CERTIFICATION for the PEER REVIEW PROCESS & EVALUATION of the PEER REVIEW PROCESS & CERTIFICATION for NON EXISTENCE of ARTIFICIAL CITATIONS and ANTI-PLAGIARISM CONTROL

Name: Mohammad Adnan Aladaileh
Institution: National Advanced IPv6 Centre of Excellence, Universiti Sains Malaysia, Penang, Malaysia
City: Penang Island.
Country: Malaysia
Phone:0060184643704
Academic Email: m_aladaileh2003@nav6.usm.my

I declare, I confirm, I certify and I sign that I received substantial, important, line by line peer review with several and substantial comments, important remarks and hints from, at least, 3 Reviewers and the Assistant Editor for my paper: Information theory-based approaches to detect DDoS attacks on software-defined networking controller a review with Authors: Mohammad A. Aladaileh, Mohammed Anbar, Iznan H. Hasbullah and Yousef K. Sanjalawe.

I would like to thank all the reviewers for their thoughtful comments and efforts towards improving our manuscript. We revised the manuscript with special attention to the comments that we received from Three (3) reviewers that were experts, specialists in the area of my paper.

I declare, confirm, certify and sign that NAUN has checked my paper for possible plagiarism by Turnitin and my paper was found without plagiarism or self-plagiarism by Turnitin. I also declare, confirm, certify and sign that also that no Associate-Editor, no Editor-in-Chief, no member of the NAUN Secretariat forced me in this Journal to add references (citations) to any previous publications of the journal.

I also declare, confirm, certify and sign that I have made all the changes, modifications, additions, studies, corrections asked by the reviewers and I have fully complied with their instructions. I also understand that before the publication the 3 (or more than 3) reviewers will check my paper to see if all the changes, modifications, additions, studies, corrections etc have been done and I authorize the NAUN to publish my paper or to reject my paper even in the 2nd round of peer review or to continue with an additional round of peer review.

I also declare, I confirm, I certify and I sign that I will not publish this paper or an important part of the paper in any other Journal (inside or outside NAUN) Conference Proceedings (inside or outside NAUN), Book (inside or outside NAUN), University Repository etc) without the written permission of the NAUN.

I also declare, I confirm, I certify and I sign that this paper or an important part of the paper has not been published other Journal (inside or outside NAUN) Conference Proceedings (inside or outside NAUN), Book (inside or outside NAUN), University Repository etc). In case of violation of the above terms, NAUN can reject any unpublished paper or even retract any published **paper.**

Please, write additional comments below (**take ideas from: https://naun.org/main/NAUN/author-testimonials.html)**

Dear Editor of NAUN Journals,
Thank you for giving me the opportunity to submit a revised draft of my manuscript titled "Information theory-based approaches to detect DDoS attacks on software-defined networking controller a review " to "International Journal of Education and Information". We appreciate the time and effort that you and the reviewers have dedicated to providing your valuable feedback on my manuscript. We are grateful to the reviewers for their insightful comments on my paper. We have been able to incorporate changes to reflect most of the suggestions provided by the reviewers. Here is a point-by-point response to the reviewers' comments and concerns.

Comments from Reviewer #1

Comment 1: Clearly specify the motivation behind this work and the contributions of this work with respect to previous works in literature.

Response: Thank you for pointing out this valuable comment. We totally agree with this comment. Therefore, we have clearly explained the motivation behind this work and the contribution in **Section I**.

"However, the centralized controller also faces challenges and issues that affect network performance in terms of security, reliability, and scalability [9].

The DDoS attack is one of the security challenges to the SDN network that could bring down the entire network, denying legitimate user access to network services or resources. DDoS is one of the most common types of attacks that target the SDN controllers [13-14]. In a DDoS attack, attackers flood the network or the controller with a large volume of traffic to the point where the controller's resources are exhausted and unable to process any more incoming packets. Therefore, many researchers have proposed approaches to tackle DDoS attack issues. Information theory-based approaches are considered the most common approaches for detecting DDoS attacks on SDN network.
The contributions of this paper are: (i) a comprehensive review of various information theory-based approaches to detect low-rate and high-rate DDoS attacks on the SDN controller; (ii) qualitative comparison of this work with existing

reviews related to similar fields in terms of information theory used and classifies the detection approaches; and (iii) in-depth discussion and insight on the existing detection approaches' gaps."

Comment 2: The reason(s) for writing the paper or the aims of the research should be given in the abstract.

Response: We totally agree with comment; therefore, we have added the aims of the research in the **abstract,** implicitly.

"This paper presents a comprehensive review of information theory-based approaches to detect low-rate and high-rate DDoS attacks on SDN controllers. Additionally, this paper provides a qualitative comparison between this work and the existing reviews on DDoS attack detection approaches using various metrics to highlight this work's uniqueness. Moreover, this paper provides in-depth discussion and insight into the existing DDoS attack detection approaches to point out their weaknesses that open the avenue for future research directions. Meanwhile, the finding of this paper can be used by other researchers to propose a new or enhanced approach to protect the controller from the threats of DDoS attacks by accurately detecting both low-rate and high-rate DDoS attacks."

Comment 3: The discussions in section VI (Research gaps and discussion) are not enough to explain the superiority of the proposed scheme well. It is suggested that the authors give more comments about the DDoS attack detection approaches.

Response: We totally agree with comment; therefore, we added more explanation on the research gaps and discussion in the manuscript (refer to Section VI).

Comment 4: The mathematical analysis of the algorithms (section V: Information theory-based algorithms to detect DDoS attacks on SDN controller) in the present form is relatively weak and should be strengthened with more details.

Response: We totally agree with comment; therefore, the manuscript was added more explanation about section V.

<u>Comments from Reviewer #2</u>

Comment 1: The aim of the paper should be clearly defined in the introduction.
Response: We clearly explained the aim of this paper in the introduction.

Comment 2: In the abstract and conclusion section summarize the article's main findings and indicate the main conclusions.

Response: We agree with this and have incorporated your valuable suggestion throughout the related sections, and therefore, we have summarized the article's main findings and indicate the main conclusions in related sections.

“This paper presents a comprehensive review of information theory-based approaches to detect low-rate and high-rate DDoS attacks on SDN controllers. Additionally, this paper provides a qualitative comparison between this work and the existing reviews on DDoS attack detection approaches using various metrics to highlight this work’s uniqueness. Moreover, this paper provides in-depth discussion and insight into the existing DDoS attack detection approaches to point out their weaknesses that open the avenue for future research directions. Meanwhile, the finding of this paper can be used by other researchers to propose a new or enhanced approach to protect the controller from the threats of DDoS attacks by accurately detecting both low-rate and high-rate DDoS attacks.”

Comment 3: Explain how this paper differs from the related ones published in the technical literature. The authors need to clarify and explain the difference of the current study with the available literature.

Response: We agree with this and have explained the difference between this paper and existing studies.

“This section provides a qualitative comparison to benchmark this work with other existing information theory-based detection approaches designed to detect low-rate and high-rate DDoS attacks on the controller using different metrics to highlight this study’s uniqueness, as shown in Table 3. The used metrics are: (i) number of theories used, (ii) approaches classified. These metrics are defined based on intensive study of many existing detection approaches. This comparison aims to understand the critical issues related to detecting DDoS attacks on the controller to find an efficient detection approach. Furthermore, it could be a guideline for future researchers in a similar domain. This review is compared with three existing reviews from [10], [39], and [40].”

<u>Comments from Reviewer #3</u>

Comment 1: Therefore, there is a need to propose an approach to detect DDoS attack on SDN controller with high detection accuracy and low false-positive regardless of the DDoS traffic rate either low or high-rate DDoS attacks that are target single victim and multiple victims.' More details are necessary.

Response: Thank you for the comment. We have updated the manuscript by replacing the text with the following, in Section VI:

“The observation of the reviewed existing information theory-based approaches reveals the following:

- Some of the existing approaches rely on a single packet header feature to detect DDoS attacks against an SDN controller triggered from a single host and attacking single or multiple targets have a low detection rate and high false-positive detection rate.
- Some of the existing approaches to detect DDoS attacks against SDN controller using two packet header features are incapable of detecting low-rate DDoS attacks on multiple targets to achieve a high detection rate and low false-positive rate.
- Some of the existing detection approaches rely only on static threshold values, making them inefficient in detecting DDoS attacks with variable traffic rates to achieve a high detection rate and a low false-positive rate.

Therefore, the future DDoS attack detection approach should address the abovementioned drawbacks of the existing approaches and fulfills the following requirements: … ”

Comment 2: In section V the authors write that 'Achieving more than one detect low and high rate DDoS attacks needs simultaneously by adopting a multi-objective optimization.' How will this affect the results? More details should be furnished.

Response: Thank you for your comment. We have updated the manuscript by replacing the abovementioned text with the following:

“ 4. Able to detect both low-rate and high-rate DDoS attacks regardless of the number of victims (single or multiple).”

Comment 3: I believe that the Figure 2 'SDN architecture' needs more details and explanations.
Response: We added more details and explanations about Figure 2.

Comment 4: add these 2 references.

Response: Thank you for your suggestion. The two references have been added to the manuscript.

Signature (insert an image file with scanned signature or print out the whole page, sign and scan)

Date: 8/4/2021
Mohammad Adnan Aladaileh