

# 1 An Efficient QOS based Routing Protocols for Next Generation 2 Network (NGN)

3 icom Technologies<sup>1</sup>, Salavadi Ananda Kumar<sup>2</sup> and Dr. K.E.Sreenivasa Murthy<sup>3</sup>

4 <sup>1</sup> Jawaharlal Nehru Technological University

5 *Received: 13 December 2013 Accepted: 5 January 2014 Published: 15 January 2014*

6

---

## 7 **Abstract**

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

21

---

22 *Index terms*— QoS AQM, NGN, red and drop tail.

## 23 **1 Introduction**

24 NGN is envisioned to be an answer to network operators and service providers to replace existing telephone networks  
25 as well as to introduce a new converged service platform between fixed and mobile telecommunication businesses  
26 [1]. It is generally agreed that the main difference between traditional telecommunication networks and NGN  
27 is the shift from separate and vertically integrated applications specific networks to a single network capable of  
28 carrying any services. NGN is essentially about delivering new services that are available to any place, at any  
29 time, on any device, through any customer chosen access mechanism. NGN is expected to coexist and inter-work  
30 among wired networks (e.g., xDSL, Metro Ethernet, FTTH, leased lines, ISDN), wireless networks (e.g., 2G, 3G,  
31 WLAN, WiMAX/WiBro) as well as satellites and broadcasting networks, all interconnected through the service  
32 provider's IP backbone networks and the Internet.

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

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

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

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

## 5 BACKGROUNDS

---

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

### 46 2 a) NGN Overview

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

53 Fig. 1 shows typical NGN components: service network, core network, access network, and user equipment  
54 [8]. The service network is composed of various servers such as Web Server, Authentication, Authorization and  
55 Accounting (AAA), SIP Proxy Server and LDAP Server, etc. The service network is only responsible for providing  
56 services and applications for NGN users. The connection between the service network and the core network can  
57 be implemented via gateways. The core network in NGN represents the transportation backbone in traditional  
58 networks, which is concerned with the transfer of information between peer entities. Besides the transfer of  
59 packets, control and management functions are also implemented in the core network. The access network in  
60 NGN is derived from the existing access technologies. To accommodate various access media, the access network  
61 is separated from the core network of NGN, which serves as an intermediate between user equipment's and core  
62 network.

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

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

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

73 ? Enabling global mobility for users across different bearer types (integration of wireless & wire line  
74 technologies). ? Integration of Ad-hoc networks ? Coverage extension in environments without networking  
75 infrastructure.

76 ? Intelligent multiple interface handling ? Filtering data streams to utilize the best interface which are based  
77 on different bearer technologies.

### 78 3 c) Ad-Hoc Networks

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

## 84 4 Protocols in Ad-hoc Networks

85 Unlike the cellular networks where base stations are essential, ad-hoc networks is backed up by communications  
86 directly between mobiles, thus the routing protocols are central and deserve our focus on their mechanisms. And  
87 in ad-hoc networks, there exists several routing protocols as listed below, which will be demonstrated in this  
88 report: 1. DSDV: Destination Sequenced Distance Vector 2. AODV: Ad-hoc On Demand Distance Vector II.

## 89 5 Backgrounds

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

98 As we have already seen, classical encryption techniques use scrambling of bits in order to encipher the  
99 message. In this section, we discuss three important classical cryptographic techniques namely, 1. Playfair  
100 Cipher 2. Vigenere Cipher

---

## 101 6 Caesar Cipher

102 The Playfair cipher uses a 5 by 5 table containing a key word or phrase. To generate the key table, one would  
103 first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the  
104 remaining spaces with the rest of the letters of the alphabet in order (put both "I" and "J" in the same space).  
105 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  
106 beginning in the upper-left-hand corner and ending in the center.

107 The Vigenere Cipher is the process of encrypting alphabetic text by using a series of different Caesar ciphers  
108 based on the letters of a keyword. To encrypt, a Vigenere square is used. It consists of the alphabet written  
109 out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet,  
110 corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses  
111 a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.  
112 The NGN functions are divided into service and transport strata. The transport stratum functions provide  
113 connectivity for all components and physically separated functions within the NGN. The service stratum functions  
114 provide session-based and non-sessionbased services, including subscribe/notify for presence information and a  
115 messaging method for instant message exchange [7]. End-user functions are connected to the NGN by user-  
116 to-network interface (UNI), while other networks are interconnected through the network-to-network interface  
117 (NNI). The applicationto-network interface (ANI) provides a channel for interactions and exchanges between  
118 applications and NGN elements.

## 119 7 III.

## 120 8 Proposed Method

121 NGN Functional Architecture

## 122 9 a) Network Discovery And Selection

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

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

## 132 10 b) Generalized Mobility

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

151 In NGN, all three types of roaming should be supported to roam through different network types, operating  
152 in different cities and countries. For true global roaming, roaming agreements must be set up among service  
153 providers among countries. Today, only a few service providers in different countries provide global roaming.  
154 The challenge is to provide more roaming agreements among the service providers in different countries. The  
155 greater challenge would be to provide inter-standard roaming in different countries. c) Qos Support Over the  
156 past decade, much research has been conducted in the area of QoS, and many protocols and methods have been  
157 proposed. However, the predominant method to support QoS by the Internet service providers (ISPs) today is  
158 over-provisioning. That is, instead of implementing complex QoS algorithms and methods, ISPs typically provide

## 13 PLAIN: ABCDEFGHIJKLMNOPQRSTUVWXYZ CIPHER: BCDEFGHIJKLMNOPQRSTUVWXYZA

---

159 enough bandwidth in their backbone trunks so that their networks are hardly overloaded and thus there exists  
160 very little delay and few packets are lost in transit. This is quite feasible since a lot of fiber trunks have been  
161 installed over the past decade and the bandwidth cost of wired Internet trunks is very cheap. In the ISP's views,  
162 it is much simpler and cheaper to provide over-provisioned networks than implementing and managing complex  
163 QoS mechanisms. Although NGN is supposed to provide higher bandwidth and more cost-effective channels than  
164 its predecessor networks, the bandwidth cost in NGN wireless networks will remain higher than wired networks.  
165 Thus, over-provisioning in NGN will not be feasible and QoS support mechanisms will definitely be needed.  
166 Providing QoS support in NGN will be a major challenge thus much work is needed.

167 Congestion is an important issue which researchers focus on in the Transmission Control Protocol(TCP)  
168 network environment. To keep the stability of the whole network, congestion control algorithms have been  
169 extensively studied. Queue management method employed by the routers is one of the important issues in the  
170 congestion control study. Active queue management (AQM) has been proposed as a router-based mechanism for  
171 early detection of congestion inside the network. In this paper we analyzed several active queue management  
172 algorithms with respect to their abilities of maintaining high resource utilization, identifying and restricting  
173 disproportionate bandwidth usage, and their deployment complexity. Simulation is done by using Network  
174 Simulator (NS2) and the graphs are drawn using X-graph.

175 Throughput: This is the main performance measure characteristic, and most widely used. In communication  
176 networks, such as Ethernet or packet radio, throughput or network throughput is the average rate of successful  
177 message delivery over a communication channel. The throughput is usually measured in bits per second (bit/s  
178 or bps), and sometimes in data packets per second or data packets per time slot. This measure how soon the  
179 receiver is able to get a certain amount of data send by the sender. It is determined as the ratio of the total  
180 data received to the end to end delay. Throughput is an important factor which directly impacts the network  
181 performance. Delay: Delay is the time elapsed while a packet travels from one point e.g., source premise or  
182 network ingress to destination premise or network degrees. The larger the value of delay, the more difficult it is  
183 for transport layer protocols to maintain high bandwidths. We will calculate end to end delay.

## 184 11 d) Routing Protocols

185 Efficient routing protocols can provide significant benefits to mobile ad hoc networks in terms of both performance  
186 and reliability. Mobile Ad-hoc Network (MANET) is an infrastructure less and decentralized network which need  
187 a robust dynamic routing protocol. Many routing protocols for such networks have been proposed so far. Amongst  
188 the most popular ones are Dynamic Source Routing (DSR), Adhoc On-demand Distance Vector (AODV), and  
189 Destination-Sequenced Distance Vector (DSDV) routing protocol. To compare the performance of AODV and  
190 DSDV routing protocol, the simulation results were analyzed by graphical manner and trace file based on Quality  
191 of Service (QoS) metrics. The simulation lasts 150 sec. At time 10, TCP connection using the DSDV ad-hoc  
192 routing protocol and the IEEE802.11 MAC protocol is initiated between node 0 and node 1.

## 193 12 e) Security

194 Over the past few years, the Internet and enterprise networks have been plagued by denial of service attacks  
195 (DoS), worms and viruses, which have caused millions of computer systems to be shutdown or infected and the  
196 stored data to be lost, ultimately causing billions of dollars in loss. The introduction of wireless LANs (e.g., IEEE  
197 802.11) into enterprises has made network security more vulnerable since rogue base stations (i.e., unauthorized  
198 private base stations) can be easily connected to existing wired networks, potentially becoming the source of  
199 security attacks inside firewalls and intrusion detection systems. Moreover, connecting malicious PC via a base  
200 station that is not well managed is also critical.

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

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

210 Plaintext: defend the east wall of the castle Cipher text: efgfoe uif fbtu xbmm pg uif dbtumf It is easy to see  
211 how each character in the plaintext is shifted up the alphabet. Decryption is just as easy, by using an offset of  
212 -1.

## 213 13 Plain: abcdefghijklmnopqrstuvwxyz Cipher: bcdefghi- 214 jklmnopqrstuvwxyz

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

---

## 216 14 Mathematical Description

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

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

## 221 15 Results

### 222 16 a) Simulation Model

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

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

233 Figure ?? : Simulation overview Figure ?? depicts the overall process of how a network simulation is conducted  
234 under NS-2. Output files such as trace files have to be parsed to extract useful information. The parsing can be  
235 done using the awk command (in UNIX and LINUX, it is necessary to use gawk for the windows environment)  
236 or Perl script. The results have been analyzed using Excel or Matlab. A software program which can shorten the  
237 process of parsing trace files (Xgraph and Trace Graph) has also been used in this paper. However, it doesn't  
238 work well when the trace file is too large. ??, we can see the graphical variation between various performance  
239 metrics like throughput, drop, delay, jitter etc.

240 Figure 9 shows how throughput varies w.r.t simulation time been depicted. At time 28 another transmission  
241 attempt occurs. While the connection still could not be established. Then at around 55 sec, both nodes 0 as well  
242 as node 1 to be within the radio of node 2 so that when tcp connection is reattempted at that time a two hop  
243 path is established between node 0 a direct connection is established.

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

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

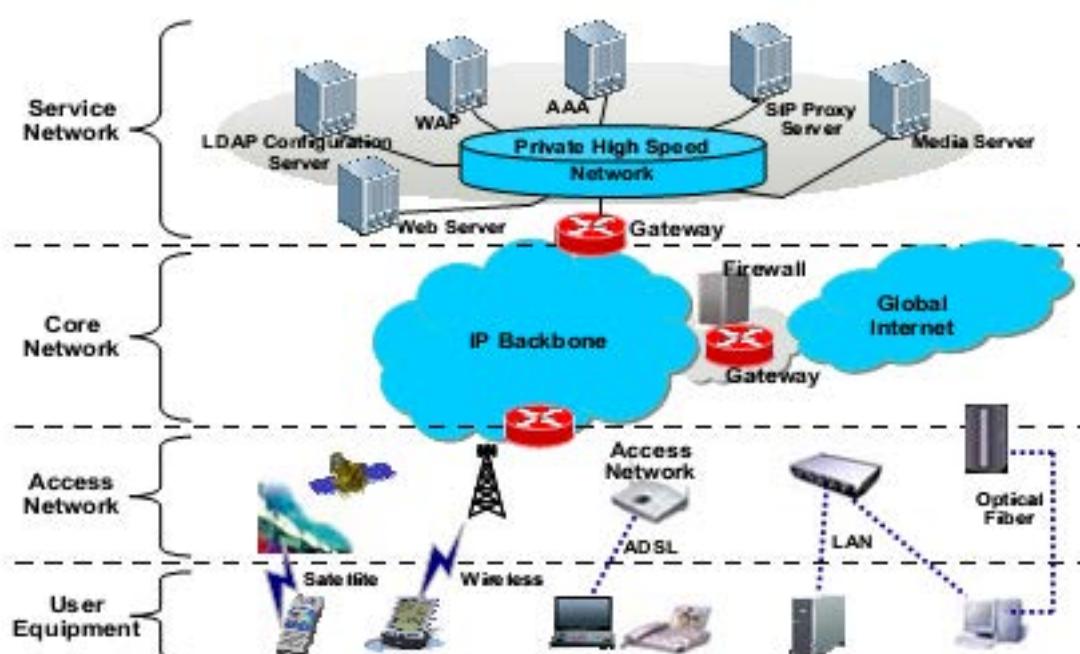
## 249 17 Conclusions

250 Simulation results show that DSDV compared with AODV, DSDV routing protocol consumes more bandwidth,  
251 because of the frequent broadcasting of routing updates. While the AODV is better than DSDV as it doesn't  
252 maintain any routing tables at nodes which results in less overhead and more bandwidth. AODV perform better  
253 under high mobility simulations than DSDV. High mobility results in frequent link failures and the overhead  
254 involved in updating all the nodes with the new routing information as in DSDV is much more than that  
255 involved AODV, where the routes are created as and when required. AODV use on -demand route discovery, but  
256 with different routing mechanics. AODV uses routing tables, one route per destination, and destination sequence  
257 numbers, a mechanism to prevent loops and to determine freshness of routes. <sup>1</sup>



Figure 1: Figure 1 :

1



2

Figure 2: Fig. 2

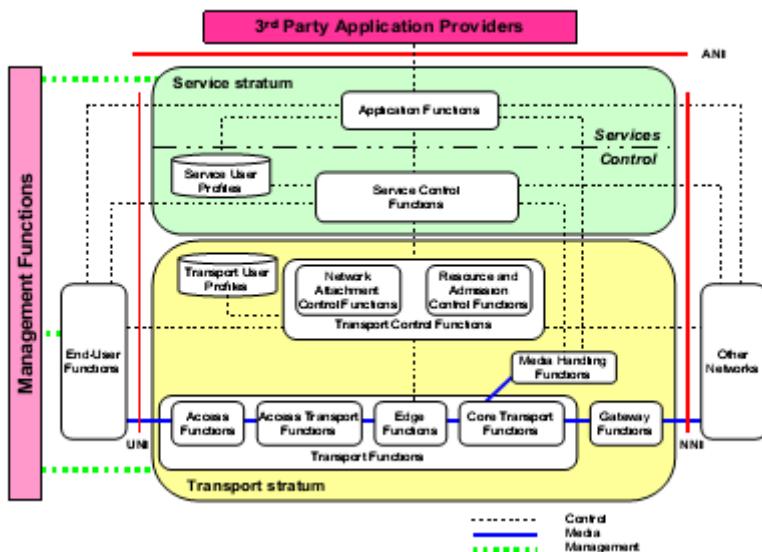


Figure 3: Figure 2 :

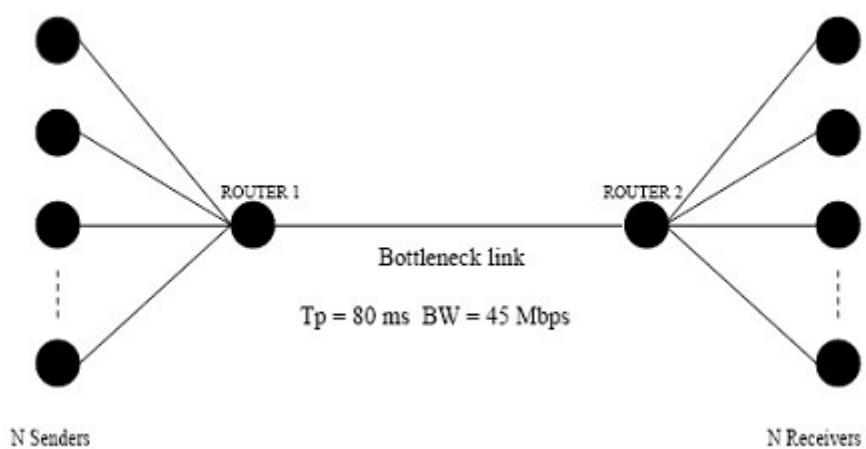


Figure 4: Figure 3 :

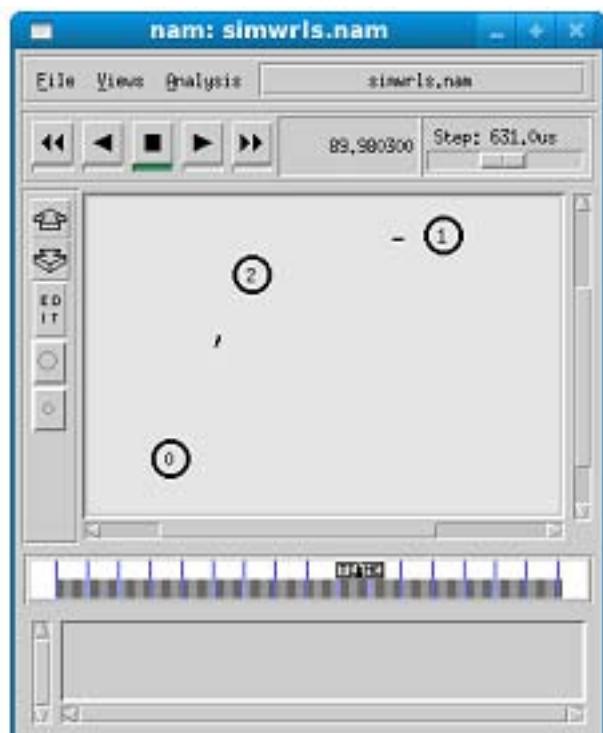


Figure 5: E

$${}_4e(x) = (x + k) \pmod{26}$$

Figure 6: Figure 4 :

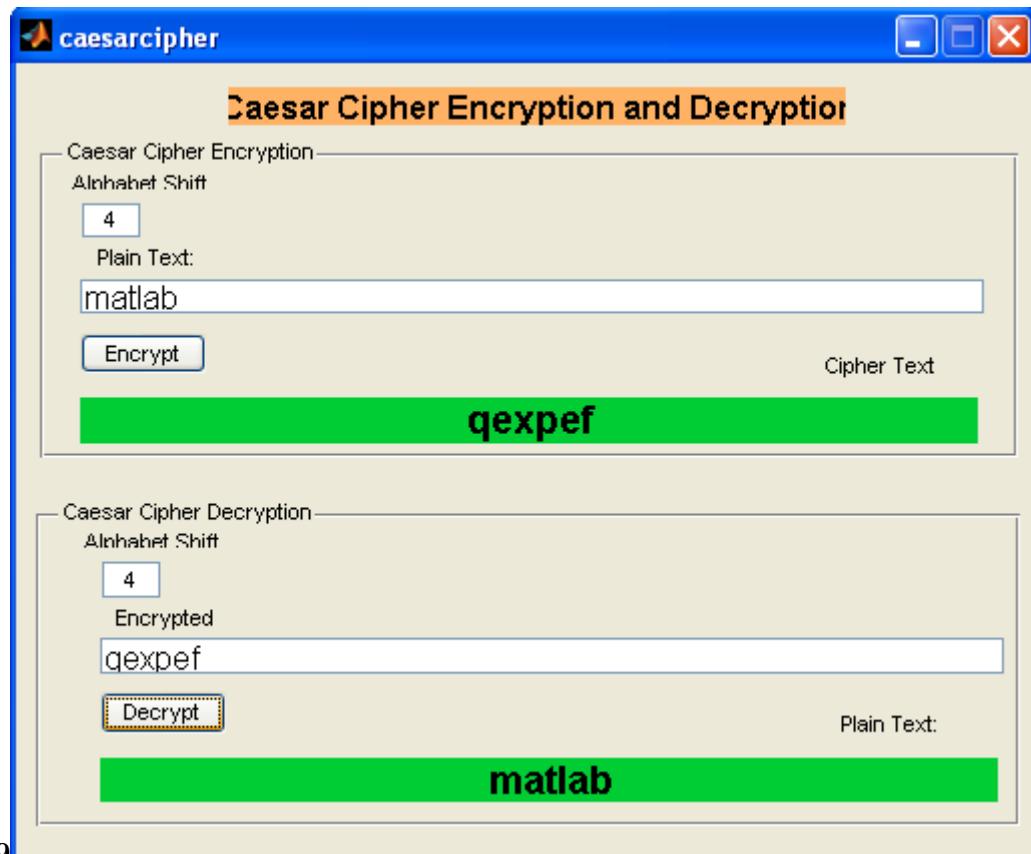
$${}_{56}e(x) = (x - k) \pmod{26}$$

Figure 7: Figure 5 :Figure 6 :



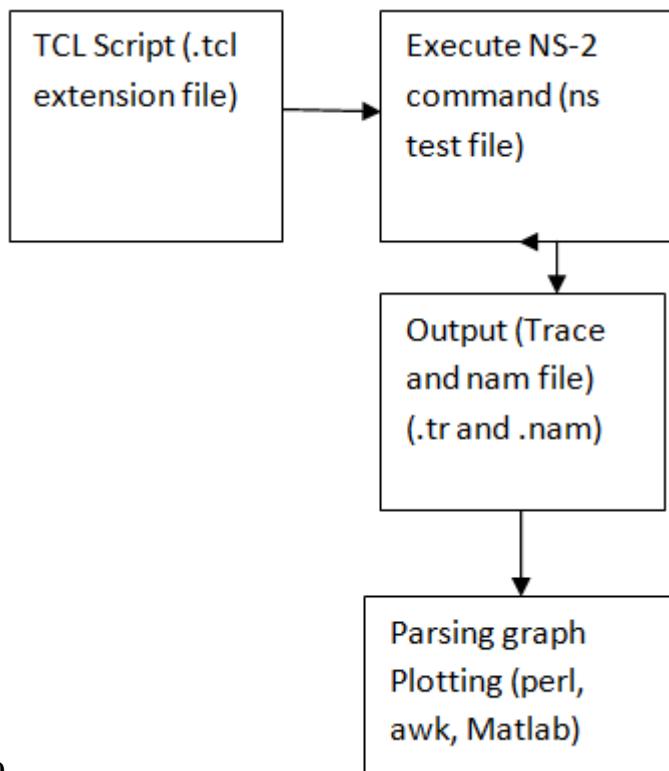
8

Figure 8: Figure 8 :



9

Figure 9: Figure 9 :



10

Figure 10: Figure 10



11

Figure 11: Figure 11 :



Figure 12: Figure 12 :



---

258 [Itu-T (2006)] *Functional requirements and architecture of the NGN*, Itu-T . Sep. 2006. (Recommendation Y.2012)

259 [Itu-T (2001)] *General overview of NGN*, Itu-T . 2001. Dec. 2004.

260 [Itu-T ()] *General principles and general reference model for Next Generation Networks*, Itu-T . 2011. Oct. 2004.

261 [Itu-T (2006)] *Mobility management requirements for NGN*, Itu-T . Nov. 2006. (Recommendation Y.2801)

262 [Li and Sandrasegaran (2005)] ‘Network Management Challenges for Next Generation Networks’. Mo Li ,  
263 Kumbesan Sandrasegaran . *IEEE Conference on Local Computer Networks*, Nov. 2005. p. .

264 [Knight et al. (2005)] ‘NGN architecture: generic principle, functional architecture, and its realization’. Keith  
265 Knight , Thomas Towle , Naotaka Morita . *IEEE Communications Magazine* Oct. 2005. 43 (10) p. .

266 [Itu-T (2006)] *Principles for the Management of the Next Generation Networks*, Itu-T . Mar. 2006. (Recommen-  
267 dation Y.2401)

268 [Itu-T (2006)] *Resource and admission control functions in Next Generation Networks*, Itu-T . Sep. 2006.

269 (Recommendation Y.2111)