ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Simulation of Current Security Scenario in Satellite Data Networks Using OMNET++

Narendra Kumar Dewangan[1], Narayan Sahu[2]

M.Tech Student, Department of Computer Science & Engineering, ITM University, Naya Raipur, C.G., India[1]

Assistant Professor, Department of Computer Engineering, ITM University, Naya Raipur, C.G., India[12]

ABSTRACT: Satellite play important role in the model life with fast data transmission and automation facilities. In simple life, we are using PDA, smartphones, laptops and many other gadgets and devices which required fast internet and data transmission facilities. In Administration scenario from Defence to primary education every field is on way of automation so we required fast and secure Internet there too. Security, relates with authentication, data integrity, confidentiality, availability and security risks in networks. Satellite is more or less work as mobile data transmitter and receiver with the moving facility and data availability at the orbital level with frequency change and time delay. This paper describes about the current security layers' present in the communication satellites networks and simulation implementation of those network using OMNET++.

KEYWORDS: Satellite Network, Security, delay, Mobile Networks, Authentication, Internet,and OMNET++.

I. INTRODUCTION

Satellite network is less or more like wireless networks, where the earth station is work like server as well as host and the geostationary station is like the communication channel to receive and send communication signal and data from one station to another. Receiver can be static and mobile both types. In today's world thinking of IoT (internet of Things) can be easily implemented by the use of low earth orbit(LEO) Satellites, many metro IT projects can be handled from far away and it can only be possible through the high-speed broadcast satellite data transmission units. Think that if satellite short models with basic data transmission facility and high data rate transmission are possible then we can connect remote areas with the internet and network broadcast technology. Provide E- services to the remote areas. By using simulation models, we can find the ability of data transmission of satellite and easily use the analysis data to implement real model of satellite. There are many network simulators are available but OMNET++ is more powerful and open source simulation model for any type of network.

In Current satellite networks the TCP/IP is depending upon the Bit Error Rate (BER), link Capacity Asymmetry (LCA) and Bandwidth Delay Product (BDP) which affect the transport layer on satellite communication networks. However, some called that TCP not work properly in the satellite network, so the new era of scientist and experts are suggested new network security protocols and mechanism to protect satellite TCP layer and make more efficient the communication in the satellite networks. Two candidate's protocols XCP and TCP-patch+ are selected as satellite specific transport protocol. For increase efficiency of satellite TCP protocols a new protocol is required to patch with the satellite TCP which make more efficient transport of internet data through the satellite networks. As we now the TCP patch+ is not compatible with the popular queue management scheme RED. So we have to search for the scheme which can make compatible connection and manage the network transmission of, internet in the satellite networks.

In satellite networks IP is works as the network layer for satellite networks, in this network border gateways performs address translation for IP networks. In case of Satellite Networks Terrestrial Gateways are act like border gateways. As we know that Border Gateway Protocol satellite version (BGP-S) already proposed [3]. Delay in satellite Network is much longer than a terrestrial network. A satellite network is designed for forward packets from one earth station to other or any type of receivers in the network. Native satellite carry the address of next terrestrial satellite unit.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

In this Paper we are describe about which types of security layers and protocols are adapted for the network security in the satellite networks and implement them using OMNET++. Section II describes the network layers security and transport layer security in the satellite network. Section III is about packet communication satellite network using protocol mentioned in the section II. Section IV is about OMNET++ implementation of above network and routing the packets and algorithms of implementation. Section V describes about the Result and outcomes of the above simulations and compare with real time network implementation. Final section VI Concluded the paper and rest section is references.

II. RELATED WORK

In previously used security mechanism to avoid the cyber-attacks in the satellite network we have following different techniques for different attacks.

A. Jamming attack is made on the physical link and frequency to jam the network and make delay in services provided by the satellites. Latest technique to prevent the jamming attack is lower the transmission power when the jamming attack is detected. When the detected jamming node is insider node than the node should be excluded from the network. In case of the satellite communication, jamming attack can be prevented by using spread spectrum, directional antenna and signal processing techniques.

B. Creating a regular access point can resist the attacker to listen the network between legitimate users and server. In steps to authenticate a regular AP and prevent an connected unauthenticated AP the network administrator can identify the APs and mark them personally. But in case of satellite network communication it is not possible due to wide area and globalization.

C. A well-organized firewall is also a good preventer of DDoS attack, It resist the duplicate packets coming from the same user. If the attacker has the dynamic MAC and IP address, then the network uses another method of preventing DDoS attack.

III. SECURITY FEATURES IN SATELLITE NETWORK LAYER AND TRANSPORT LAYER

As we know that router at terrestrial unit as works as the normal router and have address of the next Geo Stationary system. Native routers redirect the packets in the next hope and next hope have address of the destination. Good satellite network with compare to a wireless network have the property like low propagation delay and negligible multipath fading. Satellite network not uses the intelligent network for being in the communication network with terrestrial channel. In This segment, we describe the satellite network layer and transport layer features and security available in these layers.

A. SATELLITE NETWORK LAYER:

- Satellite Network is worked as the high-speed broadband wireless network with high intensity data transmission rate. Wireless LAN work on the IEEE 802.11 protocol Concepts with IP network layer has the property of data transmission. 802.11 protocol places parameters on both the physical (PHY) and access control (MAC) layers of the network. The physical layer handles the transmission of data between all nodes by using either direct sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS), or infrared (IR). IEEE 802.11 network has following specifications:

Table1. Different Wireless Network Communication bands

Properties	802.11b	802.11a	802.11g
Standard Approved	July 1999	July1999	June 2003
Maximum Data Rates	11Mbps	54Mbps	54Mbps
Modulation	CCK	OFDM	OFDM & CCK
Data Rates	1,2,5.5,11 Mbps	6,9,12,18,24,36,48,54 Mbps	CCK: 1,2,5.5,11 OFDM: 6,9,12,18,24,36,48,54 Mbps
frequencies	2.4-2.497GHz	5.15-5.35 GHz 5.425-5.675GHz 5.725-5.875GHz	2.4-2.497GHz

According to above table the transmission rates in the a,b and g networks are different and according to modulation, frequency and data transfer speed we can say that g network is better. 54 Mbps is quite enough in data transfers for audio transfer rates and radio communication.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

B. SATELLITE TRANSPORT LAYER

As we mentioned that the two protocols XCP and TCP patch+ are selected as satellite specific transport protocols. XCP outperform TCP-Patch+ except on high bit rate error environment. TCP patch+ is not compatible with active queue management scheme Red in satellite networks. TCP-patch+ performance depend upon buffer size. TCP cannot decide the difference between packet losses because of high rated bit error. So TCP reduces through put to overrides this. As the trend of growth of mobile based data communication is increased by many years and the demand of global data in less time is increased the transport of high speed data with better bit rate is required. As per demand of market the error rate should be less but no one can guarantee the communication line security at real time transfer of data from one end to another. As we know that TCP layer is an important part of ant data transport network. In today's scenario, not only signal, voice and video but also highly encrypted and secured defense related data and files are transported in the web through the satellite networks. TCP in the satellite is a major form of wireless network at local level. In the satellite network the range of data transmission is very high and accruable for the reliable communication of data. As we know that the TCP make reliable connection and in the wireless TCP has the following properties:Sending rate is identified by its congestion windows size (**cwz**) Round Trip Time (RTT) and data segment size (MSS). Since satellite networks are larger bandwidth delay product (BDP) so if MSS is constant and we want to transmit data in the same window than we required larger **cwz**due to larger BDP. In the beginning of the TCP data windows of transmission the cwz size is low as per requirement but at increase of data rates of transmission and acknowledgement the cwz size is increased.

C. SECURITY ASPECTS IN TCP LAYER AND NETWORK LAYER OF SATELLITE DATA NETWORK

In the satellite data transfer network the TCP header and IP header are encrypted. Security features are applied in the different layers in different forms. In end to end communication network with the high rate data transfer key pair are manages the authentication and authorization. But in attack condition may be this security will fail. So the network required more secured protocols and cryptography techniques to defend the attacker. In earth station we can apply TDM+CDMA security features. In present days IP encrypted are used in the earth station on the packets before sending it to geostationary stations. There are two types of the receivers in the satellite network 1. Static 2.Mobile.
In the static recovers the IP address is fixed and can authentic well by sending them the fixed key bunch for authentication and authorization. But in the mobile type receiver IP address will be dynamic and change in every instances of communication. So the security in mobile based receiver in satellite communication is harder with compare to static satellite receivers. Firewall also p[lay vital role in the internet which work on the packet filtering. In real world network the satellite based firewall with intelligent filtering system.

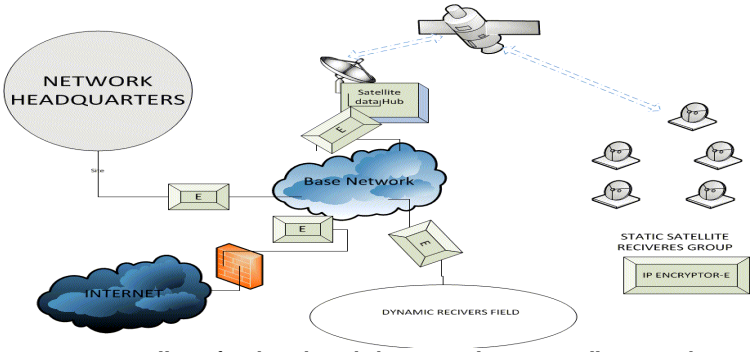

Fig. 2. Travelling of packets through the security layers in satellite network

Above figure shows that how the home earth station sends packet to the satellite and satellite distributes it among the authenticated receivers. However, each recover may have different encryption and security strategy according to hardware manufacturer and model. On the Internet, the firewall works for preventing the authorized packets and request denial.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

IV. PACKET TRANSMISSION IN SATELLITE NETWORK WITH AVAILABLE SECURITY

As we know that the architecture of wireless network in standard form is like in fig.3in which MAC layer is present in the field of data in layer as in OSI or TCP.IP model. In the MAC layer data encryption are work and the integrity and consistency are checked through this. As shown inn figure 802.11 WLAN is connected to the 802.3 Ethernet via a bridge.

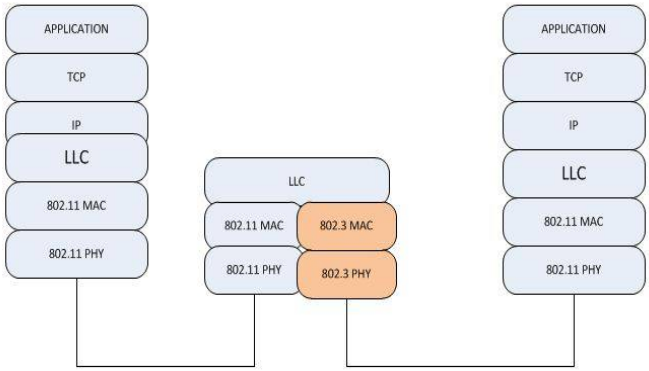

Fig. 3. Satellite Network Communication Layer Model

The above figure describes the layers of communication in the satellite data transmission model.; In which the satellite geostationary unit only have LLC, MAC and PHY layers. In transmission security mechanism of data the MAC layer play very important role.

So the data transmission in the satellite network is can be divided in the three parts:

1) **Satellite earth main station to geostationary link**: in the part data are transmitted from an 802.3 standard to the 802.11 network with conversion in power transmission signals. In the network data transmission in the satellite communication modules the data transmitted from the ground main station is encrypted in the MAC layer transmitter of the sender. At the receivers end total working standard of the satellite module is work as the wireless modules. Where 802.11 networks is working in the broadcast bandwidth and high speed network.
2) **Geostationary station to other Geostationary Station:**In the module one satellite is communicated with other in geostationary level and wireless communication is done through the 802.11 networks. in this module no human is interacted with the communication directly and communication can be done only through the automatic address generation and device authentication methods.
3) **Geostationary station to earth station:** in this part there may be two types of receivers one is static type and second is dynamic type. In the static type of recovers the LAN 802.3 is at end to end communication where various channels and networks are connected to main channel. In mobile type the connection method is wireless, so only 802.11 networks are works. In both formats the data encrypted through the double key or a pair of public and private keys.

The functions of wireless network of the satellite communication link are, MAC supports the association and association of a station in an access point. It controls synchronization and roaming of the station with an access point. Also done the power management part.

Encrypted packets are decrypted at the channel and stations inn roam filed. The flow of data from one link to other links done in the wireless mode with filtering in the satellite links, firewalls and authenticated with pair of keys shared by the earth sender station and geostationary station. For example, if a packet A sent from earth sender station with key Kpri and Kpub used for encryption of packet at earth station and decryption at geostationary station for the authentication. Now Geostationary Station creates a pair of key for different type of user at the earth station who wants to access data at the same time in different locations. So the key of first encryption of packet is different from key of decryption at last receiving site. The technology of encryption and decryption may be different in each level; key length also be different in both level. Security measures are depend upon the satellite channel providers and manufactures . Standers are margined by the local government and enforcement laws also.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

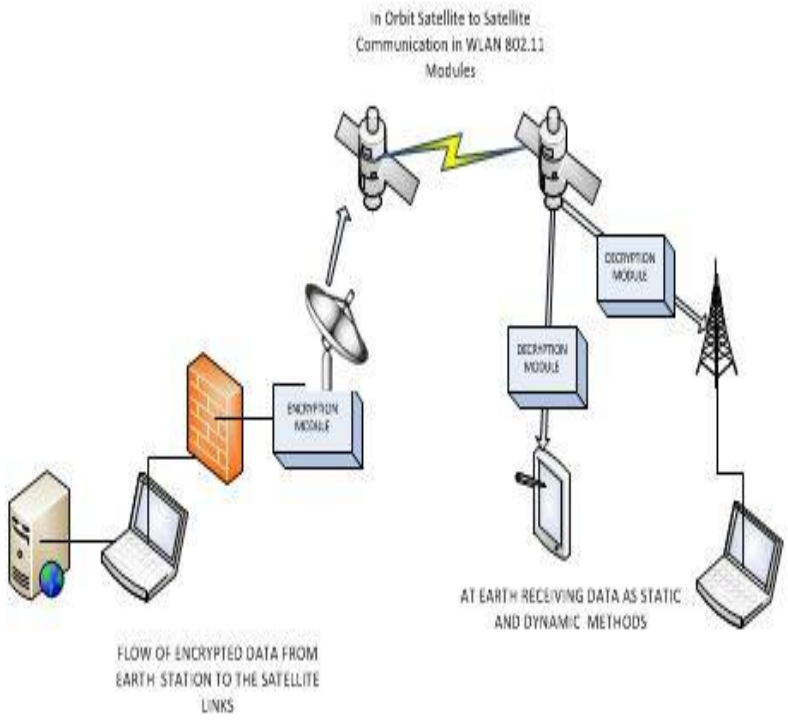

Fig.4. Satellite to satellite communication of packets in geostationary level.

Above figure describes that data transmission in long terminal inter-satellite communication links. In this type of communication link the data transmitted between two satellite unit and only verified and authenticated in Mac layer and LLC. Another layer of encryption is also available in the receivers and senders sides.

V. OMNET++ IMPLEMENTATION OF ABOVE NETWORK WITH NED AND PACKET ROUTING

In this section the experimental work is done for above network in parts.

I. Creation of NED

Main Host: Main host is working as ground station with server and computer to control data and upload data to the satellite uplink channel.

Firewall: Firewall checks outgoing and incoming packets and reply or acknowledgements for authentication.

Satellite Geostationary: In this part data coming from earth station are authenticated and decrypted, next address of packet receivers are checked and find the nearby station in which by packet will be routed.

Static Receivers: in this part a packet received from the satellite is check for errors and authentication then decrypted and send acknowledge to the satellite. Satellite uplink send acknowledge to the original sender of message.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

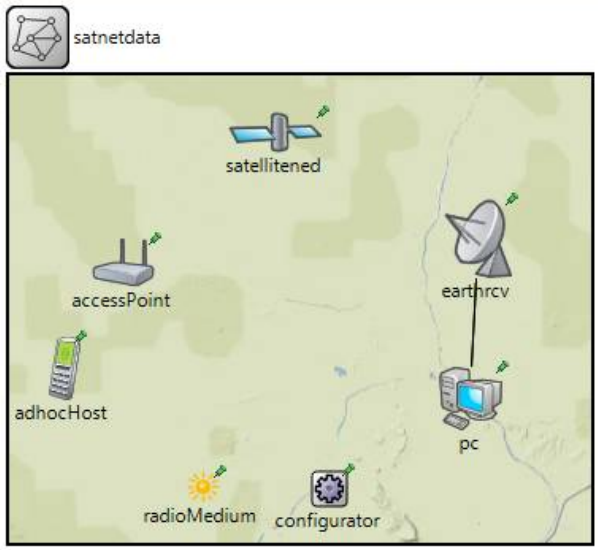

Fig.5. NED of satellite network simulation scenario in OMNeT++ 5

Above NED figure contain the physical channel as the radio channel of communication, pc as the standard host, access point as the simple wireless access point, adhoc host as the mobility based adhoc host satellitened as the geostationary unit of the satellite and earthrecv as the earth communication unit of the satellite data transmission network. As part of simulation the next section discusses the result of this simulation.

VI. RESULTS AND OUTCOMES

A. TRANSMISSION VECTOR CHART OF SIMULATION

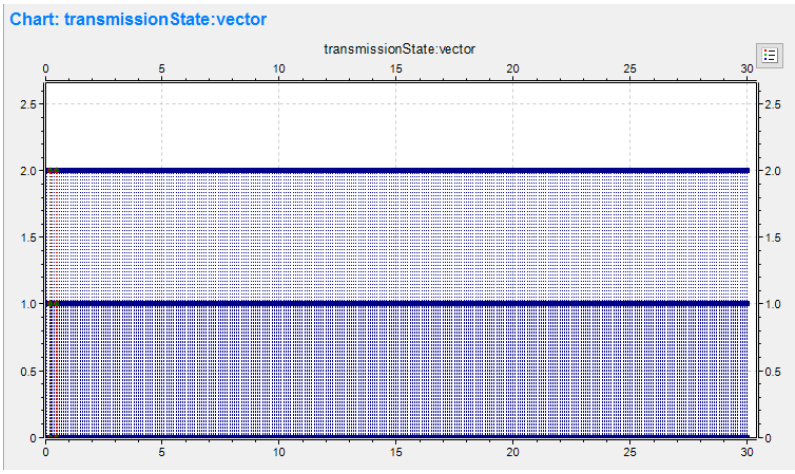

Fig.7. Transmission Vector Chart of Satellite Network (Secure)

We can easily see that as the time interval in increased the communication lines are decrease. The Transmission vary from 0 to 1 and second is from 1 to 2. The blue points shows that the data transmitted to the access points are reach at the high speed till the half communication channel up to 1.0 and in another half of the channel it is decreased.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

B. RECEIVED VECTOR CHART: THIS CHART DESCRIBES THE RECEIVED PACKETS BY DIFFERENT COMPONENTS IN THE NED.

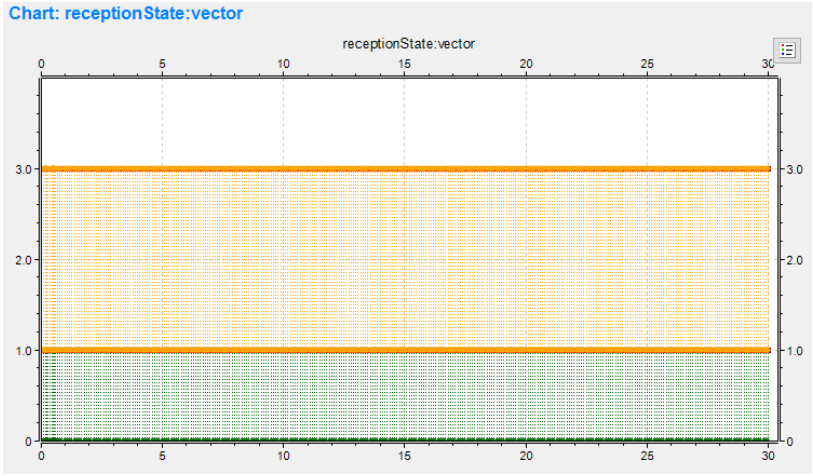

Fig.8. Satellite Reception State Vector Chart

This figure shows that the satellite reception packets are more authenticate during the communication started and up to 1 and then reliable between 1 to 3. The reception state vector in the above graph describes by the green line shows that the communication data reception by the satellite links and the orange lines of communication shows that the data reception in the adhoc mobility device.

C. SATELLITE MAC CHART

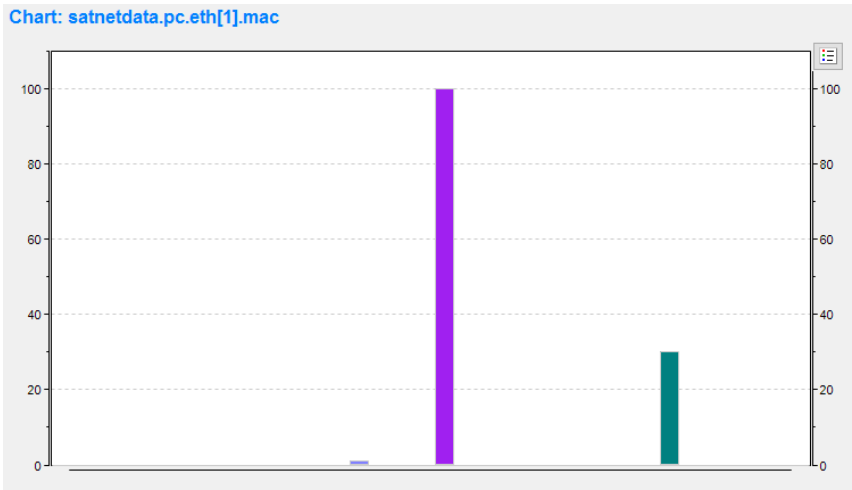

Fig.9. MAC chart of pc

In this figure the long line shows the packet receiving percentage that is 100 and green line shows the dropped packet after receiving and discarded them that is 30. The violet line shows the rate of transmission that is 100%.

VII. CONCLUSION

As we can see that different charts of results that are included the mac address chart, the sending and receiving of data chart, transmission of data from one node to another etc. Overall the packets that are comes from the authenticate users

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

are accepted by the security layers in each NED element and packets that are not authenticated are discarded by the security layer of that elements in the satellite network. Based on this satellite network security scenario we can develop the various attack and transmission enhancement projects and simulation with OMNeT++ 5. This is the base paper for more on the testing on satellite network simulation and their parts with the satellite data networks.

REFERENCES

[1]"TCP/IP Performance over Satellite Links", Craig Partridge And Timothy J. Shepard.
[2] Jiang Lei, Zhu Han, María Ángeles Vázquez-Castro and Are Hjørungnes, "Secure Satellite Communication ystems Design With Individual Secrecy Rate Constraints," IEEE Transactions On Information Forensics And Security, Vol. 6, No. 3, Pp. 661–671, Sep. 2011.
[3] Rohit Goyal, Sastri Kota, Raj Jain, Sonia Fahmy, Bobby Vandalore, And Jerry Kallaus "Analysis And Simulation Of Delay And Buffer Requirements Of Satellite-ATM Networks For TCP/IP Traffic,".
[4] Dr. Ranjit Singh, "Satellite Communications: The Indian Scenario,". Int. Journal of Engineering Research And Applications, Vol. 4,Issue 5(Version 4), Pp. 41-49, May 2014.
[5]Li Xiangqun, Wang Lu, Liu Lixiang, Hu Xiaohui, Xu Fanjiang And Chen Jing, "OMNET++ And Mixim-Based Protocol Simulator For Satellite Network".
[6] "Network Layer Integration of Terrestrial and Satellite IP Networks over BGP-S" EylemEkici, Ian F. Akyildiz and Michael D. Bender, Broadband & Wireless Networking Laboratory School of Electrical &Computer Engineering Georgia Institute of Technology,© 2001 IEEE Atlanta, GA 30332, pp-2698-2702.
[7]. "Improving TCP/IP Performance over Wireless Networks", Hari Balakrishnan, Srinivasan Seshan, Elan Amir and Randy H. Katz, In Proc. 1st ACM Int'l Conf. on Mobile Computing and Networking (Mobicom), November 95,
[8]. "Enhancing Transport Layer Capability in HAPS-SatelliteIntegrated Architecture", C. E. Palazzi, C. Roseti, M. Gerla,M. Luglio, M. Y. Sanadidi and J. Stepanek, °c 2004 Kluwer Academic Publishers. Printed in the Netherlands. Pp 1-26.
[9]. "Transport Layer Protocol Design for Satellite IP Networks", Kaiyu Zhou, Kwan L. Yeung and Victor O.K. Li, Department of Electrical and Electronic Engineering, The University of Hong KongHong Kong, PRC.