Visvesvaraya Technological University

BELGAUM, KARNATAKA - 590 014.

PROJECT REPORT

ON

"AN INTRUSION DETECTION AND PREVENTION SYSTEM FOR IMS AND VoIP SERVICES"

Submitted By

MANASA M	[4PM10CS047]
MONIKA C SHETTY	[4PM10CS054]
NANDHA H O	[4PM10CS058]
NAVAMI R	[4PM10CS060]

Submitted in partial fulfillment of the requirement for the award of degree of

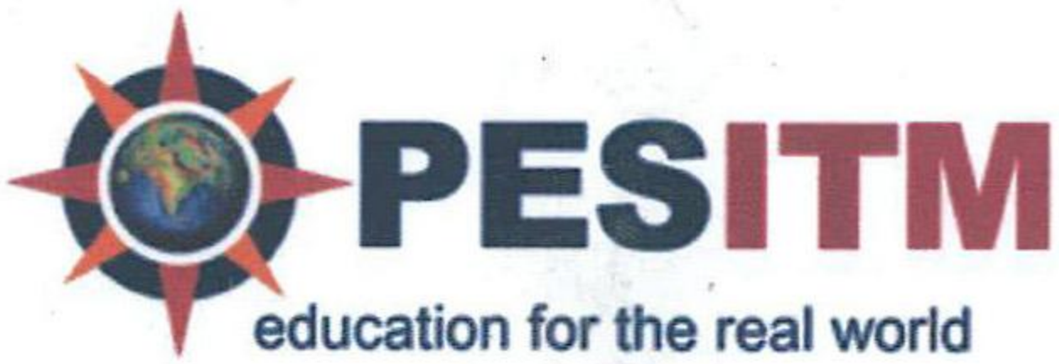
BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

Under the Guidance
of

Mr. CHETHAN L S. BE, M.Tech,
Asst. Prof., Dept. of CS & E.
PESITM, Shivamogga



PES Institute of Technology and Management

Department of Computer Science & Engineering

June-2014

CHAPTER 1

INTRODUCTION

The wireless transmission medium, adversaries can monitor any transmission. In various types of attacks, identity based spoofing attacks are especially easy to launch and can cause significant damage to network performance. In 802.11 networks, it is easy for an attacker to gather useful MAC address information during passive monitoring and then modify its MAC address by simply issuing an ifconfig command to masquerade as another device. In spite of existing 802.11 security techniques including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA),or 802.11i (WPA2), such methodology can only protect data frames - an attacker can still spoof management or control frames to cause significant impact on networks.

A wireless sensor network (WSN)[6] of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting . A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.