50153 Abdul Samiah

1. Secure Framework for Wireless LAN by Using AES-CCMP

Abstract

The Advanced Encryption Standard (AES) is computationally intensive and is infeasible to implement for replacing WEP, which is an often-used wireless security protocol that is relatively insecure over 802.11b networks. The reason is low processing power and storage capability of current hardware because AES has a number of repeated XOR and mathematical operations.

The software implementation of AES for CCMP protocol developed in this thesis makes it computationally feasible to implement AES over 802.11b networks and for replacing currently used WEP by upgrading its firmware. The aim of this implementation is to provide a better solution to secure data, which was not possible by using WEP. IEEE 802.11i task group recommended series of fixes for WEP to accommodate legacy products [1]. As legacy products cannot support AES upgrade due to their design limitations, the task group suggested development of new hardware/software solutions.

Hardware implementations of AES are based on FPGA or embedded processing techniques that off-load the encryption from main processor of WLAN adapter [3]. Existing software implementations of AES are based on modes of operations such as ECB, OCB and Counter Mode [2]. The software implementation done in this thesis is based on CCMP mode. This software implementation provides fast, simple to understand, cheaper, and easy to adopt method for computing AES with CCMP protocol with high throughput. The software for this implementation is designed in C/C++ and is compiled in Dev-C++4.9.9.1 compiler. Pentium IV @ 3.20 GHz with operating system of Windows XP is used as a processing platform.

Our software implementation uses pointers, structures and unions for programming in C. Use of pointers for saving, assigning, and also releasing memory space helps in making the best use of the available memory space. Two-dimensional and multi dimensional array representation also become easy with pointers.

Results obtained through this implementation provide better throughput and execution times as compare to other software implementations [4]. For feature work this implementation can be used for WLAN cards by upgrading existing firmware with suitable driver to support it.