# Chapter 1
# Wireless Mesh Network Security, Architecture, and Protocols

**Sachin Kumar Gupta**
*Shri Mata Vaishno Devi University, India*

**Aabid Rashid Wani**
*Shri Mata Vaishno Devi University, India*

**Santosh Kumar**
https://orcid.org/0000-0003-2264-9014
*Department of Computer Science and Engineering, Dr. SPM IIIT Naya Raipur, Chhattisgarh, India*

**Ashutosh Srivastava**
*RST Ecoenergy Private Limited, Mirzapur, India*

**Diwankshi Sharma**
*Shri Mata Vaishno Devi University, India*

## ABSTRACT

*Due to suppression of central administration in WMN, network functioning like network controls, management, routing, switching, packet forwarding etc. are distributed among nodes, either collectively or individually. So, cooperation among nodes is highly solicited. However, there may exist node's malicious activities because of its open characteristics and limited available battery power. The nodes may misbehave by refusing to provide service or dropping down the packets because of its selfishness and malicious activity. The identification of misbehaving nodes and prevention from them can be one of the biggest challenges. Hence, the prime target of the chapter is to provide an overview of existing intrusion detection and prevention approaches,*

DOI: 10.4018/978-1-7998-0373-7.ch001

*and secure routing or framework that can recognize and prevent from the malicious activities. The digital signature-based IDS to offer secure acknowledgment and an authentication mechanism has also been discussed. The expectation is the digital signature-based IDS will overcome the weakness of existing IDS.*

## INTRODUCTION

The revolution in communication technology has made the life of a common person too much easy. Because of this revolution, a lot of fields came into the market. For example, the wireless connectivity of mobile users all over the world, the real-time communications, internet of things (IoT), etc. These modern facilities are only due to the technologies like internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc. Among all these revolutionary technologies, the most important wireless technology named Wireless Mesh Networks (WMNs) that provide facilities to the great extent in day to day life of common person. The facilities are in terms of implementations like_Private, local, campus, urban regions, etc. The cause behind these applications is the nature of nodes using in deploying wireless mesh networks. As these nodes are dynamic, self-organized, self-configurable, self-healing, low-cost, easy maintenance. Among these characteristics of nodes deployed for establishing WMNs, the dynamic topology and the multi-hop nature leads WMNs vulnerabilities to security attacks. So, the network should consider security issues like authenticity of network traffic (free from masquerading of nodes), non- repudiation, authorization among users, anonymity, access control and secure routing etc. These security issues in WMNs can be achieved with some important key management schemes. These include intrusion prevention (Offense against fraudulent nodes, as well as for authentication and encryption), intrusion detection (Ideal for preventing the invasion or reducing the harm), and intrusion responses. Hence, the security-based WMNs overcome the threats from external or internal intruders (attackers) (Sgora et al., 2016).

It has been come for the long time that wireless networks should be developed and deployed efficiently. The necessity of efficient development and deployment was to fulfil our application requirements. That is the requirements needed for each application like throughput, wait time, memory, safety etc. must be e0ncountered. So, the researchers always remain behind to create new dedicated wireless technologies and standards. Keeping in mind that these technologies should met our above application requirements. Due to which number of modern technologies took birth viz IEEE 802.11(Wi Fi), IEEE 802.15 (including Bluetooth and ZigBee), and IEEE 802.16 (WiMAX). These technologies were so much important due to their affordable capabilities and wireless mesh capacities.