IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 12-15

Secure Mobile Communication

Ms. Aditi S. Pandey, Ms. Kamini S. Gajkeshwar, Ms. Juhi R.Singh,
Ms. Pratiksha D. Kamble, Ms. Pooja landage
[12345]*Computer Science & Engineering, TGPCET, Nagpur, India*

Abstract: *The tremendous advancement in the field of Communication and Information Technology over the last decade have influenced our lives greatly. Wireless communication has witnessed a growth number of users in the recent years. One of the main advantages of wireless technology is mobility, which allows mobile users to move from one network to another while maintaining their permanent IP address. This keeps transportation and high level connection while moving IP routing on the IP address, which uniquely identities a node's point of attachment to the internet.*

I. Introduction

The tremendous advancements in the field of communication and information technology over the last decades have influenced our lives greatly. Wireless communication has witnessed a growth number of users in the recent years; one of the main advantages of wireless technology is mobility, which allows mobile users to move from one network to another while maintaining their permanent IP address. This keeps transportation and high level connections while moving IP routing is Based on the IP address, which uniquely identities a node's point of attachment to the internet . In this project proposed a mechanism better security mechanism for Mobile communication. Secure communication between the MN and the HA when sending the messages 1(MN to the CN) and 3 (CoA to the CN).

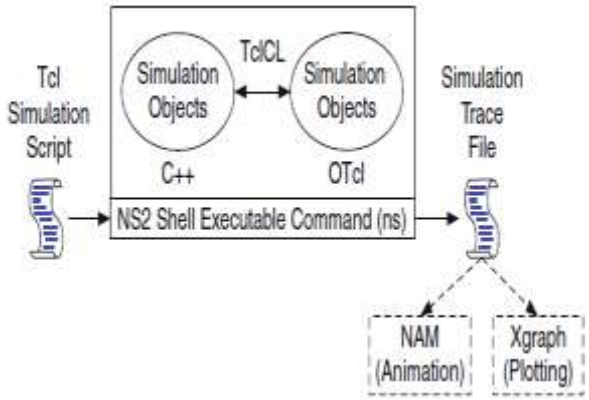
Objective

- Secure communication between the Mobile node (MN) and the Home Agent (HA).
- Calculate the mean Packet delay cost.
- Calculate mean signal cost.
- Calculate the throughput of network.
- To show the comparative analysis normal Packet delay cost, normal signal cost, normal throughput with proposed scheme

II. Proposed Work

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. Ever since, several revolutions and revisions have marked the growing maturity of the tool, thanks to substantial contributions from the players in the field. Among these are the University of California and Cornell University who developed the REAL network simulator, 1 the foundation which NS is based on. Since 1995 the Defense Advanced Research Projects Agency (DARPA) supported development of NS through the Virtual InterNetwork Testbed (VINT) project .2 currently the National Science Foundation (NSF) has joined the ride in development. Last but not the least, the group of researchers and developers in the community are constantly working to keep NS2 strong and versatile

System Architecture



NS2 provides users with executable command ns which take on input argument, the name of a Tcl simulation scripting file. Users are feeding the name of a Tcl simulation script (which sets up a simulation) as an input argument of an NS2 executable command ns. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e. a backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The C++ and the OTcl are linked together using TclCL. Mapped to a C++ object, variables in the OTcl domains are sometimes referred to as handles. Conceptually, a handle (e.g., n as a Node handle) is just a string (e.g., _o10) in the OTcl domain, and does not contain any functionality. Instead, the functionality (e.g., receiving a packet) is defined in the mapped C++ object (e.g., of class Connector). In the OTcl domain, a handle acts as a frontend which interacts withusers and other OTcl objects. It may defines its own procedures and variables to facilitate the interaction. Note that the member procedures and variables in the OTcl domain are called instance procedures (instprocs) and instance variables (instvars), respectively. Before proceeding further, the readers are encouraged to learn C++ and OTcl languages. For the detail of C++, while a brief tutorial of Tcl and OTcl tutorial are given in Appendices A.1 and A.2, respectively.NS2 provides a large number of built-in C++ objects. It is advisable to use these C++ objects to set up a simulation using a Tcl simulation script.

However, advance users may find these objects insufficient. They need to develop their own C++ objects, and use a OTcl configuration interface to put together these objects. After simulation, NS2 outputs either text-based or animation-based simulation results. To interpret these results graphically and interactively, tools such as NAM (Network Animator) and X-Graph are used. To analyze a particular behavior of the network, users can extract a relevant subset of text-based data and transform it to a more conceivable presentation.

System Flow Diagram

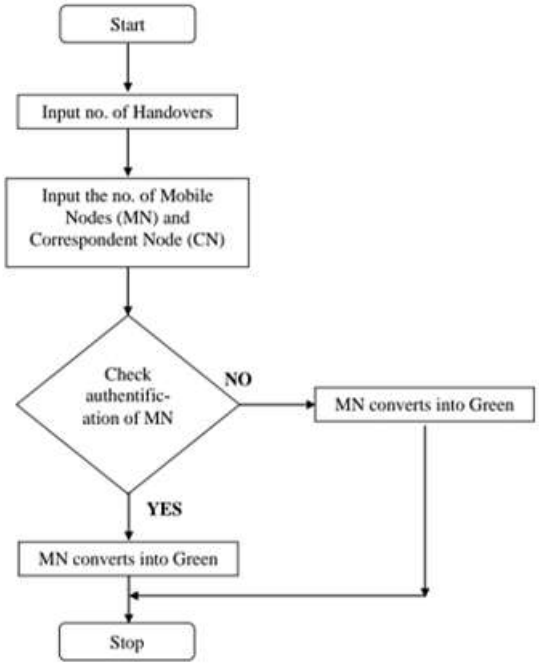


Fig 4.1 System Flow Diagram.

III. Result And Discussion

The session presents the screenshots of working system in order to demonstrate the complete process of the system.

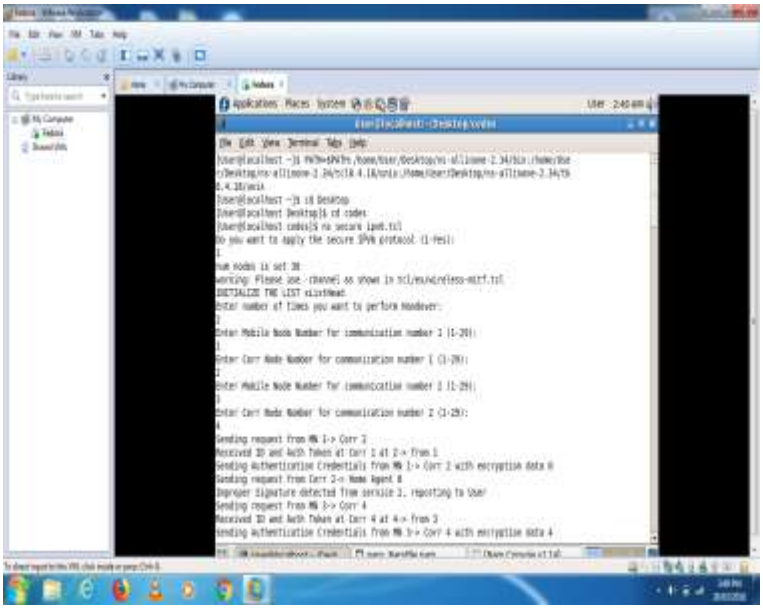


Fig 1. Using 2 Handovers

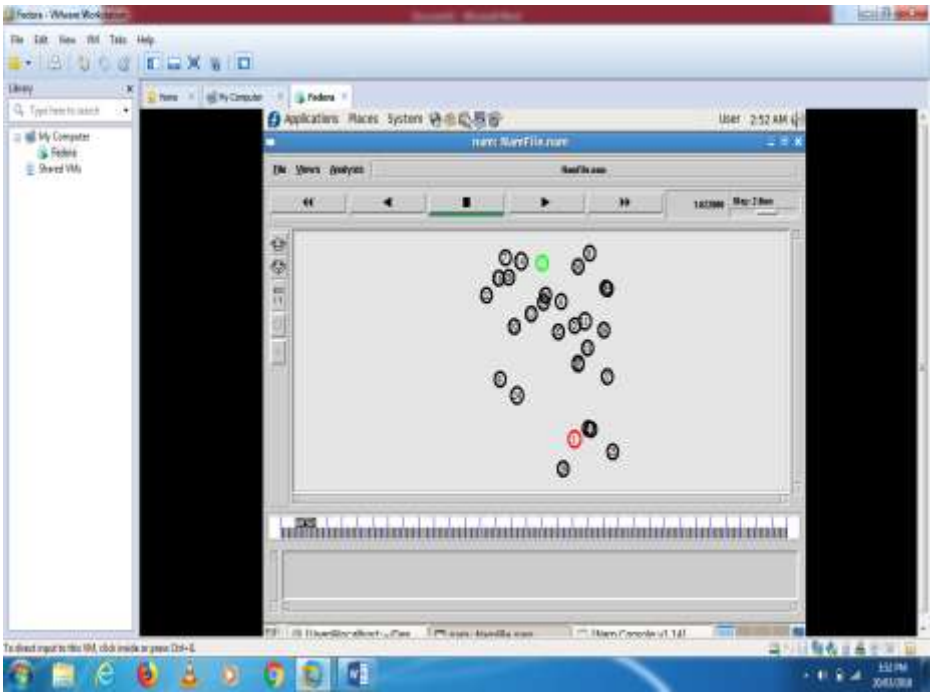


Fig 2. Output of 2 Handovers

IV. Conclusion:

In this project, we have discussed mobile communication and various threats associated with it. Mobile Communication specification is still ongoing and security issues are one of the primary consideration that need to be addresses. After studying the current security mechanism will proposed the security mechanism that can address he security threats and attacks for mobile communication, these streets prevent secure mobile communication based on nodes.

References

[1]. Xavier Perez-Costa, a Marc Torrent-Morenoab Hannes Hartensteina, "A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination", Mobile Computing and Communications Review, Volume 7, Number 4.

[2]. Zongpu Jia, Gaolei Wang1 and Ran Zhao, "A Literature Survey on Handoff for Mobile IPv6", JOURNAL OF NETWORKS, VOL. 6, NO. 8, AUGUST 2011.

[3]. Sonal V. Toshniwal, "Study of Mobile IPv6 ", International Journal of Science and Research (IJSR), Volume 5 Issue 10, October 2016.

[4]. Weimin Gao, Xiaoyong Fang, Lizhen Xiao, "STUDY THE HANDOFF MANAGEMENT OF MOBILE IPV6 NETWORK BASED ON MPLS", International Journal of Advanced Computer Technology (IJACT), VOLUME 2, NUMBER 6.

[5]. Johnny Lai1, Y. Ahmet Sekercioglu1, Norbert Jordan1, Andreas Pitsillides2, "Performance Evaluation of Mobile IPv6 Handover Extensions in an IEEE 802.11b Wireless Network Environment ".

[6]. Anne Wei, GouZhi Wei, and Benoit Geller, "Improving Mobile IPv6 Handover and Authentication in Wireless Network with E-HCF".

[7]. Tran Cong Hung, "Research Handover on Mobile IP", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), July Edition, 2012 Secure Mobile Communication.