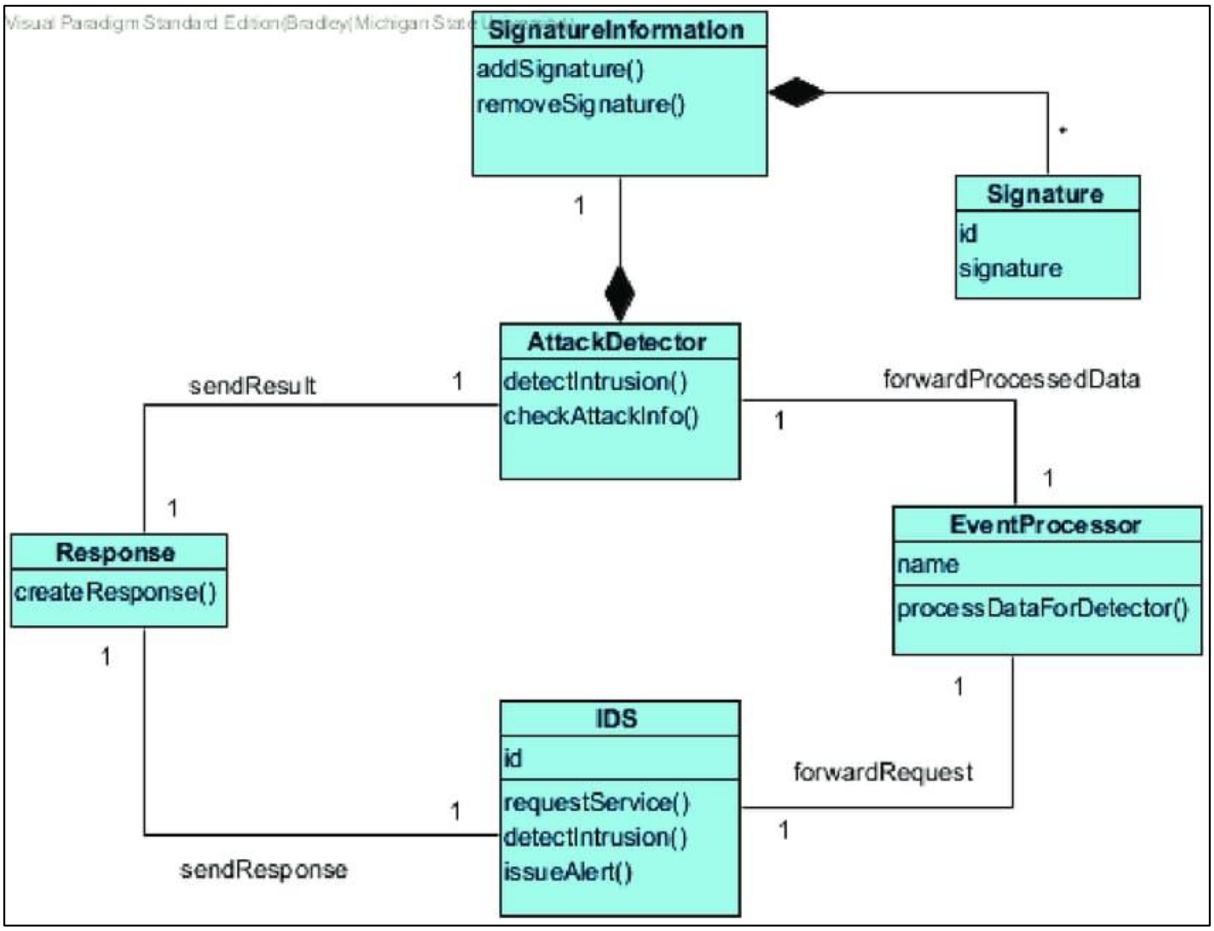
3.3 DFD Level 1 for NS2

3.3 Use Case Diagram



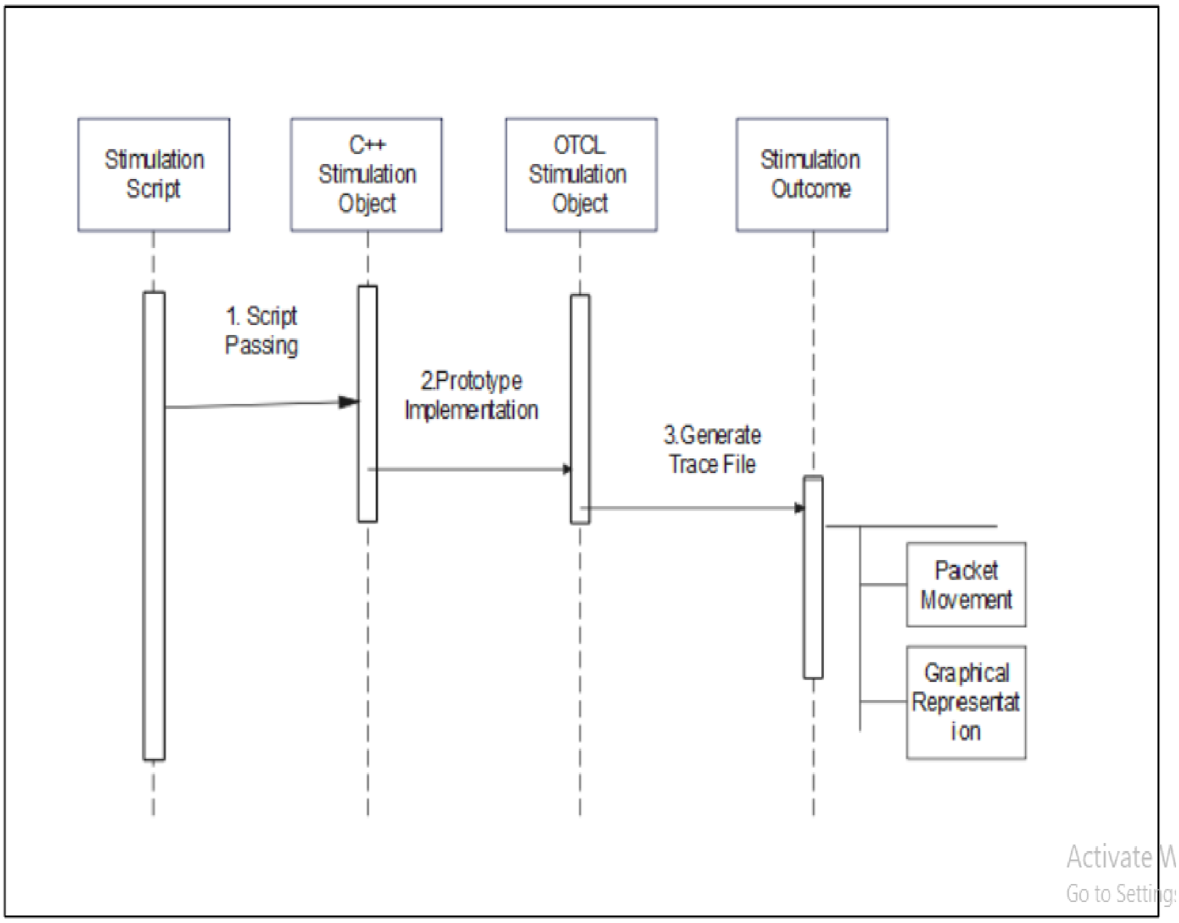
3.4 Use Case Diagram for NS2

3.4 Class Diagram



3.5 Class Diagram for NS2

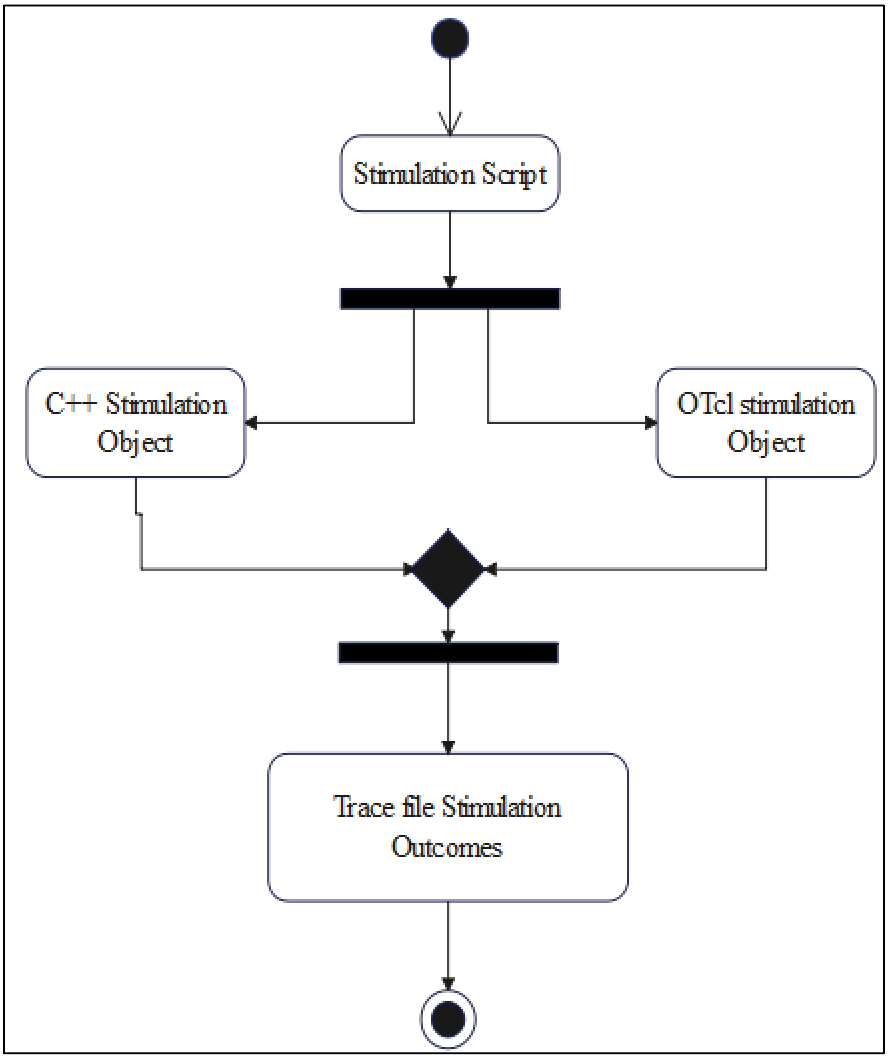
3.5 Sequence Diagram



Activate W
Go to Setting

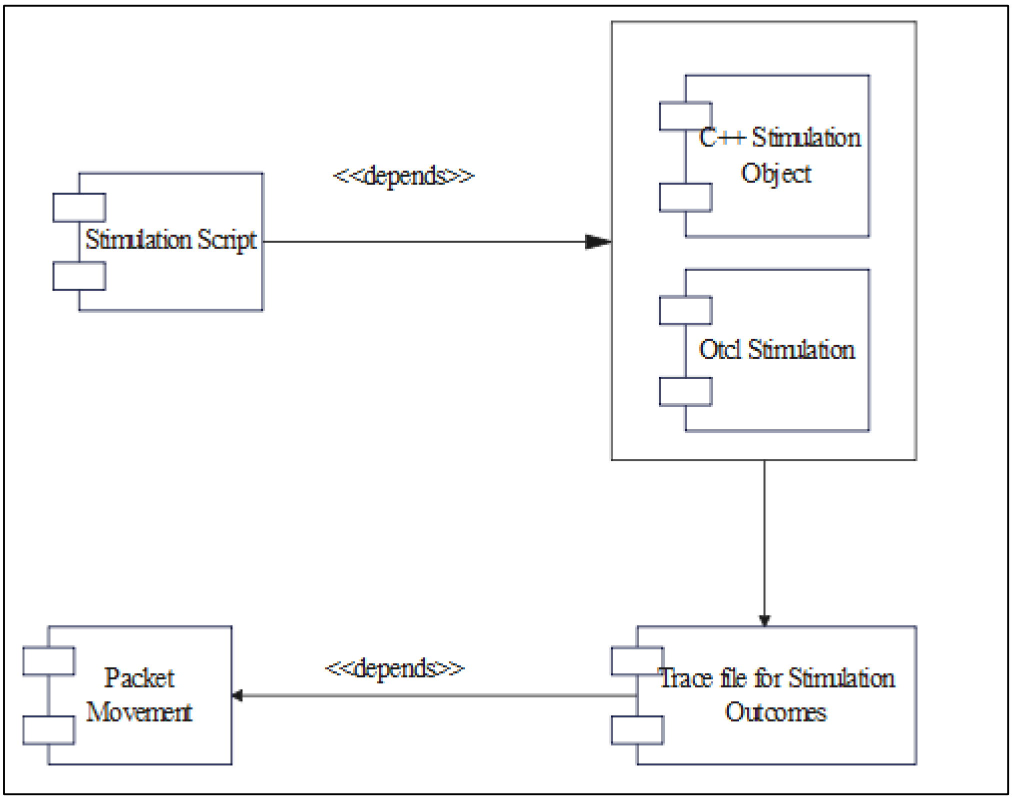
3.6 Sequence Diagram for NS2

3.6 Activity Diagram



3.7 Activity Diagram for NS2

3.7 Component Diagram

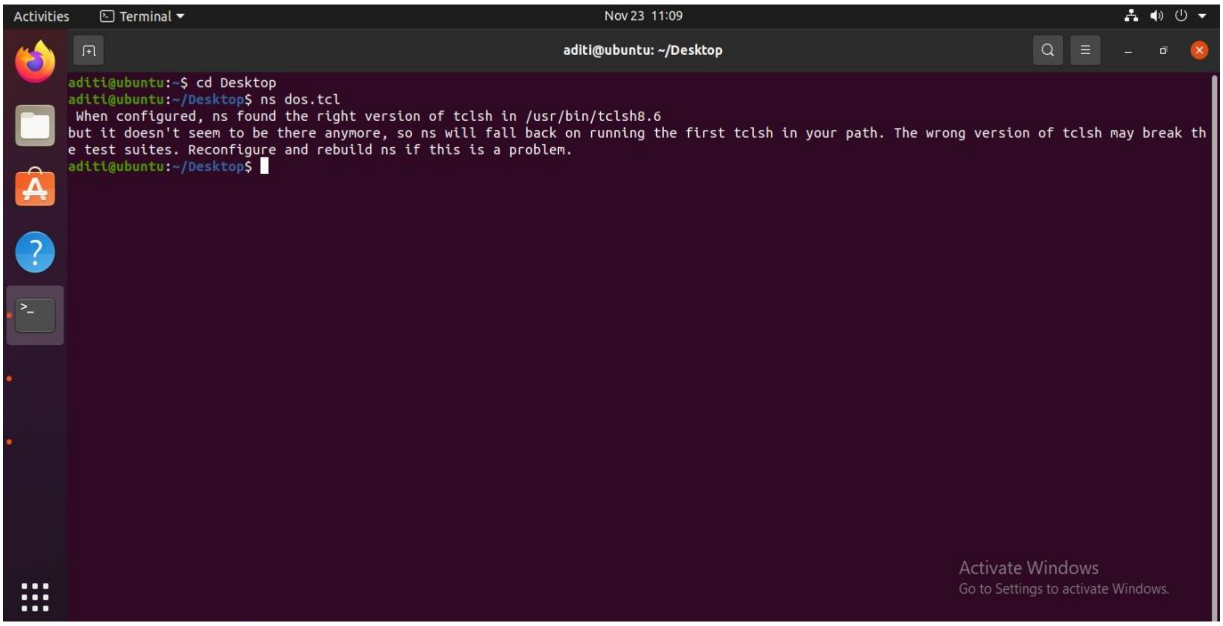


3.8 Component Diagram for NS2

4. Performance Evaluation

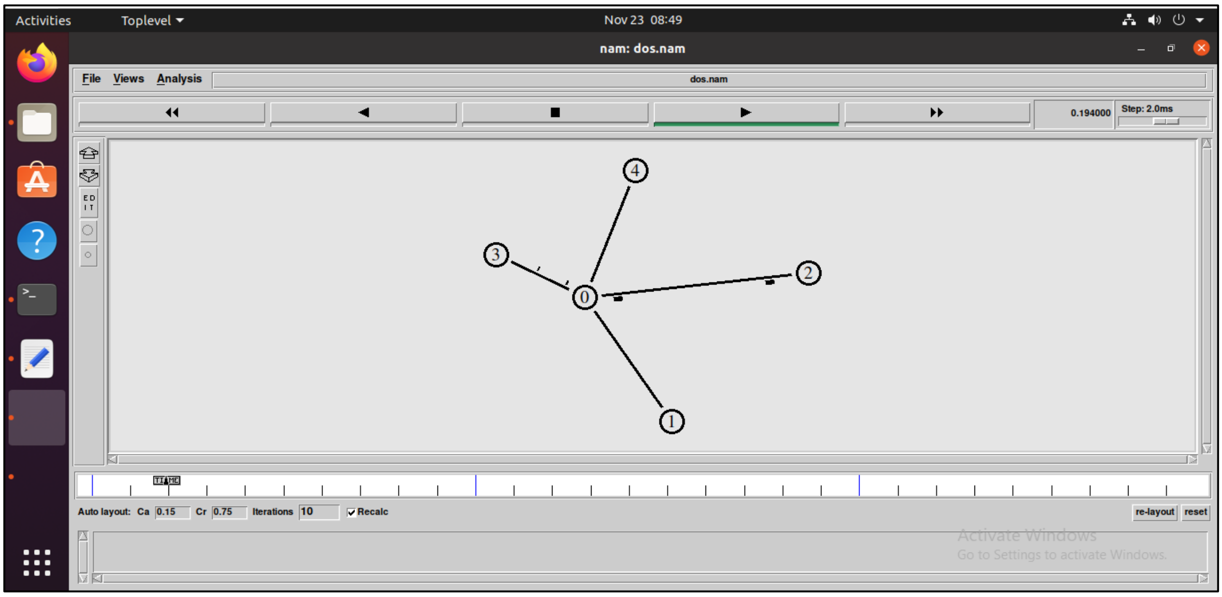
Attack No 01 Denial of Services

Simulating a Denial-of-Service (DoS) attack in NS2 involves creating a scenario where an attacker floods the network with traffic to overwhelm and disrupt the normal functioning of the network.

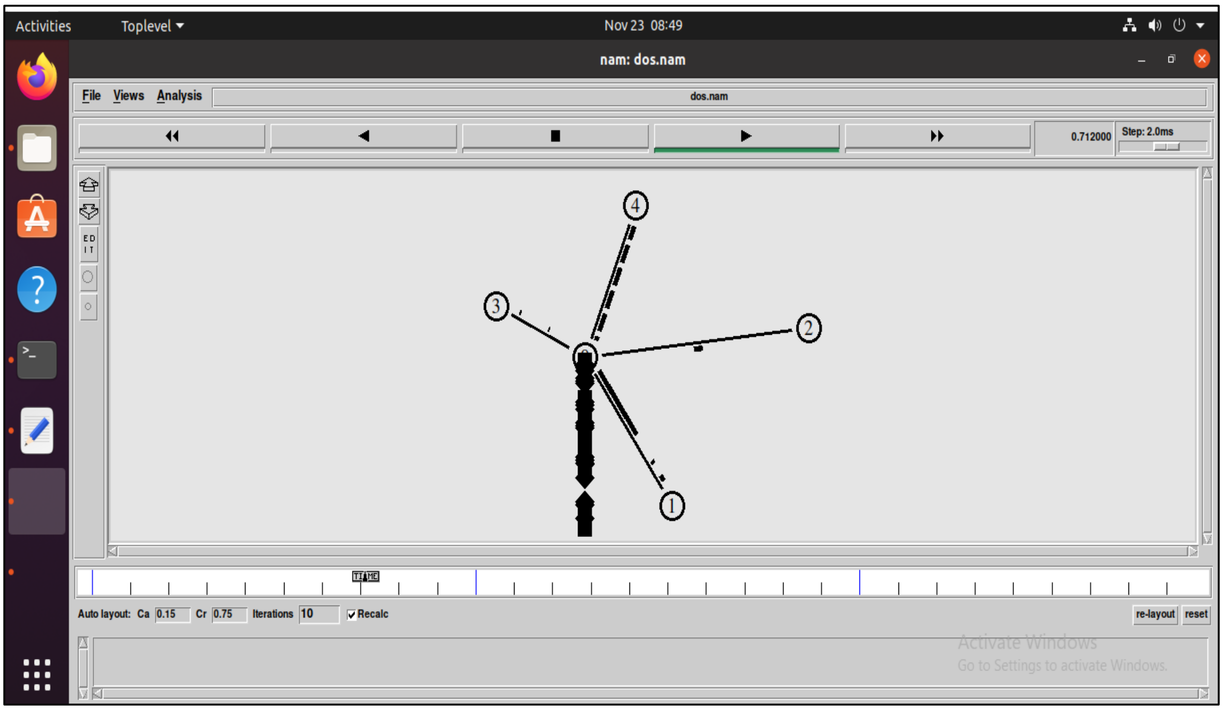


```
aditi@ubuntu:~$ cd Desktop
aditi@ubuntu:~/Desktop$ ns dos.tcl
 When configured, ns found the right version of tclsh in /usr/bin/tclsh8.6
but it doesn't seem to be there anymore, so ns will fall back on running the first tclsh in your path. The wrong version of tclsh may break th
e test suites. Reconfigure and rebuild ns if this is a problem.
aditi@ubuntu:~/Desktop$ 
```

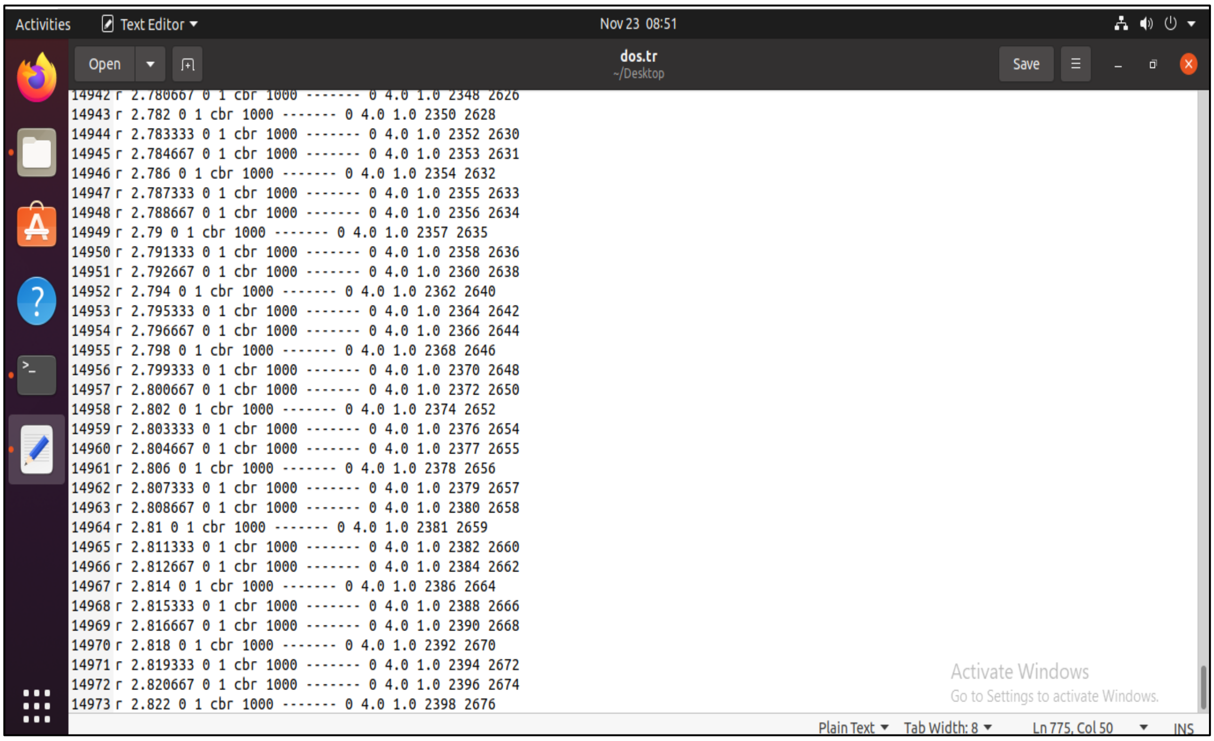
4.1 DOS Attack Terminal



4.2 Simulation of DoS 1



4.3 Simulation of DoS 2

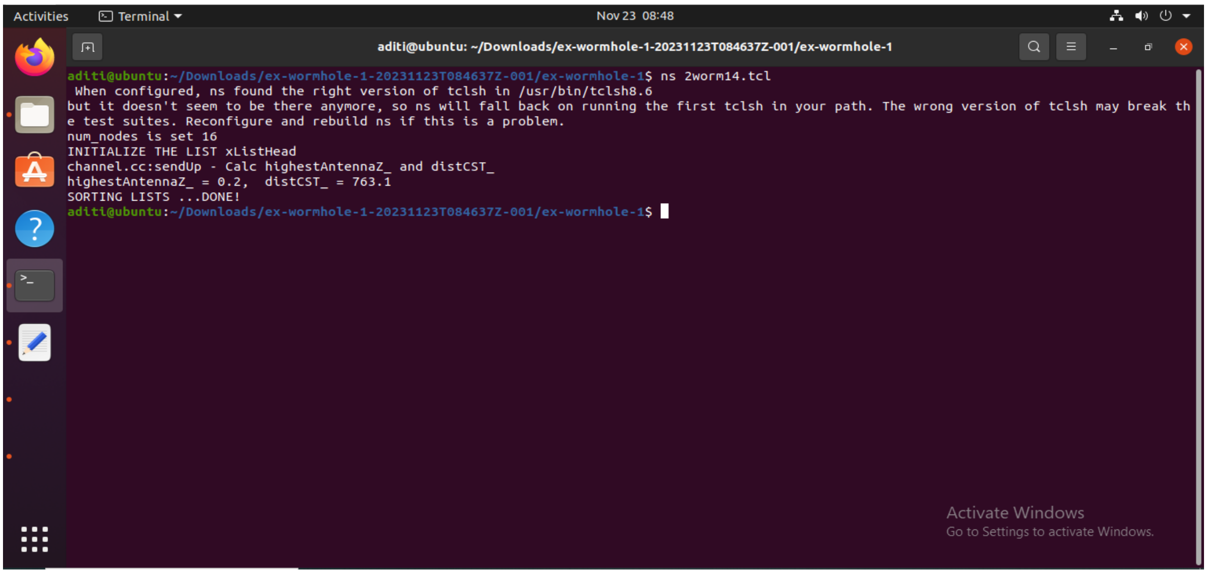


```
r 2.780667 0 1 cbr 1000 ------- 0 4.0 1.0 2348 2626
r 2.782 0 1 cbr 1000 ------- 0 4.0 1.0 2350 2628
r 2.783333 0 1 cbr 1000 ------- 0 4.0 1.0 2352 2630
r 2.784667 0 1 cbr 1000 ------- 0 4.0 1.0 2353 2631
r 2.786 0 1 cbr 1000 ------- 0 4.0 1.0 2354 2632
r 2.787333 0 1 cbr 1000 ------- 0 4.0 1.0 2355 2633
r 2.788667 0 1 cbr 1000 ------- 0 4.0 1.0 2356 2634
r 2.79 0 1 cbr 1000 ------- 0 4.0 1.0 2357 2635
r 2.791333 0 1 cbr 1000 ------- 0 4.0 1.0 2358 2636
r 2.792667 0 1 cbr 1000 ------- 0 4.0 1.0 2360 2638
r 2.794 0 1 cbr 1000 ------- 0 4.0 1.0 2362 2640
r 2.795333 0 1 cbr 1000 ------- 0 4.0 1.0 2364 2642
r 2.796667 0 1 cbr 1000 ------- 0 4.0 1.0 2366 2644
r 2.798 0 1 cbr 1000 ------- 0 4.0 1.0 2368 2646
r 2.799333 0 1 cbr 1000 ------- 0 4.0 1.0 2370 2648
r 2.800667 0 1 cbr 1000 ------- 0 4.0 1.0 2372 2650
r 2.802 0 1 cbr 1000 ------- 0 4.0 1.0 2374 2652
r 2.803333 0 1 cbr 1000 ------- 0 4.0 1.0 2376 2654
r 2.804667 0 1 cbr 1000 ------- 0 4.0 1.0 2377 2655
r 2.806 0 1 cbr 1000 ------- 0 4.0 1.0 2378 2656
r 2.807333 0 1 cbr 1000 ------- 0 4.0 1.0 2379 2657
r 2.808667 0 1 cbr 1000 ------- 0 4.0 1.0 2380 2658
r 2.81 0 1 cbr 1000 ------- 0 4.0 1.0 2381 2659
r 2.811333 0 1 cbr 1000 ------- 0 4.0 1.0 2382 2660
r 2.812667 0 1 cbr 1000 ------- 0 4.0 1.0 2384 2662
r 2.814 0 1 cbr 1000 ------- 0 4.0 1.0 2386 2664
r 2.815333 0 1 cbr 1000 ------- 0 4.0 1.0 2388 2666
r 2.816667 0 1 cbr 1000 ------- 0 4.0 1.0 2390 2668
r 2.818 0 1 cbr 1000 ------- 0 4.0 1.0 2392 2670
r 2.819333 0 1 cbr 1000 ------- 0 4.0 1.0 2394 2672
r 2.820667 0 1 cbr 1000 ------- 0 4.0 1.0 2396 2674
r 2.822 0 1 cbr 1000 ------- 0 4.0 1.0 2398 2676
```

4.4 Packets Drop of DoS

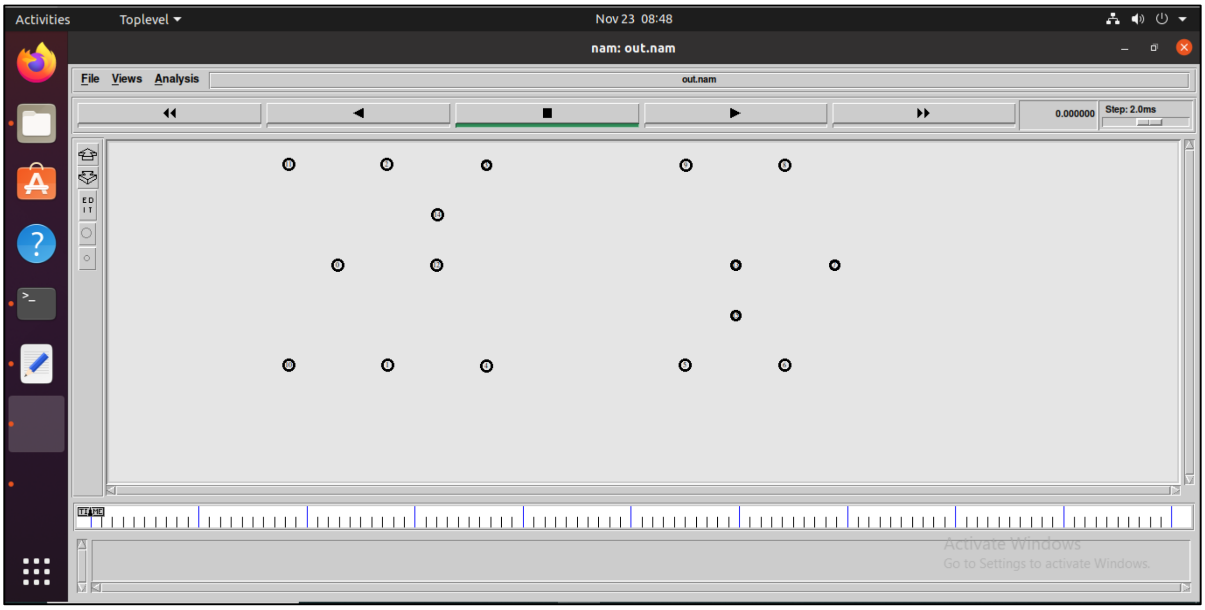
Attack No 02 Wormhole Attack

A wormhole attack is a type of security threat in wireless ad hoc networks where an attacker tunnels packets from one location in the network to another, creating a shortcut that allows the attacker to potentially gain unauthorized access to information. In the context of network simulation using NS2 (Network Simulator 2), simulating a wormhole attack involves setting up a scenario where malicious nodes create a tunnel to facilitate the unauthorized transfer of data.

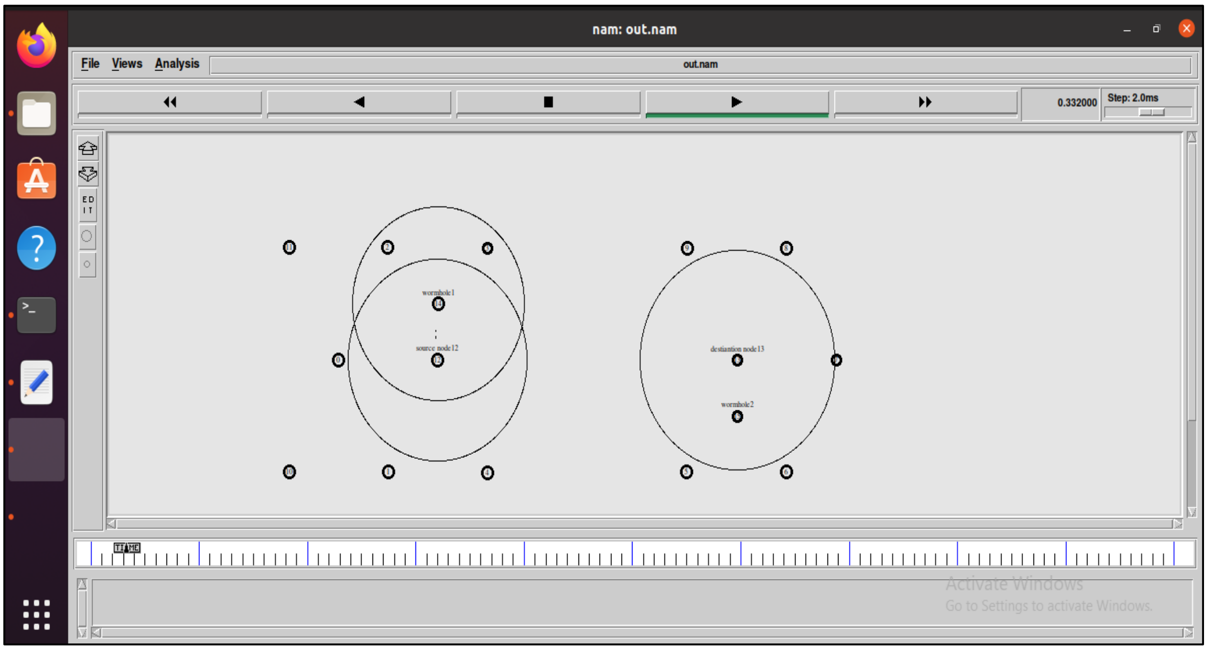

Activities
Terminal
Nov 23 08:48
aditi@ubuntu: ~/Downloads/ex-wormhole-1-20231123T084637Z-001/ex-wormhole-1
Activate Windows
Go to Settings to activate Windows.

```
aditi@ubuntu:~/Downloads/ex-wormhole-1-20231123T084637Z-001/ex-wormhole-1$ ns 2worm14.tcl
 When configured, ns found the right version of tclsh in /usr/bin/tclsh8.6
but it doesn't seem to be there anymore, so ns will fall back on running the first tclsh in your path. The wrong version of tclsh may break th
e test suites. Reconfigure and rebuild ns if this is a problem.
num_nodes is set 16
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 0.2,  distCST_ = 763.1
SORTING LISTS ...DONE!
aditi@ubuntu:~/Downloads/ex-wormhole-1-20231123T084637Z-001/ex-wormhole-1$ 
```

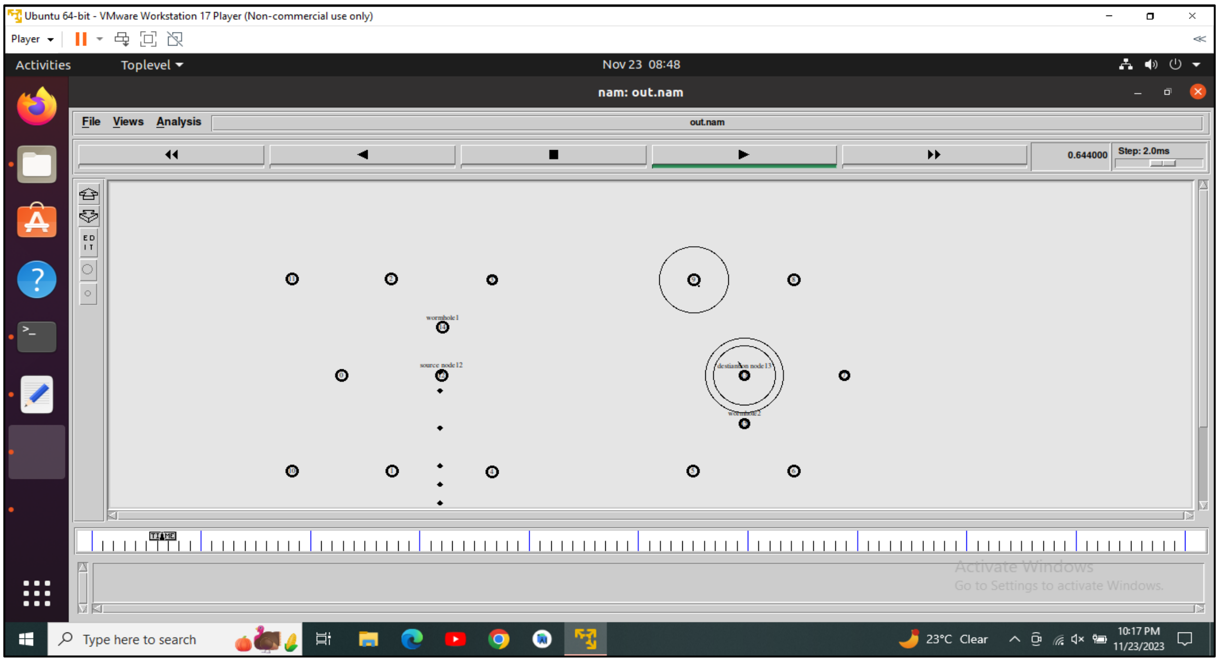
4.5 Wormhole Terminal



4.6 Wormhole Simulation 1



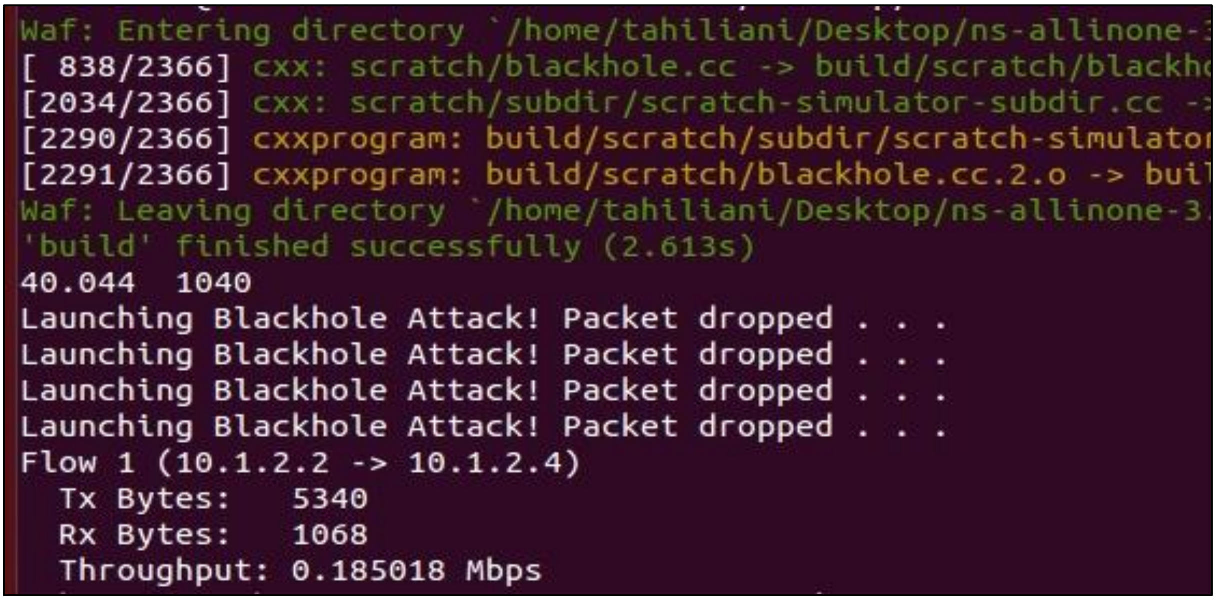
4.7 Wormhole Simulation 2



4.8 Wormhole Simulation 3

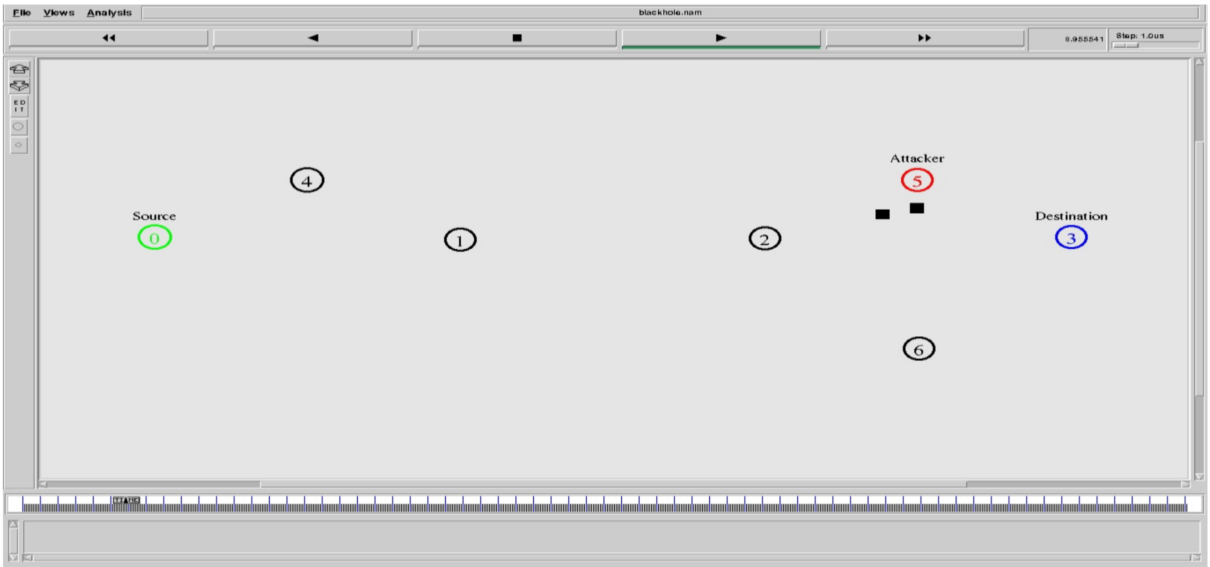
Attack No 03 Blackhole Attack

A blackhole attack is a type of security threat in wireless ad hoc networks where a malicious node attracts and absorbs data packets, without forwarding them to their intended destination. In the context of network simulation using NS2 (Network Simulator 2), simulating a blackhole attack involves creating a scenario where a node selectively drops or absorbs packets, leading to a degradation in network performance.

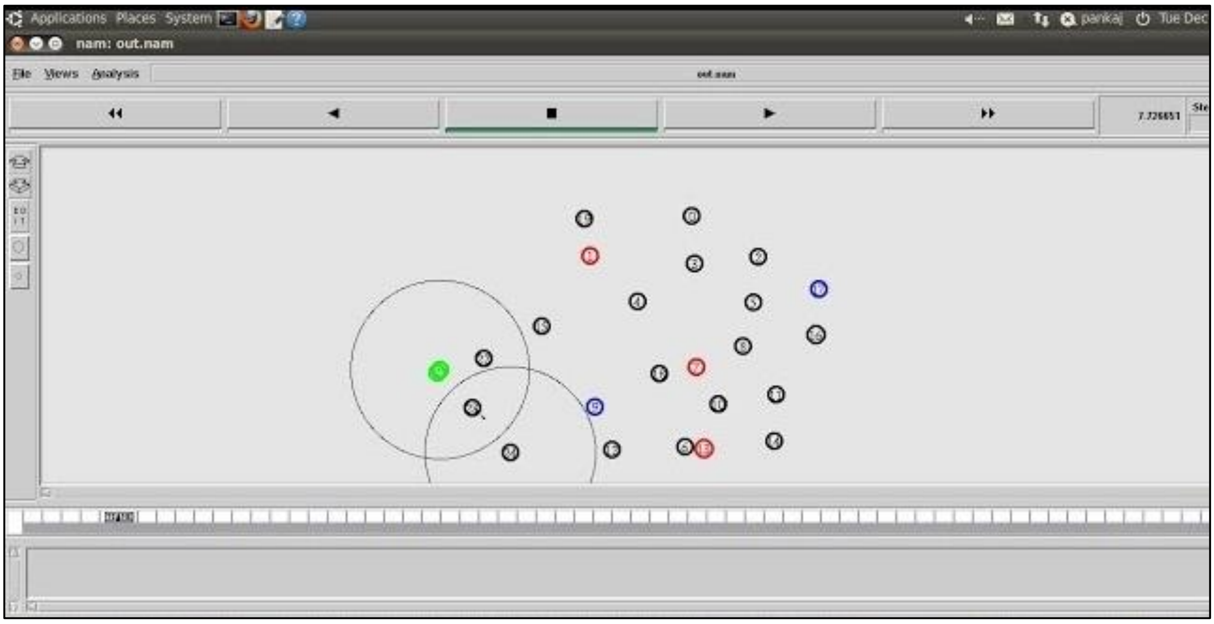


```
Waf: Entering directory `/home/tahiliani/Desktop/ns-allinone-3
[ 838/2366] cxx: scratch/blackhole.cc -> build/scratch/blackho
[2034/2366] cxx: scratch/subdir/scratch-simulator-subdir.cc ->
[2290/2366] cxxprogram: build/scratch/subdir/scratch-simulator
[2291/2366] cxxprogram: build/scratch/blackhole.cc.2.o -> buil
Waf: Leaving directory `/home/tahiliani/Desktop/ns-allinone-3.
'build' finished successfully (2.613s)
40.044  1040
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Flow 1 (10.1.2.2 -> 10.1.2.4)
  Tx Bytes:   5340
  Rx Bytes:   1068
  Throughput: 0.185018 Mbps
```

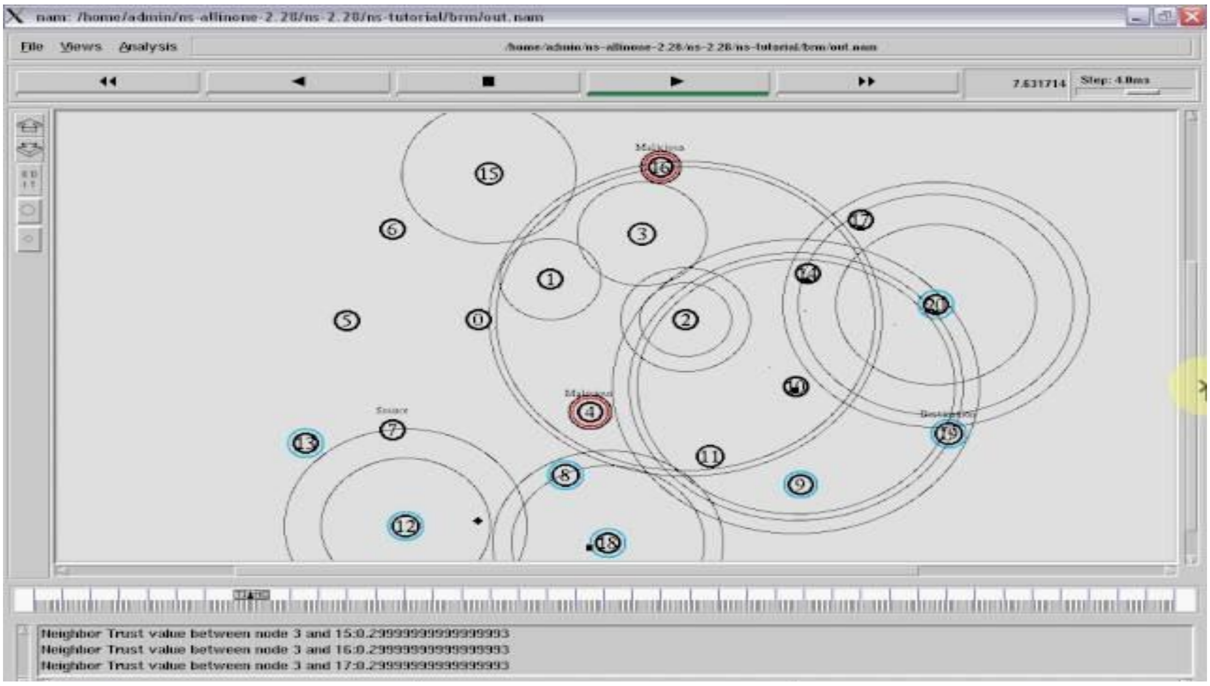
4.9 Blackhole Terminal



4.10 Blackhole Simulation 1



4.11 Blackhole Simulation 2

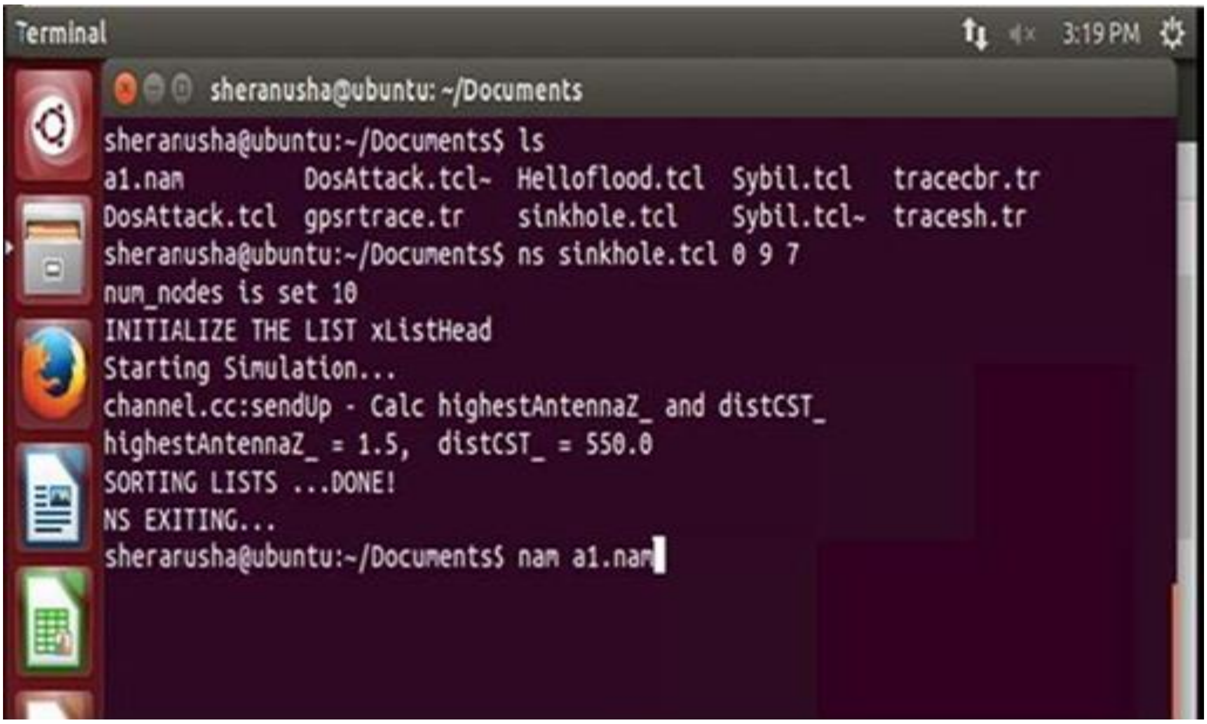

nam: /home/admin/ns-allinone-2.28/ns-2.28/ns-tutorial/brm/out.nam
File Views Analysis
/home/admin/ns-allinone-2.28/ns-2.28/ns-tutorial/brm/out.nam
7.631714
Step: 4.8ms
Malicious
Malicious
Source
Destination
15
6
16
3
17
1
14
20
5
0
2
10
4
7
13
19
11
8
9
12
18

```
Neighbor Trust value between node 3 and 15:0.29999999999999993
Neighbor Trust value between node 3 and 16:0.29999999999999993
Neighbor Trust value between node 3 and 17:0.29999999999999993
```

4.12 Blackhole Simulation 3

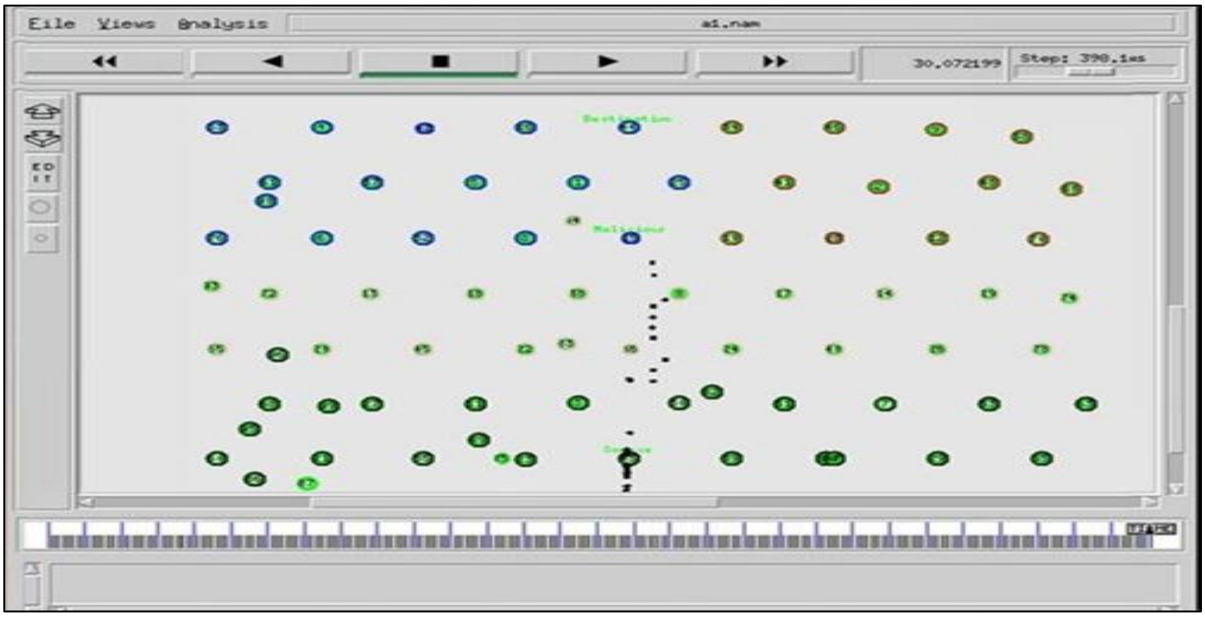
Attack No 04 Sybil Attack

A Sybil attack is a type of security threat in which a single adversary controls multiple nodes in a network, pretending to be independent entities. This attack can compromise the integrity and reliability of network protocols and services.

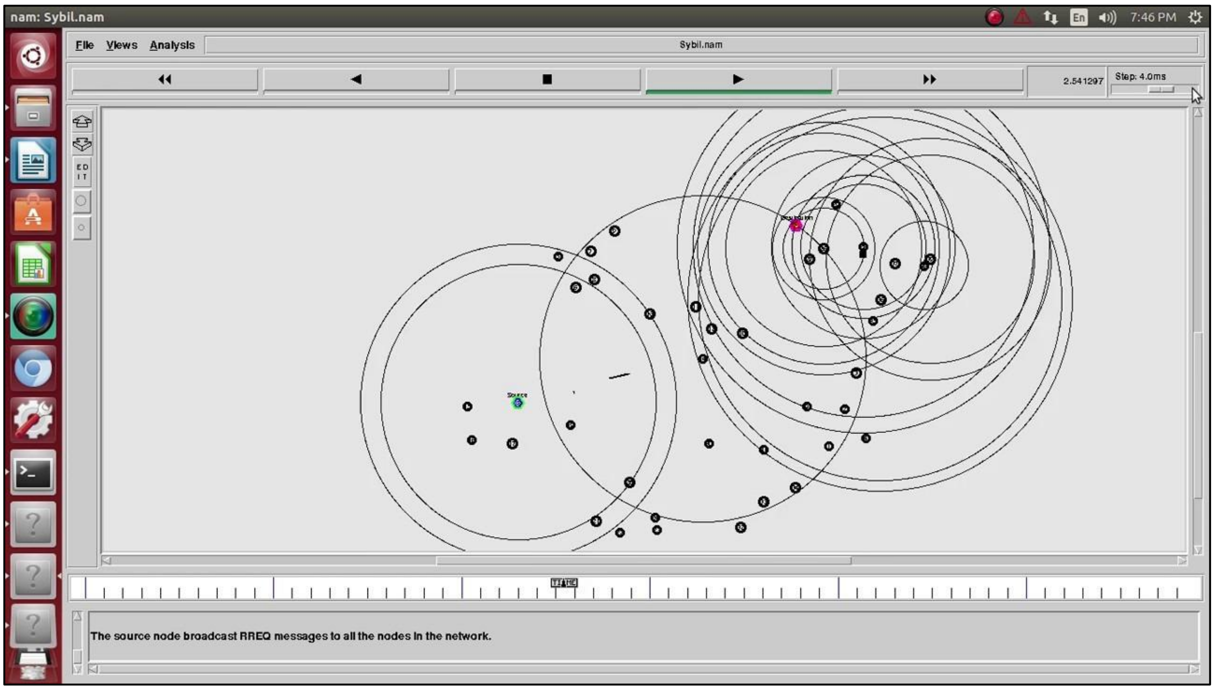


```
sheranusha@ubuntu:~/Documents$ ls
a1.nam         DosAttack.tcl~  Helloflood.tcl  Sybil.tcl   tracecbr.tr
DosAttack.tcl  gpsrtrace.tr    sinkhole.tcl    Sybil.tcl~  tracesh.tr
sheranusha@ubuntu:~/Documents$ ns sinkhole.tcl 0 9 7
num_nodes is set 10
INITIALIZE THE LIST xListHead
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
NS EXITING...
sherarusha@ubuntu:~/Documents$ nam a1.nam
```

4.13 Sybil Terminal



4.14 Sybil Simulation 1



The source node broadcast RREQ messages to all the nodes in the network.

4.15 Sybil Simulation 2

5. Conclusion

WSN’s are of huge demand. The request for wireless sensor networks are increasing rapidly, because the growth of using WSN has increased. There are some limitations in a wireless sensor network like they have limited storage capacity, limited capability of processing and limited energy to transmit data. These drawbacks can make WSN different from other networks. There are some little concerns that occur in a WSN. Based on the above mentioned difficulties in the data integrity, security, there are many solutions that are available to overcome these dangers. The attacks that are popular in a WSN like hello flood attack, sinkhole attack, Sybil attack and denial of service attack have been simulated in a simulator. On simulation, the performance and the efficiency of the network can be analyzed. The behavior and the energy parameters can be examined. A mechanism for ensuring secure data transfer and preventing the attacks in a WSN must be proposed. The parameters which determine the network performance can be calculated from the simulation. Because of the numerous attacks happening in the WSN, there is less amount of security.