Songrit Srilasak 2009: Rogue Access Point Detection and Counterattack System. Master of Engineering (Computer Engineering), Major Field: Computer Engineering, Department of Computer Engineering. Thesis Advisor: Associate Professor Anan Phonphoem, Ph.D. 85 pages.

Normally a user can access an internal server via wireless LAN with some restriction due to the organization security policy. The user may intentionally install an unregistered access point without administrative awareness for his or her convenient which causes backdoors for eavesdrop or attack from the intruders. The rouge access point may also be installed by the intruder himself without connected to the organization's network.

In this thesis, the rouge access point detection and counterattack system has been proposed. The system is designed as a centralize control by utilizing the existing registered access points to capture the broadcasting data, e.g. the identity of the access point, according to the IEEE802.11 standard. The captured data is then sent to the central server for analysis. If the received data does not match with the registered access point, the system sends control commands to the edge switch for shutting down the port that the unregistered access point is connected to. From the experiment, 4 types of unauthorized access point, both inside and outside the organization, can be correctly detected while the system is able to automatically block the internal rouge access point.

_____ _____ ___ / ___ / ___

Student's signature Thesis Advisor's signature