UNIVERSITI TEKNOLOGI MARA

# INTEGRATED COMBINED LAYER ALGORITHM OF JAMMING DETECTION AND CLASSIFICATION IN MANET

**AHMAD YUSRI BIN DAK**

Thesis submitted in fulfillment
of the requirements for the degree of
**Doctor of Philosophy**
**(Science Quantitatif)**

**Faculty of Computer and Mathematical Sciences**

**April 2019**

# AUTHOR'S DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the results of my own work, unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

| | | |
|---|---|---|
| Name of Student | : | Ahmad Yusri Bin Dak |
| Student I.D. No. | : | 2010383363 |
| Programme | : | Doctor of Philosophy |
| Faculty | : | Computer and Mathematical Sciences |
| Thesis Title | : | Integrated Combined Layer Algorithm of Jamming Detection ahd Classification in MANET |

| | | |
|---|---|---|
| Signature of Student | : | |
| Date | : | April 2019 |

# ABSTRACT

The latest technologies in Mobile Ad-Hoc Network (MANET) allows networking infrastructure to be set up quickly and easily. Every node in MANET plays a role as a router that creates remote network access regardless of time or location. As such, the dynamic nature of the infrastructure opens MANET to being vulnerable to jamming attacks. A study found that eighty one percent of attacks occurs at the physical and MAC layers of the protocol stack. This happened due to inadequate guidelines using standard parameters to detect jamming attacks. In addition, the use of techniques such as watchdogs, routing and databases cannot solve problems which is detecting an important layer thoroughly, lack of parameters in the database and failure to detect some important jammers due to limited jammer detection methods. Therefore, knowing the types and characteristics of jammers will enable researchers to develop defence techniques that can prevent jammer attacks. However, due to limited study conducted in the field of jammer classification, the defence phase has become impossible. Presently, the classification accuracy of the assessment is proportional to the size of the data. Increasing the size of the data will make it more accurate. However, in many cases it is not possible to get such large amounts of data due to certain constraints. Therefore, there is a need to find a new valuation method that does not require large data sets yet yields the same results. Thus, this study proposes the development of algorithms to detect and classify jamming attacks using a set of parameters on the physical layer and MAC in MANET. In addition, the methodology to determine the accuracy of the dataset based on limited amount of data will be evaluated. The methodology consists of five main stages. The first stage is to apply reverse engineering method to obtain the specific patterns of individual jammers. This creates the jamming detection and classification parameters. The second stage is detecting jammers by integrating both lower layers by developing Integrated Combined Layer Algorithm (ICLA). The third stage is to classify individual jammers according to the specific pattern and characteristics design as defined in jamming identification and classification parameters. It involves development of Max-Min Rule-Based Classification Algorithm. The fourth stage is to design evaluation methodology of Max-Min Rule-Based Classification Algorithm using classifier model. Finally, both algorithms are validated against the findings in various literatures. Two types of testing were conducted to evaluate the effectiveness of proposed algorithms, which is the performance and accuracy test. Performance tests were conducted against jammers' model at MAC and physical layer. The findings show a significant increase in the detection rate up to 96.26% and 69.15% of deceptive jammer and reactive jammer using ICLA compared to literature. In addition, methodologies for jamming classification to measure the accuracy for each classifier were developed and tested using SVM and WEKA. Results show that data with normalization and scaling for polynomial kernel with cross validation presented the highest accuracy assessment which is 76.142% compared to other classifiers. Therefore, jammer attack detection and classification, studies were provided with better knowledge and technology to develop more robust defence techniques.

# ACKNOWLEDGEMENT

Firstly, I wish to thank God for giving me the opportunity to embark on my PhD research and to complete this long and challenging journey. My gratitute and thanks goes to my supervisor Dr Noor Elaiza Mohd Khalid and co-supervisor, Associate Professor Dr. Kamarularifin Abd Jalil. Thank you for the support, patience and ideas in assisting me with this project. I also would like to express my gratitude to my former supervisor, Prof Dr Saadiah Yahya, for providing the facilities, knowledge, assistance and doa.

Finally, this thesis is dedicated to the loving memory of my kids, and my father and mother for their vision and determination to educate me. This piece of victory is dedicated to both of you. Alhamdulilah.

Dedicated to:

*Dak Bin Abdul, Khodijah Bt Taib, Ahmad Daniel, Farah Natasha, Ahmad Dafi and Muhammad Darwisz.*

# TABLE OF CONTENT