Project proposal

Project title	Explorations on Data Mining Techniques for Wi-Fi Intrusion Detection
First Supervisor	Dr — Dimitris Tsaptsinos
Second Supervisor	tbc
School	Computing and Information Systems
Other member of supervisory team (no more than three KU supervisors in total)	
Specific requirements beyond 2:1 degree	

Project summary

(max 4,000 characters)

MSc by Research

Intrusion detection in wireless networks is a vital aspect in wireless security systems. Existing reported work, employing data mining techniques, has concentrated in the area of wired networks and less scientific papers in comparison have appeared for wireless. The objective of the study is to learn the lessons from the work already undertaken for wired network intrusion, identify the issues that discriminate wired and wireless, to select an appropriate data mining approach and through the use of controlled experiments to evaluate and analyse the results when employed for a wireless network.
This study is of importance when considering that a given Intrusion Detection System (IDS) monitors computer network traffic and raises a vast amount of “alarms” when a security violation is taking place. Such “alarms” need to be analysed by the security analyst whom decides if this corresponds to a real or a false threat. The target of data mining techniques is to find patterns in large data sets for better understanding of existing data. Understanding of data refers to the classification of a particular “alarm” to a particular category. Classification models employed in the past include decision tree methods, linear discriminators and density estimators. The main research question of this proposal is: “Can we minimize the alarms that the human security analyst has to attend on a daily basis?”