Chapter 17
Modern Crypto Systems in Next Generation Networks: Issues and Challenges

Rajashekhar C. Biradar
Reva Institute of Technology and Management, India

Raja Jitendra Nayaka
Reva Institute of Technology and Management, India

ABSTRACT

The performance of Next Generation Networks (NGN) in terms of security, speed, synchronization, latency, and throughput with variable synchronous or asynchronous packet sizes has not been sufficiently addressed in novel crypto systems. Traditional crypto systems such as block and stream ciphers have been studied and implemented for various networks such as wire line and wireless systems. Since NGN comprises of wire line and wireless networks with variable packet-based communication carrying various traffic like multimedia, video, audio, multi conferencing, and a large amount of data transfers at higher speeds. The modern crypto systems suffer with various challenges such as algorithm implementation, variable packet sizes, communication, latency, throughput, key size, key management, and speed. In this chapter, the authors discuss some of the important issues and challenges faced by modern crypto systems in Next Generation Networks (NGN) such as algorithm implementation, speed, throughput and latency in communication, point-to-multipoint, broadcast and key size, remote key management, and communication speed.

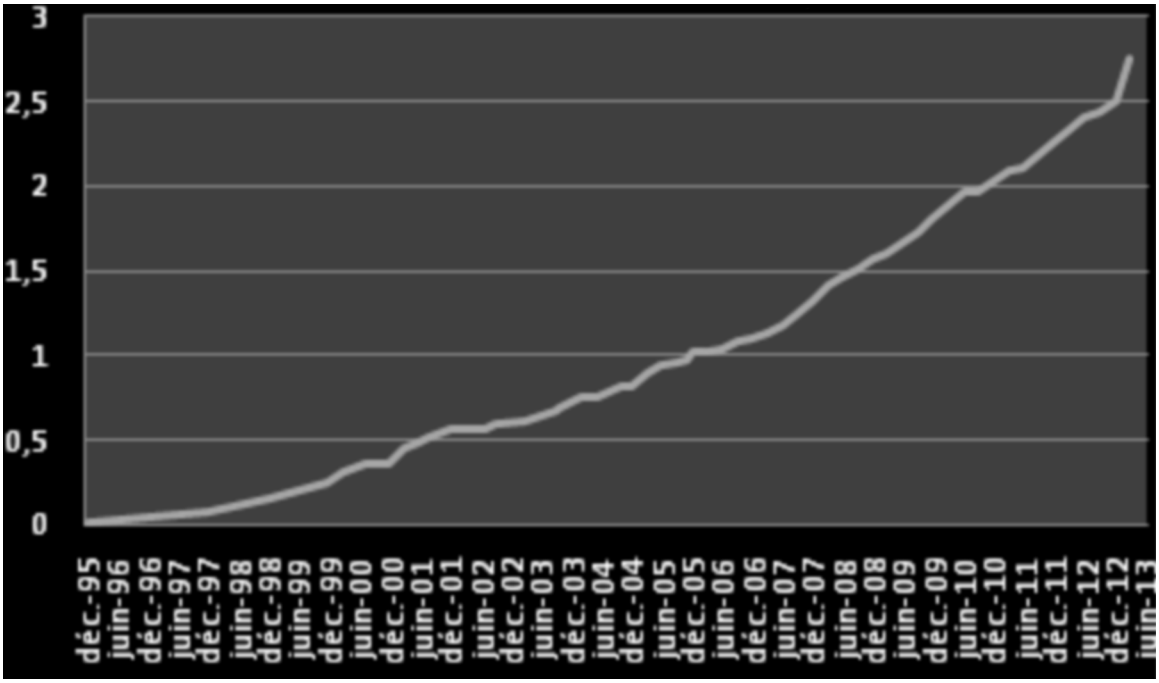
INTRODUCTION

The rising requirement of larger amount of data, video, and cloud computing are driving tremendous demand for faster and more efficient networks is shown in Figure 1 depicts that an NGN includes a packet-based network that can be used for both IP telephony, video, data and support for mobilility. Initially, the term NGN was used to refer to the transformation of the core network to IP (Internet Protocol).

NGNs must live up to the expectations of user and network service provider in terms of speed, trust and privacy. New crypto architectures require more sophisticated protection mechanisms to address various issues in modern applications.

DOI: 10.4018/978-1-4666-6324-4.ch017

Figure 1. Number of internet users (billions) (Courtesy: Sogeti Labs)



The NGN is characterized by the following parameters. (1) Variable packet-based transfer, (2) Support for a wide range of services, applications and mechanisms based on service building blocks such as real time, streaming, non-real time services, multi-media and video conferencing, (3) Broadband capabilities with end-to-end QoS (Quality of Service). (4) Interworking with legacy networks via open interfaces. (5) Generalized mobility issues. (6) Unrestricted access by users to different service providers. (6) Various identification schemes such as IP address for routing in IP networks and (7) converged services between fixed or mobile stations.

Next Generation Networks (NGNs) use high speed wireless devices with variable packet sizes that incorporate 2G/3G/LTE, Wi-Fi, Bluetooth, GPS, wireless sensor networks and other radios. It includes cellular communications, wire line or wireless broadband and other emerging applications as shown in Figure 2.

NGN network supports for a wide range of services, applications and network architectures based on service building and application. NGNs will carry not just traditional conversational services such as voice calls and data transfer but also transactional services like banking and online purchasing, streaming services like watching video-on-demand or IPTV (IP Television) and real-time interactive services such as video conferencing. NGNs must support the QoS demands of the application and it must provide adequate end-to-end bandwidth to consumers, typically several Gigabit NGN Interwork with legacy networks via standard interfaces. Existing telecommunication networks will be required for several years to support legacy services and Customer Premises Equipment (CPE) for consumers to facilitate a measured transition to NGN at interconnect points (Alptekin, 2013). NGNs typically adopt a backward compatibility model using traditional SS7 signaling and TDM at interconnect points. Mobility access to core network services becomes more generalized. It