Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 2 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Efficient QOS based Routing Protocols for Next Generation Network (NGN)

By Salavadi Ananda Kumar & Dr. K. E. Sreenivasa Murthy
Jawaharlal Nehru Technological University, India

Abstract- Next Generation Network (NGN) is envisioned to be an inter-working environment of heterogeneous networks of wired and wireless access networks, PSTN, satellites, broadcasting, etc., all interconnected through the service provider's IP backbone and the Internet. NGN uses multiple broadband, QoS-enabled transport technologies and service-related functions independent from underlying transport-related technologies. The operations and management of such interconnected networks are expected to be much more difficult and important than the traditional network environment. In this paper, we present an overview of the current status towards the management of NGN and discuss challenges in operating and managing NGN. We also present the operations and management requirements of NGN in accordance with the challenges and verified two routing protocols for QOS support and providing security using caesarchiper encryption/decryption in Ad-hoc networks and also provide QOS for wired networks by AQM techniques and simulated results of AQM, Routing protocols using NS-2 and Encryption/Decryption using Matlab tools.

General Terms : *QOS AQM, NGN, red and drop tail.*

GJCST-E Classification : *C.2.0*

Strictly as per the compliance and regulations of:

An Efficient QOS based Routing Protocols for Next Generation Network (NGN)

Salavadi Ananda Kumar [α] & Dr. K. E. Sreenivasa Murthy [σ]

Abstract- Next Generation Network (NGN) is envisioned to be an inter-working environment of heterogeneous networks of wired and wireless access networks, PSTN, satellites, broadcasting, etc., all interconnected through the service provider's IP backbone and the Internet. NGN uses multiple broadband, QoS-enabled transport technologies and service-related functions independent from underlying transport-related technologies. The operations and management of such interconnected networks are expected to be much more difficult and important than the traditional network environment. In this paper, we present an overview of the current status towards the management of NGN and discuss challenges in operating and managing NGN. We also present the operations and management requirements of NGN in accordance with the challenges and verified two routing protocols for QOS support and providing security using caesarchiper encryption/decryption in Ad-hoc networks and also provide QOS for wired networks by AQM techniques and simulated results of AQM, Routing protocols using NS-2 and Encryption/Decryption using Matlab tools.

General Terms: *QOS AQM, NGN, red and drop tail.*

I. Introduction

NGN is envisioned to be an answer to network operators and service providers to replace existing telephone networks as well as to introduce a new converged service platform between fixed and mobile telecommunication businesses [1]. It is generally agreed that the main difference between traditional telecommunication networks and NGN is the shift from separate and vertically integrated application-specific networks to a single network capable of carrying any services. NGN is essentially about delivering new services that are available to any place, at any time, on any device, through any customer-chosen access mechanism. NGN is expected to co-exist and inter-work among wired networks (e.g., xDSL, Metro Ethernet, FTTH, leased lines, ISDN), wireless networks (e.g., 2G, 3G, WLAN, WiMAX/WiBro) as well as satellites and broadcasting networks, all interconnected through the service provider's IP backbone networks and the Internet.

In this heterogeneous networking environment, in addition to the traditional challenges such as security, QoS, and charging, new challenges such as generalized mobility, and network discovery and selection exist.

Providing effective, secure and efficient operations and management of the envisioned NGN environment is a huge challenge. In order to provide the creation, deployment, and management of all kinds of services, NGN operations are highly dependent on flexible and efficient management systems and processes [2]. When the networks are evolving towards NGN, the scenario to support various services would become more complex.

The carrying of diverse traffic such as voice, data, video or signaling would be possibly integrated onto one common platform, which would call for the corresponding network management systems.

The ITU-T Recommendation Y.2401 [5] presents the management requirements, general principles and architectural requirements for managing NGN to support business processes to plan, provision, install, maintain, operate and administer NGN resources and services [4].

Thus, we examine the challenges facing the management of NGN. The standards and research activities of NGN management are also presented.

a) NGN Overview

NGN is a packet-based network to support the transfer of mixed traffic types such as voice, video, and data [1]. It will integrate services offered by traditional networks and new innovative IP services into a single service platform. The key operation of the NGN is the separation of services and transport networks, which provides QoS-enabled transport technologies and service-related functions independent from underlying transport technologies [7]. The transport functions provide transfer of information between peer entities; the services functions are concerned with the applications and services to be operated between peer entities [8].

Fig. 1 shows typical NGN components: service network, core network, access network, and user equipment [8]. The service network is composed of various servers such as Web Server, Authentication, Authorization and Accounting (AAA), SIP Proxy Server and LDAP Server, etc. The service network is only responsible for providing services and applications for NGN users. The connection between the service network and the core network can be implemented via gateways.

Author α: Research Scholar, Jawaharlal Nehru Technological University, Hyderabad. e-mail: anand.80.kumar@gmail.com
Author σ: Professor, Department of ECE, Brahmas Institute of Engineering & Technology, Nellore. e-mail: kesmurthy@rediffmail.com

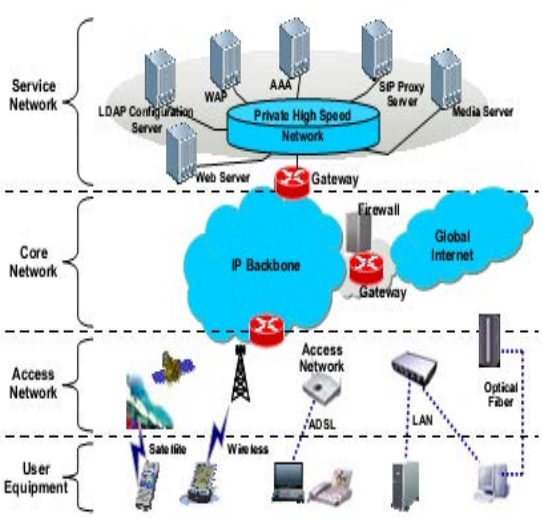

Figure 1 : NGN Network components

b) Integrated Network Platform

The core network in NGN represents the transportation backbone in traditional networks, which is concerned with the transfer of information between peer entities. Besides the transfer of packets, control and management functions are also implemented in the core network. The access network in NGN is derived from the existing access technologies. To accommodate various access media, the access network is separated from the core network of NGN, which serves as an intermediate between user equipment's and core network.

Integrated Network Platform refers to the integration of all IP capable wireless and wire line systems for the seamless delivery of Internet data services.

The goal is to allow mobile users to move transparently from wired to wireless networks or vice-versa without breaking their connection to the Internet. An office worker, connected to an Ethernet LAN, could transparently switch to a high-speed WLAN connection in order to maintain connectivity and provision of services. While moving around within the building, the node could switch transparently from one wireless subnet to another, and when leaving the building, could again switch transparently to a wide-area wireless data service such as GPRS or UMTS.

The increasing availability of wireless and wire line technologies with different properties will make the creation of an integrated network platform possible. Such integration should address following requirements:

- Enabling global mobility for users across different bearer types (integration of wireless & wire line technologies).
- Integration of Ad-hoc networks ñ Coverage extension in environments without networking infrastructure.
- Intelligent multiple interface handling ñ Filtering data streams to utilize the best interface which are based on different bearer technologies.

c) Ad-Hoc Networks

An ad-hoc network consists of a collection of mobile nodes without the required intervention of a centralized access point or existing infrastructure. The links of the network are dynamic and are based on the proximity of one node to another node. These links are likely to break and change as the nodes move across the network. Because of the temporary nature of the network links, and because of the additional constraints on mobile nodes (limited bandwidth and power), conventional routing protocols are not appropriate for ad-hoc mobile networks.

Protocols in Ad-hoc Networks

Unlike the cellular networks where base stations are essential, ad-hoc networks is backed up by communications directly between mobiles, thus the routing protocols are central and deserve our focus on their mechanisms. And in ad-hoc networks, there exists several routing protocols as listed below, which will be demonstrated in this report:

1. DSDV: Destination Sequenced Distance Vector
2. AODV: Ad-hoc On Demand Distance Vector

II. Backgrounds

AD HOC networks are networks of autonomous nodes that have wireless connections between each other. These connections can created and destroyed, changing the network topology as nodes change location, move out of range of other nodes or fail completely. Ad hoc networks pose an additional set of problems to those encountered in traditional fixed networks or wireless cellular networks. Dynamically forming the communications infrastructure from mobile devices is the source of these complications. One way of thinking about this is to imagine the problems caused by continually moving and changing the router you use to get from your local subnet to the rest of the world. How would packets get to or from you? This type of question has to be addressed along with requirements that affect traditional routing protocols such as loop free routing, completeness and stability.

As we have already seen, classical encryption techniques use scrambling of bits in order to encipher the message. In this section, we discuss three important classical cryptographic techniques namely,

1. Playfair Cipher
2. Vigenere Cipher
3. Caesar Cipher

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate

letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center.

The Vigenere Cipher is the process of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. To encrypt, a Vigenere square is used. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

III. Proposed Method

NGN Functional Architecture

Fig. 2 shows an overview of the NGN functional architecture [2]. The NGN architecture needs to offer the configuration flexibility to support multiple access technologies. It also needs to support a distributed and open control mechanism, which provides a separated service provisioning from transport network operation and speeds up the provision of diversified NGN services.

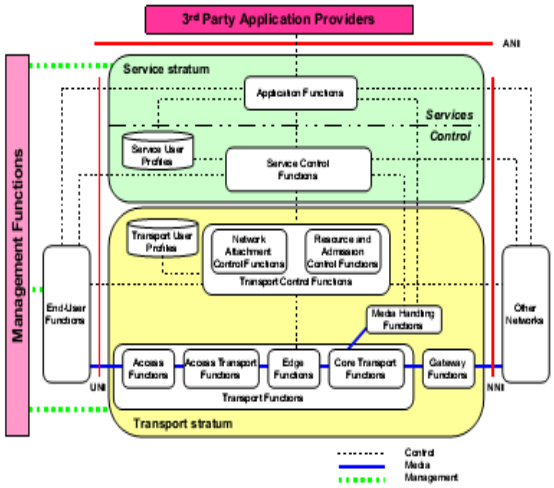

Figure 2 : NGN functional architecture

The NGN functions are divided into service and transport strata. The transport stratum functions provide connectivity for all components and physically separated functions within the NGN. The service stratum functions provide session-based and non-session-based services, including subscribe/notify for presence information and a messaging method for instant message exchange [7]. End-user functions are connected to the NGN by user-to-network interface (UNI), while other networks are interconnected through the network-to-network interface (NNI). The application-to-network interface (ANI) provides a channel for interactions and exchanges between applications and NGN elements.

a) Network Discovery And Selection

Since NGN consists of interconnected heterogeneous networks using heterogeneous user terminals, NGN should provide a seamless capability, independent of access method and network, and NGN also should address the identifying mechanisms [1]. That is, each terminal can use more than one type of network and possibly access multiple networks simultaneously for different applications (e.g., one for voice and another for receiving streaming media).

In such an environment, a terminal must be able to discover what networks are available for use. One of the proposed solutions for network discovery is to use software-defined radio devices that can scan the available networks. After scanning, they will load the required software and reconfigure themselves for the selected network. The software can be downloaded from the media such as a server, smart card, memory card or over the air.

b) Generalized Mobility

At present, mobility is used in a limited sense such as movement of user and terminal and with or without service continuity to similar public accessed networks (such as WLAN, GSM, UMTS, etc.) [6]. this means the horizontal handoff, which involves a terminal device to change cells within the same type of network to maintain service continuity. In the future, mobility will be offered in a broader sense where users may have the ability to use more access technologies, allowing movements between public wired access points and public wireless access points of various technologies. That is, in NGN environment, in addition to the horizontal handoff, the vertical handoff must also be supported. The vertical handoff mechanism allows a terminal device to change networks between different types of networks (e.g., between 3G and 4G networks) in a way that is completely transparent to end user applications. Thus, the challenge is to allow vertical handoffs between pairs of different types of networks in the presence of 2G, 3G, WLAN, WMAN, satellite, and 4G networks. The greater challenge lies when the vertical handoffs must take place with a certain set of QoS requirements still satisfied. Roaming allows a customer to automatically make and receive voice calls, send and receive data, or access other services when traveling outside the geographical coverage area of the home network. Roaming is technically supported by mobility management, authentication and billing procedures. Establishing roaming between service providers is based on roaming agreements. If the visited network is in the same country as the home network, then it is known as national roaming. If the visited network is

outside the home country, then it is known as global roaming. If the visited network operates on a different technical standard than the home network, then it is known as inter-standard roaming.

In NGN, all three types of roaming should be supported to roam through different network types, operating in different cities and countries. For true global roaming, roaming agreements must be set up among service providers among countries. Today, only a few service providers in different countries provide global roaming. The challenge is to provide more roaming agreements among the service providers in different countries. The greater challenge would be to provide inter-standard roaming in different countries.

c) Qos Support

Over the past decade, much research has been conducted in the area of QoS, and many protocols and methods have been proposed. However, the predominant method to support QoS by the Internet service providers (ISPs) today is over-provisioning. That is, instead of implementing complex QoS algorithms and methods, ISPs typically provide enough bandwidth in their backbone trunks so that their networks are hardly overloaded and thus there exists very little delay and few packets are lost in transit. This is quite feasible since a lot of fiber trunks have been installed over the past decade and the bandwidth cost of wired Internet trunks is very cheap. In the ISP's views, it is much simpler and cheaper to provide over-provisioned networks than implementing and managing complex QoS mechanisms. Although NGN is supposed to provide higher bandwidth and more cost-effective channels than its predecessor networks, the bandwidth cost in NGN wireless networks will remain higher than wired networks. Thus, over-provisioning in NGN will not be feasible and QoS support mechanisms will definitely be needed. Providing QoS support in NGN will be a major challenge thus much work is needed.

Congestion is an important issue which researchers focus on in the Transmission Control Protocol(TCP) network environment. To keep the stability of the whole network, congestion control algorithms have been extensively studied. Queue management method employed by the routers is one of the important issues in the congestion control study. Active queue management (AQM) has been proposed as a router-based mechanism for early detection of congestion inside the network. In this paper we analyzed several active queue management algorithms with respect to their abilities of maintaining high resource utilization, identifying and restricting disproportionate bandwidth usage, and their deployment complexity.

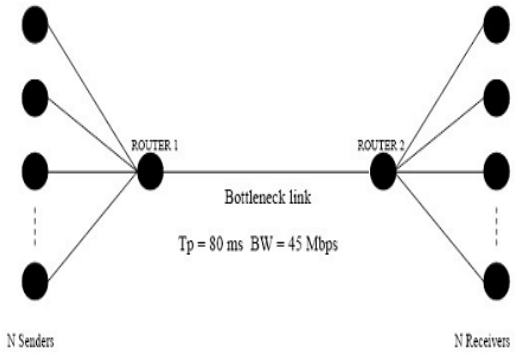

Figure 3 : Simulation topology

We compare the performance of RED, Drop tail based on simulation results, using RED and Drop Tail as the evaluation baseline. The characteristics of different algorithms are also discussed and compared. Simulation is done by using Network Simulator (NS2) and the graphs are drawn using X- graph.

Throughput: This is the main performance measure characteristic, and most widely used. In communication networks, such as Ethernet or packet radio, throughput or network throughput is the average rate of successful message delivery over a communication channel. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

This measure how soon the receiver is able to get a certain amount of data send by the sender. It is determined as the ratio of the total data received to the end to end delay. Throughput is an important factor which directly impacts the network performance.

Delay: Delay is the time elapsed while a packet travels from one point e.g., source premise or network ingress to destination premise or network degrees. The larger the value of delay, the more difficult it is for transport layer protocols to maintain high bandwidths. We will calculate end to end delay.

d) Routing Protocols

Efficient routing protocols can provide significant benefits to mobile ad hoc networks in terms of both performance and reliability. Mobile Ad-hoc Network (MANET) is an infrastructure less and decentralized network which need a robust dynamic routing protocol. Many routing protocols for such networks have been proposed so far. Amongst the most popular ones are Dynamic Source Routing (DSR), Ad-hoc On-demand Distance Vector (AODV), and Destination-Sequenced Distance Vector (DSDV) routing protocol. To compare the performance of AODV and DSDV routing protocol, the simulation results were analyzed by graphical manner and trace file based on Quality of Service (QoS) metrics.

We will simulate an ad-hoc network using different routing protocols with the help of NS and then make a comparison based on the result.

Fig 4 shows basic topology of 3 node network in which initial location of nodes 0, 1 and 2 are respectively (5, 5), (490,285) and (150,240) (the z coordinate is assumed throughout to be 0).

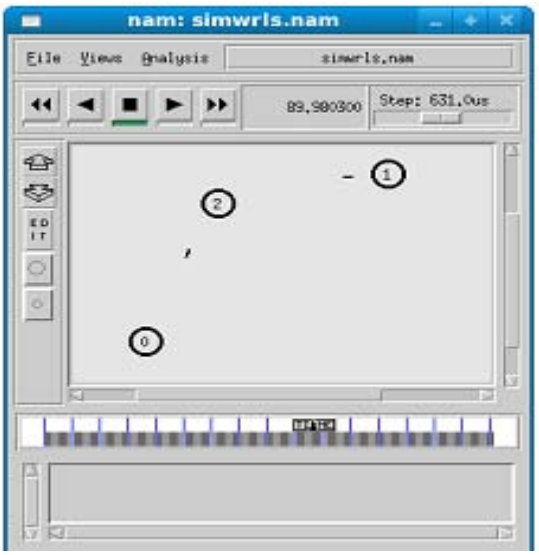

Figure 4 : Basic topology of 3-nodes network

At time 10, node 0 starts moving towards point (250,250) at a speed of 3m/sec. At time 15, node 1 starts moving towards point (45, 258) at a speed of 5m/sec. At time 110, node 0 starts moving towards point (480,300) at a speed of 5m/sec.

The simulation lasts 150 sec. At time 10, TCP connection using the DSDV ad-hoc routing protocol and the IEEE802.11 MAC protocol is initiated between node 0 and node 1.

e) Security

Over the past few years, the Internet and enterprise networks have been plagued by denial of service attacks (DoS), worms and viruses, which have caused millions of computer systems to be shutdown or infected and the stored data to be lost, ultimately causing billions of dollars in loss. The introduction of wireless LANs (e.g., IEEE 802.11) into enterprises has made network security more vulnerable since rogue base stations (i.e., unauthorized private base stations) can be easily connected to existing wired networks, potentially becoming the source of security attacks inside firewalls and intrusion detection systems. Moreover, connecting malicious PC via a base station that is not well managed is also critical.

In cryptography, a Caesar cipher, also known as the shift cipher, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on.

To pass an encrypted message from one person to another, it is first necessary that both parties have the 'key' for the cipher, so that the sender may encrypt it and the receiver may decrypt it. For the Caesar cipher, the key is the number of characters to shift the cipher alphabet. Here is a quick example of the encryption and decryption steps involved with the Caesar cipher. The text we will encrypt is 'defend the east wall of the castle', with a shift (key) of 1.

Plaintext: defend the east wall of the castle
Cipher text: efgfoe uif fbtu xbmm pg uif dbtumf

It is easy to see how each character in the plaintext is shifted up the alphabet. Decryption is just as easy, by using an offset of -1.

Plain: abcdefghijklmnopqrstuvwxyz
Cipher: bcdefghijklmnopqrstuvwxyza

Obviously, if a different key is used, the cipher alphabet will be shifted a different amount.

Mathematical Description

First we translate all of our characters to numbers, 'a'=0, 'b'=1, 'c'=2... 'z'=25. We can now represent the Caesar cipher encryption function, e(x), where x is the character we are encrypting, as:

$$e(x) = (x + k) \pmod{26}$$

Where k is the key (the shift) applied to each letter. After applying this function the result is a number which must then be translated back into a letter. The decryption function is:

$$e(x) = (x - k) \pmod{26}$$

Figure 5 : Encryption process

Figure 6 : Decryption process

IV. Results

a) Simulation Model

The objective of this paper is the performance evaluation of two routing protocol for mobile ad hoc networks by using an open-source network simulation tool called NS-2. Two routing protocols: DSDV and AODV have been considered for performance evaluation in this work. The simulation environment has been conducted with the LINUX operating system, because NS-2 works with Linux platform only.

Whole simulation study is divided into two part one is create the node (that may be cell phone, internet or any other devices) i.e. NS-2 output. It's called NAM (Network Animator) file, which shows the nodes movement and communication occurs between various nodes in various conditions or to allow the users to visually appreciate the movement as well as the interactions of the mobile nodes. And another one is graphical analysis of trace file (.tr).Trace files contains the traces of event that can be further processed to understand the performance of the network.

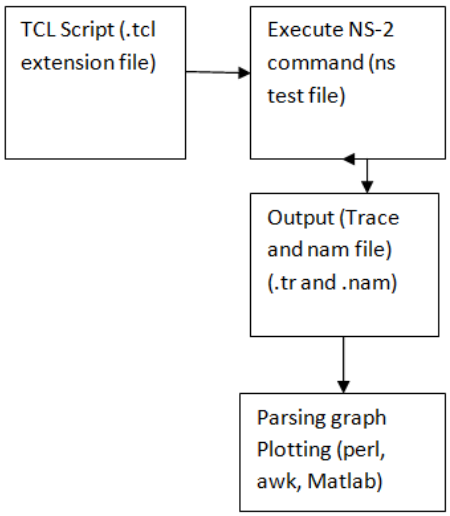

Figure 7 : Simulation overview

Figure 7 depicts the overall process of how a network simulation is conducted under NS-2. Output files such as trace files have to be parsed to extract useful information. The parsing can be done using the awk command (in UNIX and LINUX, it is necessary to use gawk for the windows environment) or Perl script. The results have been analyzed using Excel or Matlab.
A software program which can shorten the process of parsing trace files (Xgraph and Trace Graph) has also been used in this paper. However, it doesn't work well when the trace file is too large.

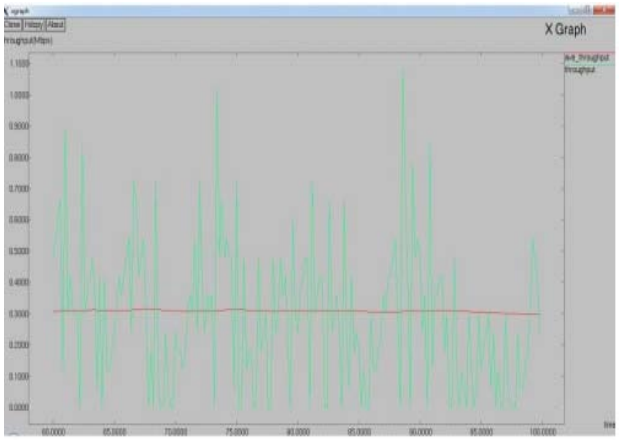

Figure 8 : Drop tail

Figure 8 shows how throughput varies w.r.t simulation time had been depicted shows unfair.

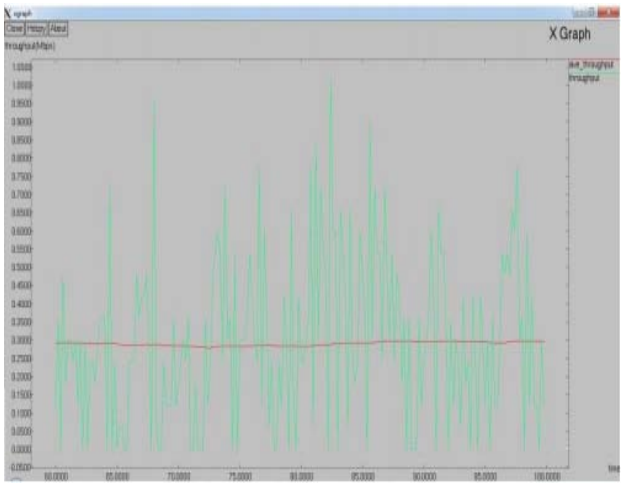

Figure 9 : RED

To generate trace file and nam file, we call tcl script in CYGWIN command shell. By varying the simulation parameter shown in table 1, we can see the graphical variation between various performance metrics like throughput, drop, delay, jitter etc.

Figure 9 shows how throughput varies w.r.t simulation time been depicted.

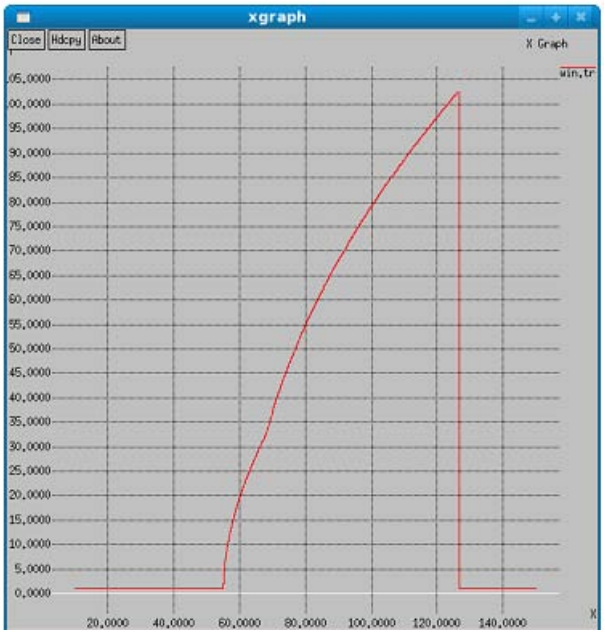

Figure 10 : window evolution before DSDV changes

At the beginning the nodes are too far away and a connection cannot be set. The first TCP signaling packet is transmitted at time 10 sec but the connection cannot be opened.

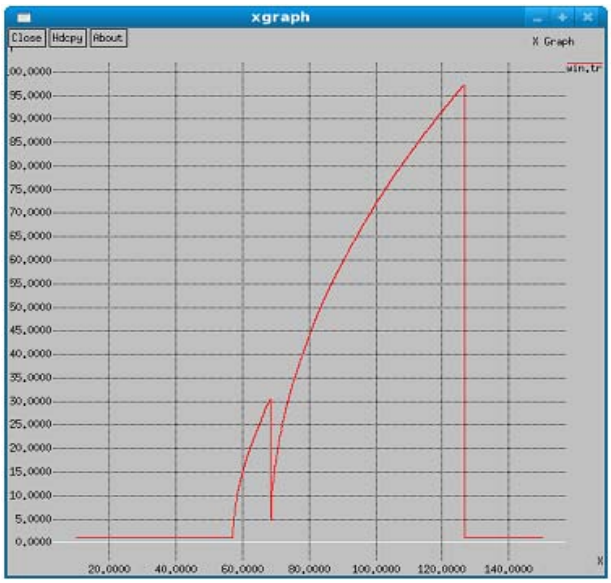

Figure 11 : window evolution after DSDV changes

Meanwhile nodes 0 and nodes 1 start moving towards node2. After 6 second (timeout) a second reatempt occurs but still the connection cannot be established and the timeout valure is doubled to 12sec.

At time 28 another transmission attempt occurs.While the connection still could not be established.Then at around 55 sec, both nodes 0 as well as node 1 to be within the radio of node 2 so that when tcp connection is reattempted at that time a two hop path is established between node 0 a direct connection is established.

At the moment of the path change there is a single TCP packet loss that cause the window to decrease slightly.At time 125.5 nodes 0 and 1 are too far apart for the connection to be maintained and the conncetion breaks.

From fig 12 it is seen that at 40sec connection is established and window size increases smoothly without any path change also no packet loss up to 144sec then window size decreases due to connection break.

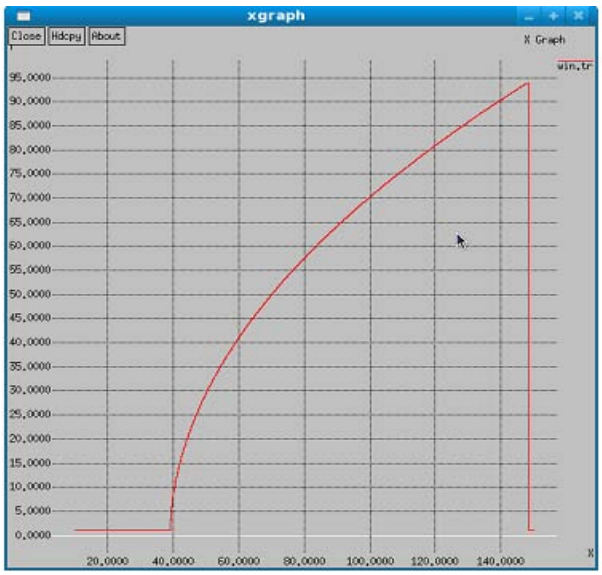

Figure 12 : window evolution over AODV changes

V. Conclusions

Simulation results show that DSDV compared with AODV, DSDV routing protocol consumes more bandwidth, because of the frequent broadcasting of routing updates. While the AODV is better than DSDV as it doesn't maintain any routing tables at nodes which results in less overhead and more bandwidth. AODV perform better under high mobility simulations than DSDV. High mobility results in frequent link failures and the overhead involved in updating all the nodes with the new routing information as in DSDV is much more than that involved AODV, where the routes are created as and when required. AODV use on -demand route discovery, but with different routing mechanics. AODV uses routing tables, one route per destination, and destination sequence numbers, a mechanism to prevent loops and to determine freshness of routes.

References Références Referencias

1. ITU-T, "General overview of NGN", Recommendation Y.2001, Dec. 2004.
2. ITU-T, "General principles and general reference model for Next Generation Networks", Recommendation Y.2011, Oct. 2004.
3. ITU-T, "Functional requirements and architecture of the NGN", Recommendation Y.2012, Sep. 2006.

4. ITU-T, "Resource and admission control functions in Next Generation Networks", Recommendation Y.2111, Sep. 2006.
5. ITU-T, "Principles for the Management of the Next Generation Networks", Recommendation Y.2401, Mar. 2006.
6. ITU-T, "Mobility management requirements for NGN", Recommendation Y.2801, Nov. 2006.
7. Keith Knight, Thomas Towle, Naotaka Morita, "NGN architecture: generic principle, functional architecture, and its realization", IEEE Communications Magazine, vol. 43, no. 10, Oct. 2005, pp.49-56.
8. Mo Li and Kumbesan Sandrasegaran, "Network Management Challenges for Next Generation Networks", IEEE Conference on Local Computer Networks, Nov. 2005, pp. 593 - 598.