ABSTRACT

Wireless communication is an essential technique in modern communication methods. People want to be connected with various networks even while they are on move.

The interconnection of devices wirelessly is known as wireless networks. Wireless Local Area Networks [WLAN], mobile phones, Wireless Sensor Networks [WSN] and Bluetooth are few examples of wireless networks which are being used world wide.

Wireless networks connect people on the move. It’s easier and cost effective. The complexity of running wire throughout the network is removed in wireless networks. But they face few problems also. The initial installation cost is high. A proper survey of the region is to be carried out before installation. More than that wireless networks are more vulnerable compared to their wired counterpart. Security of wireless networks is a serious issue which can affect confidentiality and integrity of the organization where wireless network is employed.

Efforts are made to improve security of wireless networks. Switching off Service set identifier [SSID], Filtering Medium Access Control [MAC] address, employing encryption techniques are few methods adapted in WLAN to improve security.

In this proposed work, the following security enhancement techniques of WLAN are presented.

i. Gain optimized micro strip yagi array is designed and tested for improved gain.
ii. Wearable antenna is designed to implement as WLAN AP.
iii. Implementation of gain optimized yagi antenna as sector antenna to restrict signal within the intended region.
iv. Reconfigurable yagi array is designed and tested to control signal within the required region.
v. Scanning based encryption algorithm has been implemented for WLAN signal transmission

vi. Two factor Biometric key namely ‘hybrid’ is generated to use as the key in Advanced Encryption Standard [AES] of WLAN.

Access points of WLAN have omni-directional antenna which radiates equally in all directions. As most of the buildings are in rectangle shape, even though antennas are placed at the center of the building, the radiated signal leaks out of the required region. When signal is available to outside persons, they can easily get into the network. If it is possible to restrict the signal within the required region, most of the intrusion can be avoided.

Directional antennas can be used in AP. They can radiate signal in a particular direction. These antennas can also be known as sector antennas. A method is proposed to have better directional antennas with which security can be improved.

Yagi antenna is considered to be a simple but highly efficient directional antenna. But conventional yagi antenna has side lobes and back lobes along with main lobe in forward direction. The side lobe and back lobe can be reduced by optimizing dimension of yagi antenna. The optimization is carried out by genetic algorithm concept. By employing optimized yagi array, better gain is obtained at the expense of minor lobes. Modern antennas are made up of micro strip form to have compact antennas. A gain optimized micro strip yagi array is formed and the results are compared with conventional micro strip yagi array. Return loss and Voltage standing wave ratio [VSWR] are improved with optimized array which indicates better gain. As side lobes are reduced, energy leakage in unwanted directions is avoided which in turn avoid intrusion into the network. Gain optimized yagi array is used as sector antenna.

WLAN antennas can also be fabricated with wearable materials. Instead of conventional substrate materials, cloth materials such as cotton, Jeans are used to construct antenna.
This antenna can be placed at curtains of windows, walls and roof. A dual band wearable antenna which operates at 2.4 GHz and 0.9 GHz is designed. The gain optimized yagi structure can also be fabricated as wearable antenna.

A combination of three such sector antennas each covering 120 degrees each, is placed at the center of the roof of the building. A similar set of three antennas is placed at inner walls facing inwards. Data which is to be transmitted in split up into two parts. Each part is transmitted by one antenna set. An eligible user is expected to be associated with both Antennas at the same time. As intruders cannot get the signal from both antennas, it is highly difficult for them to receive data.

Another proposed technique is the implementation of Reconfigurable Yagi antenna. Reconfigurable antennas generally switch between two different frequencies. In this technique, reconfigurable antenna operates at 2.4 GHz but the switches are placed at directors to modify the gain of the antenna. At the walls of the building, a signal monitoring unit is placed. It monitors signal level continuously against a threshold value. The threshold value is fixed such that if signal level exceeds, intruders can recognize signal from outside. If signal exceeds threshold value, few switches are opened so that directors become piece of elements which do not work as a part of yagi antenna. The gain of over all antenna system is reduced. If signal is low compared with threshold, few switches are closed so that additional directors are formed. The gain of antenna is increased. In this way, signal level at the wall can be controlled and intrusion can be avoided. Signal is also made available to all eligible users within the building.

Scanning is a basic concept of television. In scanning, the signal is available during trace period and during retrace period, signal is off. This concept is used in transmitting signal in WLAN. The encryption is also done during the trace period. An algorithm is devised to communicate in WLAN using the above mentioned technique.

Police department uses finger print to find culprits. As biometric features are unique, they are used for identification purposes. It is possible to generate cryptographic keys from
biometric features which are also unique. These keys can be applied in encryption algorithm such as Advanced Encryption Standard [AES]. But it is possible to duplicate biometric features which may harm this technique. A method is proposed to overcome this drawback. Bio-keys are generated from face and finger print. These bio-keys are then combined based on certain algorithm to generate cryptographic key which is used to encrypt communication in WLAN. Duplication may not be possible for two biometric features. As the bio-keys are combined with certain algorithm, it is difficult to trace the cryptographic key. In this technique, secured communication in WLAN is possible.

In this work, security enhancing techniques of WLAN with gain optimized sector antennas, reconfigurable antennas, scanning based algorithms and cryptographic key generation from two biometric features are presented.