# ABSTRACT

Internet of things (IoT) is an emerging topic of so many aspects nowadays. It has so many positive effects for daily routine. The integration between devices and human itself currently in large scale development. Such devices can detects heartbeat, body status, processing calculation of health in short time, etc. With the continuous development and application of the IoT, the hidden problems such as security aspects become one of the considerations.

Security aspect is one of many aspects which should be concerned in internet of things area which has massive connectivity. Furthermore the limited power and computational capability of the majority devices in the system makes it more challenging to develop other than another aspect in the system. Therefore, the needs of reliable and effective security system through the networks is highly needed. Intrusion detection system (IDS) may be one of the solution that can be applied to the system in order to solve this problem. But in such large network scale condition such as IoT, standalone IDS may have to work very hard in carrying out their duties and of course it could affect the performance too. It can be resolved with having standalone IDS implemented in high processing computer, but again, the majority of the problem that consist in IoT network security is the device limited processing power and tight energy restrictions.

In this thesis, the system was built using JADE agent-based modeling to simulate the condition which resemblance the real one. The system consist of 3 type of agents which represents 3 parts of the real environment which is IoT server, controller, and node. In order to get the intrusion detection result, 4 algorithm were used and distributed randomly on system. Also K-Means clustering were used to help the distribution of agents. Then the performance evaluation were done on the system. Several parameters such as cost-loss expectation, energy consumption, and metric of IDS efficiency were used in order to measure how the system perform. The results are reports given by IoT controller were decreased until $\sim 80\%$. Besides that, according to metric of IDS efficiency, the value of most IDS reach $\sim 1$ which means nearly perfect. Despite of the non-perfect result, the objective of the research have been achieved.

**Keywords**: Internet of Things, IoT, Collaborative Intrusion Detection System, Multi-hop Clustering, Network Security