**Response to the Handling Editor and Reviewers**

**Submission No.:** JNCA-D-16-00617

**Title:** Model Order Selection and Eigen Similarity based Framework for Detection and Identification of Network Attacks

**Journal of Network and Computer Applications (JNCA)**

**Research Paper**

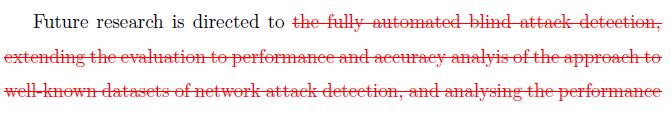
Dear Mohammed Atiquzzaman, Ph.D., Editor-in-Chief, and reviewers,

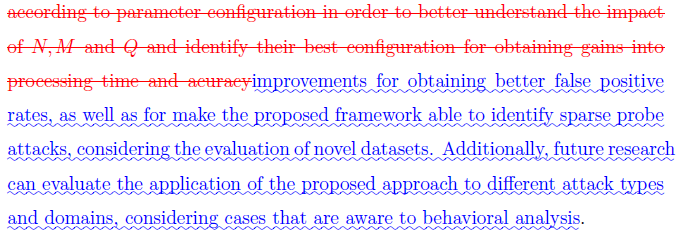
The authors would like to thank the Associate Editor-in-Chief and the Reviewers for volunteering their time in reviewing our manuscript and providing us with valuable comments which allowed us to significantly improve the readability and presentation of the paper. We have carefully revised the manuscript based on the reviewer’s comments and suggestions. All changes in the paper have been marked with a red color for the removed text and a blue color for the added text. The following is our point-by-point responses to the raised comments.

Kind regards,

The authors.

1. EDITOR
   1. **COMMENT:** *The referees have suggested that certain aspects of the paper should be re-examined, before it can be considered further for publication.*
      1. **REPLY:** We thank the Editor for the time, work, and positive evaluation of our paper.
2. REVIEWER #2
   1. **COMMENT:** *The main concern is about the dataset itself, you can make a model just with this features, seq number and port number, also there is so many data sets available why you did not try use them on your model. It is very hard to say if your model is very useful or it is just working on this dataset only, I can see there is work and there is an idea but you can't prove it like this*
      1. **REPLY:** We thank this reviewer for the stimulating comments and for appreciating the contribution of our paper, as well as for the suggestions. We extended our experiments by applying our model to a well-known dataset, which is the DARPA 1998. The Section 2 has been update to include related works that evaluated the selected dataset and other options. We added the Subsection 3.4 in order to discuss the use of the DARPA dataset for evaluation of the proposed approach. We also added Subsection 5.6 in order to present a summarized view of results obtained from the application of the proposed framework.
   2. **COMMENT:** *There is so many attack types on different layers. You used just three types only synﬂood, fraggle and port scan attack. Other data sets has more so you need to test your approach on them*
      1. **REPLY:** We thank the reviewer for the comment. We have added the evaluation of the well-known DARPA 1998 dataset, which is broadly used for attack detection techniques evaluation, the changes in the text is mentioned in reply 2.1.1. However, we agree that is still necessary to evaluate the proposed approach beyond flood and probe attack detection, regarding different datasets or domains. In this sense, we added this point as future work.





1. REVIEWER #3
   1. **COMMENT:** *The authors attempted to propose an approach to detect malicious activities based on model order selection and eigen similarity. They modelled legitimate traffic, malicious, and noise, and perform the evaluation by detecting port scanning and syn flooding attacks in real traffics. One benefits of this work might be that the proposed approach does not rely on the knowledge of source and destination IP addresses. However, the reviewer suggests the authors to consider revising the following listed issues.*
      1. **REPLY:** We thank the reviewer #3for appreciating the contributions in our paper and for the constructive comments.
   2. **COMMENT:** *It looks like the authors only emulate attacks from a local network (LAN). This may limit the contribution of this work.*

## **REPLY:** We are grateful with this suggestion. In order to evaluate the proposed approach regarding inside and outside traffic, we extended our experiments by applying our model to a well-known dataset, which is the DARPA 1998, also considering the comments of the reviewer #2 and reply 2.1.1. The Section 2 has been update to include related works that evaluated the selected dataset and other options. We added the Subsection 3.4 in order to discuss the use of the DARPA dataset for evaluation of the proposed approach. We also added the subsection 5.6 in order to presents a summarized view of results obtained from the application of the proposed framework.

* 1. **COMMENT:** *The references may be outdated -- the latest citation is up to year 2012.*

## **REPLY:** We are thankful for your observation. We made a new literature review and considered more recent references regarding the topic of our paper. As a consequence, Section 2 has been update to include new related works and recent citations have been added to the text.

* 1. **COMMENT:** *The authors did not compare this work against other similar (but not MOS-based) works that detects network probes and flooding attacks.*

## **REPLY:** We thank the reviewer for this constructive comment. We have added a result comparison of the proposed framework against two works that aims the detection of network probe and flood attack, one based on PCA and the second based on signal processing techniques. The results are presented and discussed in Subsection 5.6.

## 

* 1. **COMMENT:** *It looks like there is not a formal analysis on the TP and FP rate of the proposed approach.*

## **REPLY:** Thank you for your helpful observation. In subsection 5.6 we have added an analysis of True Positives (TP), False Positive (FP) and misclassification rate. We also improved our results discussion comparing the obtained results with related works.

* 1. **COMMENT:** *The authors claimed that the proposed approach can be used to detect unknown and novel attacks, but they only evaluated the proposed approach using well-known attacks (probe and flooding attacks). It is not clear how to detect unknown attacks and what could be the effectiveness on detecting unknown attacks.*

## **REPLY:** Thank you very much for your comment. The proposed work focus on the detection of flood and probe attacks through techniques that do not require previous knowledge about the environment or training for classification of normal or abnormal behaviors. In the literature, signal processing techniques have been applied to attack detection due to their capability to blindly detect anomalies, since these anomalies are previously unknown. In our proposal, we focus on flood and probe attacks, regarding the behaviors that characterize these types of attacks. Since DoS can exploit system vulnerabilities through few packets, or consume resources through large amount of network, characterizing flood attacks, we replaced the term DoS by flood along the paper and we added the following text for better clarify this point.

## 

## The description of the selected dataset also highlights the focus of the proposed approach, according to the following text that was added in subsection 3.4.

## 

* 1. **COMMENT:** *The scalability of the proposed approach is not known, and the authors may have to provide complexity analysis on the storage and computation costs of the proposed approach.*

## **REPLY:** We thank the reviewer for this constructive comment. We moved the complexity analysis to Section 6 and added the performance evaluation of processing time over variations of network traffic time, frame time and number network ports evaluated for attack detection.

* 1. **COMMENT:** *The symbols are sometimes inconsistent. For example, the capital U and capital S both indicate legitimate traffic!?s*

## **REPLY:** Thank you very much for the observation. Both capital S and capital U mistakenly stood for legitimate traffic. Therefore, capital S has been replaced by the capital U in order to correct the notation. The whole text has been broadly and carefully revised, with special care for the symbols and notations.