IEEE 802.11 WLAN is very susceptible to many security threats. Among the many attacks which can be launched on WLAN, Denial-of-Service (DoS) attack is the most severe one causing more damage. The main goal of DoS attacks is to prevent legitimate users from accessing network resources, services, and information. This attack can be caused by flooding other wireless clients with bogus packets creating a denial of service of these clients.

An 802.11 station (STA) must first authenticate and then associate itself with an access point (AP) before starting the communication. In deauthentication or disassociation attack, huge amounts of fake deauthentication or disassociation requests will be sent to the access point (AP) by the attackers. The other type of attack is authentication and association attack in which a burst of fake association and authentication request frames are sent by the attackers leading to exhaustion of APs.

Existing Game Inspired Defense Architecture (GIDA) module reduces the DoS attacks in TCP-friendly flows. But there is no framework that has been suggested to provide complete solution to defend against all these DDoS attacks in IEEE 802.11 WLAN.

In this thesis, a secure framework for DDoS detection and defense for IEEE 802.11 WLAN is proposed. The framework describes the solution for three attacks. UDP flooding attack is detected using the game theory decision model by analyzing the traffic flows. Using a Master Session Key (MSK), hash function is generated. For the authentication and association attacks, client puzzle based defense mechanism is used in the AP. The client solves a puzzle which has been send by the AP. The puzzle can be protected by means of hash function and easily adjusted by the AP. De-
authentication or disassociation attacks on AP can be protected by the random bit authentication mechanism that inserts the current 3-bit unit into the unused bit positions of each frame, and then advances the index to point to the next unit. The respective frames can be protected by the hash function and master session key.

Accurately detecting and avoiding DDoS attack in IEEE 802.11 WLAN is challenging since the detection techniques may involve lot of false positives. Fuzzy based DDoS attack mitigation technique is proposed for reducing the false positives in WLAN. The traffic level (TL) is categorized into green, red and black based on the two thresholds T1 and T2. In the adaptive response technique, the Confidence of Attack (CoA) and Network Performance Degradation (NPD) are measured. In DDoS avoidance technique, fuzzy logic decision model is applied. The TL, CoA and NPD metrics are submitted as input to the fuzzy logic model and fuzzy decision rules are formed. Based on the outcome of the rules, response action is taken which includes punishing and isolation of attackers, recovery of service from victim nodes etc.

The performance of the proposed framework is compared with existing techniques based on the metrics delay, average packet delivery ratio and packet drop for the Constant Bit rate (CBR) and TCP traffic flows. NS-2 simulation result shows that the proposed framework provides reduced delay, higher delivery ratio and lesser packet drops when compared to the existing techniques.