Chapter 9
Cryptographic Algorithms for Next Generation Wireless Networks Security

Vishnu Suryavanshi
GHRCE Nagpur, India

G. C. Manna
BSNL, India

ABSTRACT

At present a majority of computer and telecommunication systems requires data security when data is transmitted the over next generation network. Data that is transient over an unsecured Next Generation wireless network is always susceptible to being intercepted by anyone within the range of the wireless signal. Hence providing secure communication to keep the user's information and devices safe when connected wirelessly has become one of the major concerns. Quantum cryptography algorithm provides a solution towards absolute communication security over the next generation network by encoding information as polarized photons, which can be sent through the air security issues and services using cryptographic algorithm explained in this chapter.

INTRODUCTION

Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications in next generation wireless network is that of cryptography, which the focus of this chapter is.

DOI: 10.4018/978-1-7998-1763-5.ch009

Security in computer world determines the ability of the system to manage, protect and distribute sensitive information (Abdel-Karim R. Al Tamimi 2006). The most attractive and fast growing network is 802.11 in wireless networks. In 1997IEEE 802.11 introduced standards for wireless local network (WLAN) communication, some of these standards are:

- Using the 2.4 GHz radio spectrum and 11 Mbps max data rate is 802.11b.
- Using the 5 GHz radio spectrum and 54 Mbps max data rate is 802.11a.
- Using the 2.4 GHz radio spectrum and 54 Mbps max data rate is 802.11g.

Wireless Robust Security Network is 802.11i (Quality of service). It is used in quality of service for traffic prioritization to give delay sensitive application such as multimedia and voice communication priority(SANS, 2005).Next generation wireless technology 3G, 4G and more has been gaining rapid popularity in recent years.

They have ubiquitous wireless communications and services as Integration of multi-networks is using IP technology; similar technology to the wired Internet where users are freed from their local networks, not just IP end-to-end but over-the-air packet switching, high bandwidth / high-speed wireless and highly compatible with wired network infrastructures like ATM, IP.

These technologies are facing security problems in the software products used to access the vast Internet, operating systems, www browsers and e-mail programs(Chandra, et al., 2008).For secure data transformation cryptographic algorithms plays a key role.

A cryptographic technique provides three forms of security namely confidentiality, data integrity and authentication. Confidentiality refers to protection of information from unauthorized access (Daemean & Rijmen, 1999). Information has not been manipulated in any unauthorized way is ensured by data integrity. Authentication can be explained in two groups as entity authentication and message authentication. Detecting any modifications to the message provides message authentication. Entity authentication assures the receiver of a message, about both the identity of the sender and his active participation (Kumar & Purohit, 2010)

Need of a standard depends on the ease of use and level of security which it provides. Here, the distinction between wireless usage and security standards show that the security is not maintained well up to with the growth past of end user's usage. The hackers monitor and even change the integrity of transmitted data in current wireless technology. Lack of rigid security standards has caused companies to invest millions on securing their wireless networks.

Securing Next Generation Wireless Networks is an extremely challenging and interesting area of research. Unprotected wireless networks are vulnerable to several security attacks including eavesdropping and jamming that have no counterpart in wired networks. Moreover, many wireless devices are resource limited, which makes it challenging to implement security protocols and mechanisms.

The main objective of this chapter to study and analyze use of Cryptographic Algorithms for Next Generation wireless networks Security in terms confidentiality, Confidentiality, Integrity, Availability, Anti-virus, anti-spyware software, firewall, Authentication, Access control, and Cryptanalysis.