



**INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS**

Name of the Student : Mayank Agarwal
Roll Number : 10610109
Programme of Study : Ph.D.
Thesis Title : Intrusion Detection System for Attacks in 802.11 Wi-Fi Networks: A Discrete Event System Approach
Name of Thesis Supervisor(s) : Dr. Santosh Biswas & Prof. Sukumar Nandi
Thesis Submitted to the Department : CSE
Date of completion of Thesis Viva-Voce Exam : 12th May 2017
Key words for description of Thesis Work : IDS, DES Modeling, Wi-Fi vulnerability, security attacks, MAC Layer

SHORT ABSTRACT

Wireless Fidelity (Wi-Fi) networks has brought about a paradigm shift in the area of communication but has also opened doors for malicious users to launch a variety of security attacks on these networks. In the first contribution of this thesis, we propose an Intrusion Detection System (IDS) for detecting evil twin attack in Wi-Fi network. In the second contribution of this thesis, we propose a novel insider attack termed as 'Advanced Stealth Man-in-the-Middle (ASMiTM)' attack which enables an attacker to launch a Man-in-the-Middle attack in WPA2 encrypted Wi-Fi network. We also propose an IDS for detecting the proposed ASMiTM attack. In the third contribution of this thesis, we propose an IDS for detecting Power Save DoS (PS-DoS) attack in Wi-Fi network. In the final contribution of this thesis, we propose an IDS for detecting rogue DHCP server attack in Wi-Fi network. All of the proposed IDSs are developed using the Failure Detection and Diagnosis (FDD) theory of Discrete Event System (DES). Developing of the proposed IDSs using the DES framework helps to prove the correctness and completeness of the IDS which ensures that the attacker does not escape detection under any circumstances. In addition, the IDSs proposed for the above attacks do not require any sort of protocol modifications, encryptions, certificate management etc., and can be readily deployed on both legacy as well as modern network.