User Menu
- Home
- Manage Accounts
- Change Password
- Edit Profile
- Logout

Submissions Menu
- Submit Manuscript
- Display Submitted Manuscripts
- English Editing
- Discount Vouchers
- Invoices
- LaTex Word Count

Reviewers Menu
- Volunteer Preferences

Article Information Overview

Manuscript ID	electronics-1603932
Status	Website online
DOI	10.3390/electronics11050737
Publication Certificate	Download Publication Certificate (PDF)
Banner	Download Banner (PDF)
Website Links	Abstract HTML version PDF version Manuscript
Article type	Article
Title	SUKRY: Suricata IDS with Enhanced kNN Algorithm on Raspberry Pi for Classifying IoT Botnet Attacks
Journal	*Electronics*
Volume	11
Issue	5
Section	Computer Science & Engineering
Special Issue	Security and Privacy in IoT Enabled Modern Applications Using Deep/Machine Learning and Blockchain Technology
Abstract	The focus of this research is the application of the k-Nearest Neighbor algorithm in terms of classifying botnet attacks in the IoT environment. The kNN algorithm has several advantages in classification tasks, such as simplicity, effectiveness, and robustness. However, it does not perform well in handling large datasets such as the Bot-IoT dataset, which represents a huge amount of data about botnet attacks on IoT networks. Therefore, improving the kNN performance in classifying IoT botnet attacks is the main concern in this study by applying several feature selection techniques. The whole research process was conducted in the Rapidminer environment using three prebuilt feature selection techniques, namely, Information Gain, Forward Selection, and Backward Elimination. After comparing accuracy, precision, recall, F1 score and processing time, the combination of the kNN algorithm and the Forward Selection technique (kNN-FS) achieves the best results among others, with the highest level of accuracy and the fastest execution time among others. Finally, kNN-FS is used in developing SUKRY, which stands for Suricata IDS with Enhanced kNN Algorithm on Raspberry Pi.
Keywords	botnet attack; IoT; machine learning; kNN; feature selection; Suricata; Raspberry Pi

Author Information

Submitting Author	Irfan Syamsuddin
Corresponding Author	Irfan Syamsuddin
Author #1	Irfan Syamsuddin
Affiliation	1. Department of Computer and Networking Engineering, State Polytechnic of Ujung Pandang, Makassar 90245, Indonesia
E-Mail	irfans@poliupg.ac.id
Author #2	Omar Mohammed Barukab
Affiliation	2. Faculty of Computing and Information Technology-Rabigh, King Abdulaziz University, Jeddah 21911, Saudi Arabia
E-Mail	obarukab@kau.edu.sa

Manuscript Information

Received Date	3 February 2022
Revised Date	21 February 2022
Accepted Date	24 February 2022
Published Date	27 February 2022
Figure Count	15
Table Count	7
Reference Count	60

Editor Decision

Decision	Accept in current form
Comments	Accepted in current form.
Decision Date	24 February 2022

Review Report

Reviewer 1	Review Report (Round 1) Review Report (Round 2)
Reviewer 2	Review Report (Round 1)
Reviewer 3	Review Report (Round 1) Review Report (Round 2)

APC information

Journal APC:	2,000.00 CHF
Total Payment Amount:	2,000.00 CHF

Related Papers Published in MDPI Journals

If you have any questions or concerns, please do not hesitate to contact electronics@mdpi.com.

susy.mdpi.com/user/manuscripts/review_info/dbee26d885e46b991bd8ce9965926516

Journals Information Initiatives About irfans@poliupg.ac.id My Profile Logout Submit

User Menu
- Home
- Manage Accounts
- Change Password
- Edit Profile
- Logout

Submissions Menu
- Submit Manuscript
- Display Submitted Manuscripts
- English Editing
- Discount Vouchers
- Invoices
- LaTex Word Count

Reviewers Menu
- Volunteer Preferences

Manuscript Information Overview

Manuscript ID	**electronics-1464904**
Status	Rejected
Article type	Article
Title	Enhancing the Performance of kNN Algorithm in Classifying IoT BotNet Attacks using Feature Selection Techniques
Journal	*Electronics*
Section	Artificial Intelligence
Abstract	In the present study k Nearest Neighbor algorithm is being studied in terms of classifying Botnet attacks within IoT environment. There are several advantages of using kNN algorithm in classification issues such simplicity, effectiveness and robustness. However, it does not perform well in handling large dataset such as Bot-IoT dataset that represents huge amount data of botnet attacks in IoT networks. In such case, kNN often shows lower accuracy and longer execution time. Therefore, improving kNN performance in classifying IoT Botnet attack is the main concern in this study by applying several feature selection techniques. The whole research processes are conducted in Rapidminer environment using three prebuilt feature selection techniques namely, Information Gain, Forward Selection and Backward Elimination. It is finally found that Forward Selection is the best feature selection technique to improve the performance of kNN algorithm (kNN-FS) in classifying Bot-IoT dataset by achieving best results in all five evaluation criteria.
Keywords	botnet attack; IoT; machine learning; kNN; feature selection
Manuscript File	manuscript.docx

Author Information

Submitting Author	Irfan Syamsuddin
Corresponding Author	Irfan Syamsuddin
Author #1	Irfan Syamsuddin
E-Mail	irfans@poliupg.ac.id
Author #2	Omar Mohammed Barukab
E-Mail	obarukab@kau.edu.sa

Manuscript Information

Received Date	30 October 2021
Revised Date	6 December 2021
Submission to First Decision (Days)	39
Submission to Publication (Days)	
Round of Revision	2
Page Count	17

Editor Decision

Decision	Reject and decline resubmission
Decision Date	22 December 2021

Review Report

Reviewer 1	Review Report (Round 1) Review Report (Round 2) Review Report (Round 3)
Reviewer 2	Review Report (Round 1)
Reviewer 3	Review Report (Round 1) Review Report (Round 2)

APC information

Journal APC:	1,800.00 CHF
Total Payment Amount:	1,800.00 CHF

Previously Published Papers

Syamsuddin, I.; Barukab, O.M. SUKRY: Suricata IDS with Enhanced kNN Algorithm on Raspberry Pi for Classifying IoT Botnet Attacks. *Electronics* **2022**, *11*, 73. doi: 10.3390/electronics11050737

electronics-11649....pdf | MDPI _ Reply revi....html | FIRST ROUND Res....pdf | electronics-1464S....pdf | ICTE_2020_302_R1.pdf | Tampilkan semua

Journal: Electronics (https://www.mdpi.com/journal/electronics) (ISSN 2079-9292)

Manuscript ID: electronics-1603932

Type: Article

Title: SUKRY: Suricata IDS with Enhanced kNN Algorithm on Raspberry Pi for Classifying IoT Botnet Attacks (https://www.mdpi.com/2079-9292/11/5/737)

Authors: Irfan Syamsuddin * , Omar Mohammed Barukab

Section: Computer Science & Engineering (https://www.mdpi.com/journal/electronics/sections/computer_science_engineering)

Special Issue: Security and Privacy in IoT Enabled Modern Applications Using Deep/Machine Learning and Blockchain Technology (https://www.mdpi.com/journal/electronics/special_issues/Security_IoT_MLBC)

Abstract: In this paper, k-Nearest Neighbor algorithm is being studied in terms of classifying Botnet attacks within IoT environment. There are several advantages of using kNN algorithm in classification issues such simplicity, effectiveness and robustness. However, it does not perform well in handling large dataset such as Bot-IoT dataset that represents huge amount data of botnet attacks in IoT networks. In such case, kNN often shows lower accuracy and longer execution time. Therefore, improving kNN performance in classifying IoT Botnet attack is the main concern in this study by applying several feature selection techniques. The whole research processes were conducted in Rapidminer environment using three prebuilt feature selection techniques namely, Information Gain, Forward Selection and Backward Elimination. After comparing accuracy, precision, recall, F1-score and processing time, the combination of kNN algorithm and Forward Selection technique (kNN-FS) achieves the best results among others to enhance kNN performance in classifying Bot-IoT attacks in IotT network. Finally, kNN-FS is then applied in Suricata IDS running on Raspberry Pi machine, named Sukry.

The coverletter for this review report has been saved in the database. You can safely close this window.

Authors' Responses to Reviewer's Comments (Reviewer 1)

Author's Notes: Authors applied K-nearest neighbors algorithm combined with 3 feature selection algorithms implemented in the RapidMiner tool to

the open Bot-IoT dataset and got better accuracy (99.89%) than cited results (98.9% using Decision Tree). Please include comparison to other methods not using kNN to the Table 7, such as the result using Decision Tree which is better than the result obtained with kNN.

answer : *We have revised the table 7 accordingly, thanks much*

Comparison of the execution time and required computational resources is also interesting, but is not present in the paper.

answer : *There is no confirmation regarding execution time from previous papers, they only provide accuracy, therefore in our paper there is only comparison of accuracy, From this point of view, we also justify the importance of mentioning execution time in making comparative study, not only level of accuracy.*

We mentioned this is Discussion section 5,
thank you very much.

Description of feature selection techniques is too short and consists of a single paragraph. It is unclear from the description how Information Gain feature selection works, all that is said is that it "works by reducing the number of feature[s] by measuring entropy reduction before and after separation in terms of its dependency".

answer : We have improved these in 3.3. Feature Selection Techniques and kNN Algorithm

Description of Bot-IoT dataset should include the size of the training and test set. What are the sizes of the parts used for test and training?

answer : *We have mentioned the size clearly. In 3.1. Dataset, Thank you*

On page 7, line 184, reference [7] in sentence "The idea of kNN is that it will classify new objects based on k of their 183 closest neighbors, where k is a predetermined positive integer" points to "Available online: https://www.newark.com/iot-trends-2021 (accessed on Sep 30, 2021)." rather than a description of kNN.

answer : *We have corrected and Improved the introduction section properly. Many thanks*

It looks like bibliography is managed manually and references are not checked automatically which is error-prone. I have not checked all other references and suggest using automatic reference

management tools such as BibTeX or those built in MS Office.

answer : *Thank you very much*

answer : *Thank you very much*

In the pseudo-code of kNN algorithm it is not defined what variable "m" means.

answer : *We already corrected this as well in 3.3. Feature Selection Techniques and kNN Algorithm. Thank you*

English could be improved, for example "that only effective for known botnets" -> "that *are* only effective for known botnets", "several approach to apply different algorithms have been applied", "similar studies utilizing machine learning frameworks are proposed in several studies", "confirmed the *effectively of* using", "causing kNN requires" -> "causing kNN to require".

answer : *Many thanks for the corrections*

Review Report Form

English language and style

( ) Extensive editing of English language and style required
( ) Moderate English changes required
(x) English language and style are fine/minor spell check required
( ) I don't feel qualified to judge about the English language and style

	Yes	Can be improved	Must be improved	Not applicable
Does the introduction provide sufficient background and include all relevant references?	( )	(x)	( )	( )
Is the research design appropriate?	(x)	( )	( )	( )
Are the methods adequately described?	( )	( )	(x)	( )
Are the results clearly presented?	( )	(x)	( )	( )
Are the conclusions supported by the results?	(x)	( )	( )	( )

Comments and Suggestions for Authors

Authors applied K-nearest neighbors algorithm combined with 3 feature selection algorithms implemented in the RapidMiner tool to the open Bot-IoT dataset and got better accuracy (99.89%) than cited results (98.9% using Decision Tree). Please include comparison to other methods not using kNN to the Table 7, such as the result using Decision Tree which is better than the result obtained with kNN. Comparison of the execution time and required computational resources is also interesting, but is not present in the paper. Description of feature selection techniques is too short and consists of a single paragraph. It is unclear from the description how Information Gain feature selection works, all that is said is that it "works by reducing the number of feature[s] by measuring entropy reduction before and after separation in terms of its dependency". Description of Bot-IoT dataset should include the size of the training and test set. What are the sizes of the parts

used for test and training? On page 7, line 184, reference [7] in sentence "The idea of kNN is that it will classify new objects based on k of their 183 closest neighbors, where k is a predetermined positive integer" points to "Available online: https://www.newark.com/iot-trends-2021 (accessed on Sep 30, 2021)." rather than a description of kNN. It looks like bibliography is managed manually and references are not checked automatically which is error-prone. I have not checked all other references and suggest using automatic reference management tools such as BibTeX or those built in MS Office. In the pseudo-code of kNN algorithm it is not defined what variable "m" means. English could be improved, for example "that only effective for known botnets" -> "that *are* only effective for known botnets", "several approach to apply different algorithms have been applied", "similar studies utilizing machine learning frameworks are proposed in several studies", "confirmed the *effectively of* using", "causing kNN requires" -> "causing kNN to require".

Submission Date	03 February 2022
Date of this review	07 Feb 2022 17:10:51

Journal	Electronics (https://www.mdpi.com/journal/electronics) (ISSN 2079-9292)
Manuscript ID	electronics-1603932
Type	Article
Title	SUKRY: Suricata IDS with Enhanced kNN Algorithm on Raspberry Pi for Classifying IoT Botnet Attacks (https://www.mdpi.com/2079-9292/11/5/737)
Authors	Irfan Syamsuddin * , Omar Mohammed Barukab
Section	Computer Science & Engineering (https://www.mdpi.com/journal/electronics/sections/computer_science_engineering)
Special Issue	Security and Privacy in IoT Enabled Modern Applications Using Deep/Machine Learning and Blockchain Technology (https://www.mdpi.com/journal/electronics/special_issues/Security_IoT_MLBC)

Abstract

In this paper, k-Nearest Neighbor algorithm is being studied in terms of classifying Botnet attacks within IoT environment. There are several advantages of using kNN algorithm in classification issues such simplicity, effectiveness and robustness. However, it does not perform well in handling large dataset such as Bot-IoT dataset that represents huge amount data of botnet attacks in IoT networks. In such case, kNN often shows lower accuracy and longer execution time. Therefore, improving kNN performance in classifying IoT Botnet attack is the main concern in this study by applying several feature selection techniques. The whole research processes were conducted in Rapidminer environment using three prebuilt feature selection techniques namely, Information Gain, Forward Selection and Backward Elimination. After comparing accuracy, precision, recall, F1-score and processing time, the combination of kNN algorithm and Forward Selection technique (kNN-FS) achieves the best results among others to enhance kNN performance in classifying Bot-IoT attacks in IotT network. Finally, kNN-FS is then applied in Suricata IDS running on Raspberry Pi machine, named Sukry.

The coverletter for this review report has been saved in the database. You can safely close this window.

Authors' Responses to Reviewer's Comments (Reviewer 2)

Author's Notes

There are several aspects of the article that could be improved.

First of all, it is recommended to improve the quality of the images.

Some of them appear blurred.

answer :*We have improved the quality of images. Thank you*

Secondly, in Figure 5, Figure 8, Figure 11, etc., there are two exclamation marks that do not understand their meaning, it could be explained if it has any value.

answer : *We have corrected the figures as well , Thanks much*

On the other hand, I find of great interest the implementation on raspberry pi, however, I lack details to reproduce the experiment. You could provide more details such as in the case of.

answer : *We have described the experiment procedure in section 4.5 SUKRY Implementation , the suggested paper also cited as new ref no 58, Thank you*

Finally, the solution is very interesting and I would consider encapsulating the solution for use as a secure design pattern. In "Development of Applications Based on Security Patterns" a language for the description of patterns is presented that could be considered as a future line of work, for a more mature work.

answer :*Thank you very much for the suggestion. We already improved the discussion in section 5.*

Review Report Form

English language and style

( ) Extensive editing of English language and style required
( ) Moderate English changes required
(x) English language and style are fine/minor spell check required
( ) I don't feel qualified to judge about the English language and style

	Yes	Can be improved	Must be improved	Not applicable
Does the introduction provide sufficient background and include all relevant references?	(x)	( )	( )	( )
Is the research design appropriate?	( )	(x)	( )	( )
Are the methods adequately described?	(x)	( )	( )	( )
Are the results clearly presented?	(x)	( )	( )	( )
Are the conclusions supported by the results?	(x)	( )	( )	( )

Comments and

In this paper, a new algorithm for Botnet attack classification in IoT environment is proposed. Some advantages of this algorithm for identifying botnet attacks in IoT networks are identified

Suggestions for Authors

identifying botnet attacks in IoT networks are identified.

They make use of Rapidminer throughout the research process using three predefined feature selection techniques (Information Gain, Forward Selection and Backward Elimination). A comparative study is made between F1 score and processing time, the combination of kNN algorithm, obtaining good results of Forward Selection technique (kNNN-FS) achieves the best results among others to improve the performance of kNN in classifying Bot-IoT attacks in IotT network. As a highlight of the article is the application of Suricata IDS in a real pilot on a Raspberry Pi machine.

There are several aspects of the article that could be improved. First of all, it is recommended to improve the quality of the images. Some of them appear blurred. Secondly, in Figure 5, Figure 8, Figure 11, etc., there are two exclamation marks that do not understand their meaning, it could be explained if it has any value. On the other hand, I find of great interest the implementation on raspberry pi, however, I lack details to reproduce the experiment. You could provide more details such as in the case of. "P2ISE: Preserving Project Integrity in CI/CD Based on Secure Elements" in which details are shown to reproduce the experiment concretely.
Finally, the solution is very interesting and I would consider encapsulating the solution for use as a secure design pattern. In "Development of Applications Based on Security Patterns" a language for the description of patterns is presented that could be considered as a future line of work, for a more mature work.

Submission Date	03 February 2022
Date of this review	07 Feb 2022 10:35:06

Journal	Electronics (https://www.mdpi.com/journal/electronics) (ISSN 2079-9292)
Manuscript ID	electronics-1603932
Type	Article
Title	SUKRY: Suricata IDS with Enhanced kNN Algorithm on Raspberry Pi for Classifying IoT Botnet Attacks (https://www.mdpi.com/2079-9292/11/5/737)
Authors	Irfan Syamsuddin * , Omar Mohammed Barukab
Section	Computer Science & Engineering (https://www.mdpi.com/journal/electronics/sections/computer_science_engineering)
Special Issue	Security and Privacy in IoT Enabled Modern Applications Using Deep/Machine Learning and Blockchain Technology (https://www.mdpi.com/journal/electronics/special_issues/Security_IoT_MLBC)

Abstract

In this paper, k-Nearest Neighbor algorithm is being studied in terms of classifying Botnet attacks within IoT environment. There are several advantages of using kNN algorithm in classification issues such simplicity, effectiveness and robustness. However, it does not perform well in handling large dataset such as Bot-IoT dataset that represents huge amount data of botnet attacks in IoT networks. In such case, kNN often shows lower accuracy and longer execution time. Therefore, improving kNN performance in classifying IoT Botnet attack is the main concern in this study by applying several feature selection techniques. The whole research processes were conducted in Rapidminer environment using three prebuilt feature selection techniques namely, Information Gain, Forward Selection and Backward Elimination. After comparing accuracy, precision, recall, F1-score and processing time, the combination of kNN algorithm and Forward Selection technique (kNN-FS) achieves the best results among others to enhance kNN performance in classifying Bot-IoT attacks in IotT network. Finally, kNN-FS is then applied in Suricata IDS running on Raspberry Pi machine, named Sukry.

The coverletter for this review report has been saved in the database. You can safely close this window.

Authors' Responses to Reviewer's Comments (Reviewer 3)

Author's Notes

Although the paper covers an interesting topic that falls within the scope of the journal, unfortunately I cannot recommend publishing

scope of the journal, unfortunately I cannot recommend publishing the paper in this form (I recommend major revision). The authors seem to have done some good research in a very important topic, however were not able to communicate that through writing and discussion. The paper has many shortcomings, in my opinion - in the following - I explain the main shortcomings in terms of structure, objective, declaration of the problem. In addition to the lack of clarity of the objective

answer : Thank you very much for the suggestions. We have made extensive revision based on these recommendations as can be seen in section 1. Introduction and section 2. Relevant Studies

Unfortunately, writing and formatting of the article are not suitable, and required more efforts to refinement. The overall paper needs to be rewritten. So it can be said there is a major writing issues, in terms of grammar: use of adverbs, pronouns, gerunds, definite vs. indefinite articles, plural and singular and pronouns. Furthermore lack of proper punctuation makes it hard to read. Long sentences turning into complete paragraphs!

answer : Thanks much, We have corrected language errors.

- No adequate coverage of related work, few paragraphs embedded into the introduction and in the section 2, without analysis or discussion

answer : *We have improved section* 2. Relevant Studies *by additional related references with comments and appropriate analysis . Thank you*

- The problem definition must be declared

answer : We have mentioned clearly in section 1 Introduction. Thanks much

- Overall, the proposed schema(s) seems to be simple (specially static one) There are no rules or rules to arrange the steps provided in the proposed schema. I feel as though the authors have provided a schema based on the empirical method

Pseudo code of 184 kNN algorithm is represented below depicted in fig 4 is very trivial

answer : We have corrected it. Thanks much

A lot of paragraph and definition must be eliminated

answer : We have corrected and improved them as well . Thank you so much

Analysis and discussion of the results not enough to validate the proposal

proposal

answer : We have improved the discussion in section 5. Thank you so much for the positive feedbacks.

Review Report Form

English language and style

( ) Extensive editing of English language and style required
( ) Moderate English changes required
(x) English language and style are fine/minor spell check required
( ) I don't feel qualified to judge about the English language and style

	Yes	Can be improved	Must be improved	Not applicable
Does the introduction provide sufficient background and include all relevant references?	( )	(x)	( )	( )
Is the research design appropriate?	( )	( )	(x)	( )
Are the methods adequately described?	( )	(x)	( )	( )
Are the results clearly presented?	( )	( )	(x)	( )
Are the conclusions supported by the results?	( )	(x)	( )	( )

Comments and Suggestions for Authors

This paper presents a solution that aims to improve the performance of kNN algorithm specifically in 74 dealing with BotNet IoT dataset by applying feature selection techniques.

Although the paper covers an interesting topic that falls within the scope of the journal, unfortunately I cannot recommend publishing the paper in this form (I recommend major revision). The authors seem to have done some good research in a very important topic, however were not able to communicate that through writing and discussion. The paper has many shortcomings, in my opinion - in the following - I explain the main shortcomings in terms of structure, objective, declaration of the problem. In addition to the lack of clarity of the objective

- Unfortunately, writing and formatting of the article are not suitable, and required more efforts to refinement. The overall paper needs to be rewritten. So it can be said there is a major writing issues, in terms of grammar: use of adverbs, pronouns, gerunds, definite vs.

indefinite articles, plural and singular and pronouns. Furthermore lack of proper punctuation makes it hard to read. Long sentences

lack of proper punctuation makes it hard to read. Long sentences turning into complete paragraphs!

- No adequate coverage of related work, few paragraphs embedded into the introduction and in the section 2, without analysis or discussion

- The problem definition must be declared

- Overall, the proposed schema(s) seems to be simple (specially static one) There are no rules or rules to arrange the steps provided in the proposed schema. I feel as though the authors have provided a schema based on the empirical method

Pseudo code of 184 kNN algorithm is represented below depicted in fig 4 is very trivial

A lot of paragraph and definition must be eliminated

Analysis and discussion of the results not enough to validate the proposal

Submission Date	03 February 2022
Date of this review	08 Feb 2022 16:23:57

Response to Reviewer 2:

- There are a bunch of ambiguity in the abstract:
  Response: *we have improved the abstract to avoid ambiguity.*

- The written of the paper is not justified since the problem that the paper is addressed is not clear. Please clearly mention the pitfalls of the state of the arts research.
  Response: *the problem to be addressed in the study is lower performance of kNN in dealing with large size dataset in this case Botnet dataset. This part has been added in the last part of section 1.*

- The superiority of the proposed scheme is not exposed and compared with the state of the arts.
  Response: *we already mentioned 2 previous research using kNN in section "4.4. Performance Comparison", in which we cited paper 42 and 43 that obtained lower kNN accuracy level than our proposal.*

- After the comparison with the existing research, the authors/author should explain the percentage of improvement in comparison with the research in the literature.
  Response: *the percentage of difference has also been added in the same section "4.4. Performance Comparison"*

- In section 1, the author fails to provide motivations of the proposed scheme. I recommend the author to include the interesting applications of the proposed scheme.
  Response: *motivation of our study has been mentioned in section 1 paragraph 9.*

- The motivation of the practical use of the theoretic design should be clearly addressed. The best way to show this is by practical example or explanations.
  Response: *Specific motivation of practical use is not our coverage since we consider main motivation (no 5) has been clearly mentioned already.*

- Are there any deficiencies of the design in this paper and how to make further improvement, to make your results less conservative?
  Response: *we consider the presentation of of the paper fits the scope of our study.*

- The author needs the help of someone whose command over the language is good to edit the paper so that composition and grammar of the language used are correct.
  Response: *We have improve some English errors*

- The authors should add and justify (by referring to published materials) the parameters of implementation setup.
  Response: *Real implementation is beyond of the scope of our study.*

Response to Reviewer 3:

The paper is interesting especially because of the IoT issue it raises. IoT infrastructure is particularly vulnerable to all kinds of attacks. The paper addresses the selected issue of using kNN to classify IoT BotNet Attacks. I would like to point out that the structure of the paper is generally correct. However, additions are required in several places in the manuscript.

1. The source entries for the statements made in line 58-69 should be indicated.
   Response: *The source of statements in these lines are now with clear citations.*

2. Section 3.1 needs improvement. Referring only to item [37] is not sufficient. There is a lack of assumptions and precise information about the functioning of BotNet Attacks in IoT environment. There is no architecture of the IoT environment, or accurate information about the dataset on which the analysis is based. Table 1 can refer to any network traffic and does not clearly indicate that it refers to the IoT environment. This section needs to be expanded to clearly indicate how the adopted data maps to the IoT BotNet Attacks.
   Response: *The source 37 is actually the original paper from which the dataset obtained, and we supported this by mentioning ref no 38,39,40 and 41 in the following sentences. So, actually we have provided 5 sources to justify the selection of dataset. In addition to Table 1, it shows all features of the BotNet IoT dataset taken from reference no 37, so this table clearly shows whole features or attributes of the dataset.*

3. There is also no information on whether and to what extent the method used has practical applications for ongoing monitoring of attacks, whether it can be implemented in a production environment and what requirements would be involved. From this perspective, it would be interesting to know the calculation time and whether the proposed solution can be used for ongoing monitoring or only for historical data analysis.
   Response: *Practical production environment is beyond the scope of our study, therefore we do not mention it in the paper.*

Comments and Suggestions for Authors

This manuscript presents already explored issues. The reviewer didn't find any new contribution in this submission. Similar experiments have been reported in the literature.No novelty is found as most of the work is just rebuilding the existing work.

Response to Reviewer 1:

We have listed contribution of the paper in the last part of section 1. These are the novelty proposed in our study.

In summary, the main contributions of this research are as follows:

- *Present kNN algorithm application in classification of botnet attacks in IoT networks using huge size dataset.*
- *Implement and evaluate different feature selection techniques to kNN algorithm to achieve the best results*
- *Justify the best combination of feature selection techniques and kNN algorithm based on accuracy levels and execution time.*
- *The whole implementations are applied in Rapidminer environment.*

User Menu

Home (/user/myprofile)
Manage Accounts (/user/manage_accounts)
Change Password (/user/chgpwd)
Edit Profile (/user/edit)
Logout (/user/logout)

Submissions Menu

Submit Manuscript (/user/manuscripts/upload)
Display Submitted Manuscripts (/user/manuscripts/status)
English Editing (/user/pre_english_article/status)
Discount Vouchers (/user/discount_voucher)
Invoices (/user/invoices)
LaTex Word Count (/user/get/latex_word_count)

Reviewers Menu

Volunteer Preferences (/volunteer_reviewer_info/view)

Manuscript Information Overview

Manuscript ID	**electronics-1464904**
Status	Rejected
Article type	Article
Title	Enhancing the Performance of kNN Algorithm in Classifying IoT BotNet Attacks using Feature Selection Techniques
Journal	*Electronics* (https://www.mdpi.com/journal/electronics)
Section	Artificial Intelligence (https://www.mdpi.com/journal/electronics/sections/Artificial_Intell)
Abstract	In the present study k-Nearest Neighbor algorithm is being studied in terms of classifying Botnet attacks within IoT environment. There are several advantages of using kNN algorithm in classification issues such simplicity, effectiveness and robustness. However, it does not perform well in handling large dataset such as Bot-IoT dataset that represents huge amount data of botnet attacks in IoT networks. In such case, kNN often shows lower accuracy and longer execution time. Therefore, improving kNN performance in classifying IoT Botnet attack is the main concern in this study by applying several feature selection techniques. The whole research processes are conducted in Rapidminer environment using three prebuilt feature selection techniques namely, Information Gain, Forward Selection and Backward Elimination. It is finally found that Forward Selection is the best feature selection technique to improve the performance of kNN algorithm (kNN-FS) in classifying Bot-IoT dataset by achieving best results in all five evaluation criteria.
Keywords	botnet attack; IoT; machine learning; kNN; feature selection
Manuscript File	manuscript.docx (/user/manuscripts/displayFile/dbee26d885e46b991bd8ce9965926516)
PDF File	manuscript.pdf (/user/manuscripts/displayFile/dbee26d885e46b991bd8ce9965926516/latest_pdf)

Author Information

Submitting Author	Irfan Syamsuddin
Corresponding Author	Irfan Syamsuddin
Author #1	Irfan Syamsuddin
E-Mail	irfans@poliupg.ac.id

Author #2	Omar Mohammed Barukab
E-Mail	obarukab@kau.edu.sa

Manuscript Information

Received Date	30 October 2021
Revised Date	6 December 2021
Submission to First Decision (Days)	39
Submission to Publication (Days)	
Round of Revision	2
Page Count	17

Editor Decision

Decision	Reject and decline resubmission
Decision Date	22 December 2021

Review Report

Reviewer 1	Review Report (Round 1) (/user/manuscripts/review/22083001?report=15539553) Review Report (Round 2) (/user/manuscripts/review/22083001?report=16199586) Review Report (Round 3) (/user/manuscripts/review/22083001?report=16361878)
Reviewer 2	Review Report (Round 1) (/user/manuscripts/review/22091427?report=15546506)
Reviewer 3	Review Report (Round 1) (/user/manuscripts/review/22155926?report=15600479) Review Report (Round 2) (/user/manuscripts/review/22155926?report=16199579)

APC information

Journal APC:	1,800.00 CHF
Total Payment Amount:	1,800.00 CHF

Previously Published Papers

Syamsuddin, I.; Barukab, O.M. SUKRY: Suricata IDS with Enhanced kNN Algorithm on Raspberry Pi for Classifying IoT Botnet Attacks. *Electronics* **2022**, *11*, 737. doi: 10.3390/electronics11050737 (https://doi.org/10.3390/electronics11050737)

Related Papers Published in MDPI Journals

If you have any questions or concerns, please do not hesitate to contact electronics@mdpi.com (mailto: electronics@mdpi.com).

Journal: Electronics (https://www.mdpi.com/journal/electronics) (ISSN 2079-9292)

Manuscript ID: electronics-1464904

Type: Article

Title: Enhancing the Performance of kNN Algorithm in Classifying IoT BotNet Attacks using Feature Selection Techniques

Authors: Irfan Syamsuddin * , Omar Mohammed Barukab

Section: Artificial Intelligence (https://www.mdpi.com/journal/electronics/sections/Artificial_Intell)

Abstract: In the present study k-Nearest Neighbor algorithm is being studied in terms of classifying Botnet attacks within IoT environment. There are several advantages of using kNN algorithm in classification issues such simplicity, effectiveness and robustness. However, it does not perform well in handling large dataset such as Bot-IoT dataset that represents huge amount data of botnet attacks in IoT networks. In such case, kNN often shows lower accuracy and longer execution time. Therefore, improving kNN performance in classifying IoT Botnet attack is the main concern in this study by applying several feature selection techniques. The whole research processes are conducted in Rapidminer environment using three prebuilt feature selection techniques namely, Information Gain, Forward Selection and Backward Elimination. It is finally found that Forward Selection is the best feature selection technique to improve the performance of kNN algorithm (kNN-FS) in classifying Bot-IoT dataset by achieving best results in all five evaluation criteria.

The coverletter for this review report has been saved in the database. You can safely close this window.

Authors' Responses to Reviewer's Comments (Reviewer 3)

Author's Notes: Please see the attachment.

Author's Notes File: Report Notes (/user/review/displayFile/22155926/ON6Jik4v?file=author-coverletter&report=15600479)

Review Report Form

English ( ) Extensive editing of English language and style required

( ) Moderate English changes required

language and style	( ) Moderate English changes required (x) English language and style are fine/minor spell check required ( ) I don't feel qualified to judge about the English language and style

	Yes	Can be improved	Must be improved	Not applicable
Does the introduction provide sufficient background and include all relevant references?	( )	(x)	( )	( )
Is the research design appropriate?	( )	(x)	( )	( )
Are the methods adequately described?	( )	( )	(x)	( )
Are the results clearly presented?	( )	( )	(x)	( )
Are the conclusions supported by the results?	( )	(x)	( )	( )

Comments and Suggestions for Authors

The paper is interesting especially because of the IoT issue it raises. IoT infrastructure is particularly vulnerable to all kinds of attacks. The paper addresses the selected issue of using kNN to classify IoT BotNet Attacks. I would like to point out that the structure of the paper is generally correct. However, additions are required in several places in the manuscript.

Firstly, the source entries for the statements made in line 58-69 should be indicated.

Section 3.1 needs improvement. Referring only to item [37] is not sufficient. There is a lack of assumptions and precise information about the functioning of BotNet Attacks in IoT environment. There is no architecture of the IoT environment, or accurate information about the dataset on which the analysis is based. Table 1 can refer to any network traffic and does not clearly indicate that it refers to the IoT environment. This section needs to be expanded to clearly indicate how the adopted data maps to the IoT BotNet Attacks.

There is also no information on whether and to what extent the method used has practical applications for ongoing monitoring of attacks, whether it can be implemented in a production environment and what requirements would be involved. From this perspective, it would be interesting to know the calculation time and whether the proposed solution can be used for ongoing monitoring or only for historical data analysis.

Additionally, the quality of the figures should be improved.

Submission Date	30 October 2021
Date of this review	11 Nov 2021 13:55:30

Journal: Electronics (https://www.mdpi.com/journal/electronics) (ISSN 2079-9292)

Manuscript ID: electronics-1464904

Type: Article

Title: Enhancing the Performance of kNN Algorithm in Classifying IoT BotNet Attacks using Feature Selection Techniques

Authors: Irfan Syamsuddin * , Omar Mohammed Barukab

Section: Artificial Intelligence (https://www.mdpi.com/journal/electronics/sections/Artificial_Intell)

Abstract: In the present study k-Nearest Neighbor algorithm is being studied in terms of classifying Botnet attacks within IoT environment. There are several advantages of using kNN algorithm in classification issues such simplicity, effectiveness and robustness. However, it does not perform well in handling large dataset such as Bot-IoT dataset that represents huge amount data of botnet attacks in IoT networks. In such case, kNN often shows lower accuracy and longer execution time. Therefore, improving kNN performance in classifying IoT Botnet attack is the main concern in this study by applying several feature selection techniques. The whole research processes are conducted in Rapidminer environment using three prebuilt feature selection techniques namely, Information Gain, Forward Selection and Backward Elimination. It is finally found that Forward Selection is the best feature selection technique to improve the performance of kNN algorithm (kNN-FS) in classifying Bot-IoT dataset by achieving best results in all five evaluation criteria.

The coverletter for this review report has been saved in the database. You can safely close this window.

Authors' Responses to Reviewer's Comments (Reviewer 2)

Author's Notes: Please see the attachment.

Author's Notes File: Report Notes (/user/review/displayFile/22091427/9jAns2EW?file=author-coverletter&report=15546506)

Review Report Form

English: ( ) Extensive editing of English language and style required
(x) Moderate English changes required

language and style	(x) Moderate English changes required ( ) English language and style are fine/minor spell check required ( ) I don't feel qualified to judge about the English language and style

	Yes	Can be improved	Must be improved	Not applicable
Does the introduction provide sufficient background and include all relevant references?	(x)	( )	( )	( )
Is the research design appropriate?	(x)	( )	( )	( )
Are the methods adequately described?	(x)	( )	( )	( )
Are the results clearly presented?	(x)	( )	( )	( )
Are the conclusions supported by the results?	(x)	( )	( )	( )

Comments and Suggestions for Authors

There are a bunch of ambiguity in the abstract:

The written of the paper is not justified since the problem that the paper is addressed is not clear. Please clearly mention the pitfalls of the state of the arts research.

The superiority of the proposed scheme is not exposed and compared with the state of the arts.

After the comparison with the existing research, the authors/author should explain the percentage of improvement in comparison with the research in the literature.

In section 1, the author fails to provide motivations of the proposed scheme. I recommend the author to include the interesting applications of the proposed scheme.

The motivation of the practical use of the theoretic design should be clearly addressed. The best way to show this is by practical example or explanations.

Are there any deficiencies of the design in this paper and how to make further improvement, to make your results less conservative?

The author needs the help of someone whose command over the language is good to edit the paper so that composition and grammar of the language used are correct.

The authors should add and justify (by referring to published materials) the parameters of implementation setup.

Submission Date	30 October 2021
Date of this review	21 Nov 2021 21:29:39