The increase in capacity and system data rate may lead to capacity problems and hence become one of the crucial issues in any Mobile Communication Networks. Although the Long Term Evolution (LTE) is called the 4th Generation of the Mobile Cellular Communication Network, it can no longer solve the problem regarding the capacity of the cell. In order to cope with the increase in demand for stable and high data rates among mobile users, femtocell or Home Evolve Node B (HeNB) has been developed to improve indoor capacity and coverage. Deploying femtocells in macrocell are one of the efficient ways to improve the performance of mobile services in high traffic congested areas. Deploying femtocells in macrocell are one of the efficient ways to improve the performance of mobile services in high traffic congested areas. Femtocell is a small and lightweight base station that aims for indoor usage such as at home or in an enterprise and provide better user experiences to users. However, femtocell deployments caused interference between femtocells itself and also to the existing macrocells. This thesis studied the two combining interference methods in LTE Heterogeneous Networks (HetNets) in order to reduce interference in HetNets which is the Fractional Frequency Reuse (FFR) and Dynamic Power Control (DPC) methods. The FFR method highlights the significance of two parameters which are the fraction of radius in center region (rth) as well as the fraction of the system bandwidth (β) allocated for the center area while the DPC method highlights the importance of the parameter Path Loss (PL) compensation factor (α). This thesis proposed a new hybrid mathematical model for interference management by identifying the effect of rth, β and α on the improvements value of capacity, throughput as well as the Signal to Interference plus Noise ratio (SINR). The proposed rth, β and α value were then used in simulation model by using the MATLAB software to analyze the number of handovers occurred for the proposed method and comparing its performance improvement with the conventional method. The simulation results showed that the proposed method give higher values of the macrocell and femtocell SINR by 135.71% and 50.54% respectively. It showed that there was a significant reduction the inter-cell interference in LTE HetNets by offloading the macrocells traffic to the femtocells and higher load balancing performance can be achieved and hence reducing the number of handovers.

Recently, BYOD or Bring Your Own Device has become one of the most popular methods for enterprises to provide mobility and flexibility in workplaces. The emergence of new technologies and features of mobile devices makes them integral part of every aspect of daily business activities. On the other hand, mobile devices are not well protected compared to computers and their users pay less attention to security updates and solutions, therefore, these new capabilities (e.g. high internet speed and processing power) have motivated the attackers to migrate to mobile infrastructures. Thus, mobile security has become a crucial issue in BYOD or Bring Your Own Device as the employees use their own mobile devices to access an organization data and systems. The mobile attacks and threats come in different forms, such as viruses and worms. However, Mobile Botnets or MoBots are more dangerous as they pose serious threats to mobile devices and communication networks. Bot and Botnets are sophisticated form of organized cyber-crime, which infect different targets (e.g. computers or mobile devices) without attracting the users’ attention, which subsequently communicates with each other by using a Command and Control (C&C) mechanism. The main intention of Botnets is to steal the private and personal information (e.g. Zeus and Zitmo) or sensitive information of organizations (e.g. Flame and Stuxnet), thus, several techniques such as encryption and use of standard protocols (e.g. HTTP and Port 80) employed by Botmasters to develop foolproof C&C mechanism which are difficult to detect. For instance, the AnserverBot, DroidDream, Geinimi, and DroidKungFu are the real world examples of mobile Botnets that use HTTP protocol to hide their activities amongst normal web traffic and stealthily communicate with C&C servers. In fact, Botmasters configure the Bots with regular interval to periodically visit a certain websites contains their updated instructions. Although the periodic behavior of HTTP Bots has been significantly used as a detection measure, most of current studies can detect Bots with fixed interval only. This research proposed a decision tree based model to identify the level of periodicity of HTTP and WEB activities in order to classify them into several categories such as Non-periodic, Periodic, Weak Periodic, Uniform Periodic and Strong periodic. Based on the literature this is the first reported use of classification to categorize the periodic C&C traffic. The results show that the proposed model is able to classify the communication patterns with 95% accuracy and very low rate of false positive of 1.2 % only. However, the level of periodicity alone is not a sufficient factor to detect mobile HTTP Botnets as there are numbers of normal applications such Gmail session, auto refresh pages, and etc. that may pose the same periodic pattern as Botnets. Thus, in addition to this model, a cooperative model using feed forward neural network is also proposed to look for any evidence of mobile Botnet activities. The proposed cooperative detection model is significantly able to detect the mobile HTTP Botnets with 97.8 % of accuracy and 0.5% false positive only.