Chapter 10
Efficient Energy Saving Cryptographic Techniques with Software Solution in Wireless Network

Alka Prasad Sawlikar
RCERT Chandrapur, India

Zafar Jawed Khan
RCERT Chandrapur, India

Sudhir Gangadharrao Akojwar
Government College of Engineering, India

ABSTRACT

To reduce communication costs, to protect our data from eavesdropping and from unauthorized users, cryptographic algorithms are used. Cryptographic module has to be developed for combining the operation of compression and encryption synchronously on the file. The information file is preliminary processed and then converts into one intermediary form so that it can be compressed with better efficiency and security. In this paper an optimized approaching coding technique which deals with both the issues of size and security is introduced and characterized experimentally using the performance measurement approach java in which file of any data length can be practically compressed and encrypted using new encryption technique and a novel energy saving technique in wireless communication network with efficient hardware solution is presented. To improve the strength and capability of algorithms and to compress the transmitted data an intelligent and reversible conversion technique is applied.

DOI: 10.4018/978-1-7998-1763-5.ch010

INTRODUCTION

From last consecutive years we have seen an unrivalled explosion in the amount of information or text data which is transmitted via many digital devices and for reducing the traffic, there is a need of strong cryptographic techniques so that large amount of information can be transmitted. For this a number of novel compression algorithms have been proposed earlier such as LZW, RLE, DWT, DCT and HUFFMAN. However, few of the above algorithms have been able to achieve best compression ratio.

Advantage of security is to ensure that our information remains confidential and only access by authorized user and ensure that no one has been able to change that one, so it provide full accuracy. Compression is used to compress and secure the data, because it uses less space and saves money. It increases speed of data transfer from disk to memory. Requirements for data security are confidentiality, authentication, integrity and freshness. It involves transforming data of a given frame, called source message to data of a reduced sized frame called code word.

There are different security techniques which are existing like AES, DES, ECC, RSA. Cryptography is valuable for protecting sensitive data online, especially in a world in which an increasing more systems are connected and unsafe to outside attack. It is also a valuable tool for authentication, allowing a user to verify his identity and statements using a public key encryption system. The main advantage of cryptography is as a security tool. Because any system connected wirelessly is bound to eventually be attacked by adversary, and it can be extremely tough to create a system that is invulnerable to outsiders. However, the mathematical analysis involved in encryption is complex enough that even if enemies manage to steal an encrypted file; he may never be able to break the code and access the contents. Strong encryption can be a last line of defense against outsiders, and can protect data even when it is being transferred through a connection that is not secure.

The public and private keys associated with public key cryptography which offers unique advantages to their users like if a user encrypts data with his private key, anyone can get original intelligent data with his public key, verifying that he and only he could have sent the transmission. A public key can also encode data that only that specific user can decode, creating secure one-way communications on the Internet.

Currently compression and encryption methods are doing simultaneously. Combination of two processes into one provides more security by this hybridization.

While combining both compression and encryption data will be first compressed using compression techniques and then encryption techniques will applied and then comparative analysis will be done. If encryption and compression are done at the same time then it takes less processing time and more speed.

Security of information is always been in demand since past few years and plenty of occurrences highlight the importance of the security of text data. As it is known, cryptography is a skill of hiding data and has been known from a long time, e.g. credit cards, debit cards, saving accounts, important documents and what not, everything needs protection. The most principal issue in world today is the large amount of valuable information that is flowing among various networks and present network development demands swap of information with more compression and security in both the time and space for data transmission for data storage (Jain, Lakhtaria, & Srivastav, 2013). This can be done by compression and encryption, such type of scheme is known as encryption compression crypto scheme. This ciphering or encryption is indeed a secure coding technique, whose purpose is to reduce the space for data storage and