Implementation of Wired and Wireless Networks, Analysis Simulation and Result Comparison using NS2

Rahul Mishra
CSE, M. Tech. Final Year Student, Sobhasaria Engineering College, Sikar – 332001, Rajasthan, India

ABSTRACT
In this the author presents how to use simulation for implementation, designing and studying wired and wireless networks. In order to achieve the defined task, analyze literature sources related to wired and wireless communication networks. Briefly describe the basic wired and wireless networks categories. Analyze the Network simulator ns-2 and give its detailed description. Present a brief comparison of ns-2 simulator with other open source network simulators. Specify the configuration for the simple wired and wireless network with two nodes first and then with many nodes and create corresponding model by using ns-2 simulator. Demonstrate selected characteristics of the specified network configuration using the simulation model. For proposed work we will add something that can easily simulate the geographical areas and hence results in fast transmission and a secure environment.

Keywords: Network, NS2, Wired and Wireless, Protocols.

INTRODUCTION
Communication refers to exchange of information between two entities. Communication networks in general divide into two main categories:
Wired networks exist between a number of devices connected to each other using connecting media, such as cables and routers. Wired networks can be applied within an area limited by the cables and routers that allow for sending and receiving of data. Wireless networks, on the other hand, are free of such space limitations and are more easily able to connect different devices to each other. Wireless nodes can play the roles of both hosts and routers, which forward the packets to neighboring nodes. In recent days, wireless networks are mostly used than wired networks. The reasons for using wireless networks are cost effectiveness of network deployment and its applicability to environments where wiring is not possible or it is preferable solution compared with wired networks. When designing wireless networks and/or studying their behaviour under various conditions, software simulation tools are often used.
Whether it is a wired or wireless network, it should have a network topology. A communication network topology refers to the schematic representation of switching elements, routers, transmission links and other peripherals. It acts as a layout for communication network which exists in real time scenario. Network topologies can be classified into two types based on the layouts:
1. Physical network layout
2. Logical network layout
Physical network layout is the actual layout of computer cables, routers and other network devices. Logical network layout is the way in which network appears to the devices in use. Commonly used topologies are bus, ring and star. The analysis of a sophisticated network becomes difficult as there is a hectic calculation involved at each and every node spaced at a 100-200 km interval.
There are four basic types of transmissions standards for wireless networking. These types are produced by the Institute of Electrical and Electronic Engineers (IEEE). These standards define all aspects of radio frequency wireless networking. They have established four transmission standards; 802.11, 802.11a, 802.11b, 802.11g.
The basic differences between these four types are connection speed and radio frequency. 802.11 and 802.11b are the slowest at 1 or 2 Mbps and 5.5 and 11Mbps respectively. They both operate off of the 2.4 GHz radio frequency. 802.11a operates off of a 5 GHz frequency and can transmit up to 54 Mbps and the 802.11g operates off of the 2.4 GHz frequency and can transmit up to 54 Mbps. Actual transmission speeds vary depending on such factors as the number and size of the physical barriers within the network and any interference in the radio transmissions.
Wireless networks are reliable, but when interfered with it can reduce the range and the quality of the signal. Interference can be caused by other devices...
operating on the same radio frequency and it is very hard to control the addition of new devices on the same frequency. Usually if your wireless range is compromised onseed, more than likely, interference is to blame.

There are many benefits to a wireless network. The most important one is the option to expand your current wired network to other areas of your organization where it would otherwise not be cost effective or practical to do so. An organization can also install a wireless network without physically disrupting the current workplace or wired network. Wireless networks are far easier to move than a wired network and adding users to an existing wireless network is easy. Organizations opt for a wireless network in conference rooms, lobbies and offices where adding to the existing wired network may be too expensive to do so.

**Need For Simulation**

The cost of building test-bed or actual systems for performance analysis is sometimes not effective or even not feasible. The intensity of the problem increases, as more and more real world applications deploying mobile agents are proposed and each need different configuration parameters for performance studies. For these reasons, it is necessary to build a simulation model of the existing network topology and study it as a surrogate for an actual system.

Considering the above facts, a proper simulation tool should be selected in order to simulate the network model. The following are some of the factors:

1. Stress Test of the Network
2. Balance Power and Ease of Use
3. Confirm That Devices Are Connected Correctly
4. Provide Statistically Useful Data

**Network Simulator2 (NS2)**

NS2 is an object-oriented, discrete event-driven network simulator developed at University of California Berkeley written in C++ and OTcl. NS2 is very useful for developing and investigating variety of protocols. They mainly include protocols regarding TCP behavior, router queuing policies, multicasting, multimedia, wireless networking and application-level protocols.

NS software promotes extensions by users. It provides a rich infrastructure for developing new protocols. Also, instead of using a single programming language that defines a monolithic simulation, NS uses the split-programming model in which the implementation of the model is distributed between two languages. The goal is to provide adequate flexibility without losing performance. In particular, tasks such as low-level event processing or packet forwarding through simulated router require high performance and are not modified frequently once put into place.

**C++ - OTcl Linkage**

NS supports a compiled class hierarchy in C++ and also similar interpreted class hierarchy in OTcl. From the user’s perspective, there is a one-to-one correspondence between a class in the interpreted hierarchy and a class in the compiled hierarchy. The root of this class hierarchy is the class Tcl Object. Users create new simulator objects through the interpreter. These objects are instantiated within the interpreter and are closely mirrored by a corresponding object in the compiled hierarchy. The interpreted class hierarchy is automatically established through methods defined in class Tcl Class while user instantiated objects are mirrored through methods defined in class Tcl Object. Fig 1 C++ & OTcl linkage the following classes are mainly responsible for maintaining C++ and OTcl linkage.

i. Class Tcl
ii. Class Tcl Object
iii. Class Tcl Class
iv. Class Embedded Tcl
v. Class InstVar

**IMPLEMENTATION OF A SIXTEEN NODE WIRELESS NETWORK**

1. **Ad hoc On Demand Distance Vector Protocol (AODV):** The Ad-Hoc On-demand Distance Vector (AODV) routing protocol is one of several published routing protocols for mobile ad-hoc networking. Wireless ad-hoc routing protocols such as AODV are currently an area of much research among the networking community. Thus, tools for simulating these protocols are very important. Each AODV router is essentially a state machine that processes incoming requests from the network entity. When the network entity needs to send a message to another node, it calls upon AODV to determine the next-hop. Whenever an AODV router receives a request to send a message, it checks its routing table to see if a route exists. Each routing table entry consists of the following fields:

   i. Destination address
   ii. Next hop address
iii. Destination sequence number

iv. Hop count

If a route exists, the router simply forwards the message to the next hop. Otherwise, it saves the message in a queue, and then it initiates a route request to determine a route. Upon receipt of the routing information, it updates its routing table and sends the queued messages. AODV nodes use four types of messages to communicate among each other. Route Request (RREQ) and Route Reply (RREP) messages are used for route discovery. Route Error (RERR) messages and HELLO messages are used for route maintenance. The following sections describe route determination and route maintenance in greater detail.

1.1. AODV Route Discovery

When a node needs to determine a route to a destination node, it floods the network with a Route Request (RREQ) message. The originating node broadcasts a RREQ message to its neighboring nodes, which broadcast the message to their neighbors. To prevent cycles, each node remembers recently forwarded route requests in a route request buffer. As these requests spread through the network, intermediate nodes store reverse routes back to the originating node. Since an intermediate node could have many reverse routes, it always picks the route with the smallest hop count. When a node receiving the request either knows of a “fresh enough” route to the destination, or is itself the destination, the node generates a Route Reply (RREP) message, and sends this message along the reverse path back towards the originating node. As the RREP message passes through intermediate nodes, these nodes update their routing tables, so that in the future, messages can be routed through these nodes to the destination. It is possible for the RREQ originator to receive a RREP message from more than one node. In this case, the RREQ originator will update its routing table with the most “recent” routing information; that is, it uses the route with the greatest destination sequence number.

2. Dynamic Source Routing Protocol (DSR)

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse. This may result in high overhead for long paths or large addresses, like IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis.

This protocol is truly based on source routing whereby all the routing information is maintained (continually updated) at mobile nodes. It has only two major phases, which are Route Discovery and Route Maintenance. Route Reply would only be generated if the message has reached the intended destination node (route record which is initially contained in Route Request would be inserted into the Route Reply). To return the Route Reply, the destination node must have a route to the source node. If the route is in the Destination Node's route cache, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Request message header (this requires that all links are symmetric). In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The erroneous hop will be removed from the node's route cache; all routes containing the hop are truncated at that point. Again, the Route Discovery Phase is initiated to determine the most viable route. Dynamic source routing protocol (DSR) is an on-demand protocol.

3. Implementation of sixteen node network using AODV routing protocol

A sixteen node ad hoc wireless network is defined and the AODV routing protocol is chosen in order to route the data packets from the source node to destination. The following figure shows the output of NAM for sixteen node ad hoc.

Fig 1: Output of NAM showing wireless network with sixteen nodes
For the above defined network, a source node and a destination node is defined. The AODV routing protocol chooses the shortest route in order to transmit the data packets efficiently. Once the route is identified, the source node transmits the data packets to destination. In our network, we chose node 13 as source and node 5 as destination. The source and destination node can be changed as per requirement. The node 13 generates an RREQ message to its neighboring nodes.

The neighboring node with a smallest hop is determined and from the neighbor node the message will be transmitted to other nodes which have smallest hops from the current node. As these requests spread through the network, intermediate nodes store reverse routes back to the originating node. When the message reaches the destination node, the node generates a Route Reply (RREP) message, and sends this message along the reverse path back towards the originating node. As the RREP message passes through intermediate nodes, these nodes update their routing tables, so that in the future, messages can be routed through these nodes to the destination. For the wireless network, the performance is evaluated by calculating its parameters such as throughput. The following graphs show the throughput and average number of packets received.

CONCLUSION

Using NS2, real time networks such as implementation of high speed LAN in a closed geographical area such as an apartment, office complex can be easily simulated and current implementations such as A Secure Intrusion Detection System for MANETs used in military applications, Fast And Secure Data Transmission In MANET for civilian applications and Self-Reconfigurable Wireless Mesh Networks used mainly in civil applications can be simulated which comes as further extension to this paper work.

REFERENCES


vi. Maarten Burghout , “ Experimental Analysis of the impact of RTT differences on the Throughput of two competing TCP flows,” Individual Research Assignment , University Of Twente Netherlands, June 2008


xvii. Dr . Neeraj Bhargava , Dr . Ritu Bhargava , Anchal Kumawat and Bharat Kumar , “ Performance of TCP – Throughput on NS2 by using different Simulation Parameters , (IJACR) , Volume 2 , Number 4 , Issue 6 , December 2012