Journal of Computer Science

Review

AI-Based Techniques for DDoS Attack Detection in WSN: A Systematic Literature Review

[1]**Mohammed Al-Naeem,** [2]**Mohammed Ashikur Rahman,**
[2]**Adamu AbuBakar Ibrahim and** [1]**M.M. Hafizur Rahman**

[1]*Deptartment of Computer Networks and Communications, College of Computer Science and Information Technology, King Faisal University, Al Ahsa 31982, Saudi Arabia*
[2]*KICT, International Islamic University Malaysia, Kuala Lumpur, Selangor, Malaysia*

Article history
Received: 29-03-2020
Revised: 28-05-2020
Accepted: 29-06-2020

Corresponding Author:
Mohammed Ashikur Rahman
KICT, International Islamic University Malaysia, Kuala Lumpur, Selangor, Malaysia
Email: ashiknsu@gmail.com

Abstract: Wireless Sensor Networks (WSNs) are currently being used in various industries such as healthcare, engineering, the environment and so on. Security is a significant issue for WSN due to its infrastructure and limited physical security. Distributed Denial of Service (DDoS) is one of the most vulnerable attacks that can be defined as attacks launched from multiple ends into a set of legitimate sensor nodes in the WSN to drain their inadequate energy resources. Nowadays, Artificial intelligence techniques are performing better accuracy than the traditional methods to detect intrusion for the various attack. This Systematic Literature Review (SLR) attempts to investigate the current status of DDoS detection techniques and to identify the most capable and effective detection system using artificial intelligence to detect distributed DoS attack. Preferred Reporting Item for Systematic Review and Meta-Analysis (PRISMA) statement is used to conduct this review. Based on 15 out of 983 that met inclusion criteria, Support Vector Machine (SVM) and Artificial Neural Network (ANN) is the most used AI-based techniques to detect distributed denial of service attack in the wireless sensor network. The performance of AI techniques-based detection system for DDoS attack in WSN is remarkable.

Keywords: Artificial Intelligence, Distributed Denial of Service, Wireless Sensor Network, SLR

Introduction

The wireless sensor network is a combination of self-configured sensors that can communicate via radio link without any centralized controlling system (Yu and Tsai, 2008). Distributed communication and sensing are the main features of a Wireless Sensor Network (WSN). In a different environment, for example, health, institutes, data centers and modern industries, the use of WSN is increasing extensively (Cheng *et al*., 2016; Ogbodo *et al*., 2017). Besides, WSN is composed of different independent, minor, minimal effort and low power sensor nodes. These nodes can accumulate data from the vast network and send data to concentrated backend elements called base stations or sinks for additional processing (Alsheikh *et al*., 2014). Security is one of the fundamental properties of any communication network, and WSNs were accompanied by a significant security flaw (Pelechrinis *et al*., 2011). Because of its untrussed environments operation, WSNs have been becoming popular to the researcher (Baig *et al*., 2006). An attacker can easily inject messages in WSNs because it uses radio communication which can be captured and inject malicious messages to perform a denial of service attack (Yu and Tsai, 2008).

DDoS attacks become a significant threat to its constancy because of the imperative nature of mobile sensors (Mazur *et al*., 2016). A Distributed DoS attack is easy to execute, but it is an excellent technique to attack the WSN (Mallikarjunan, 2016). DDoS is considered as a piece of digital fighting strategies (Shiaeles *et al*., 2012). In addition, DDoS attack can be conducted by flooding the packets to an exact server to make them nauseous in both the wired and wireless networks (Ashikur and Maruful, 2017; Patil and Gaikwad, 2015). Dispersed

Science Publications

DoS Attacks is to assemble numerous frameworks over the Internet with infected zombies/agents (Di and Er, 2007; Gavrić and Simić, 2018).

Artificial intelligence was introduced machine learning algorithms as a technique that provide huge adaptability benefits in wireless sensor network (Alsheikh *et al*., 2014). During the previous decade, WSNs have seen a progressively severe selection of advanced AI techniques (Dwivedi *et al*., 2018; Patel, 2013). Artificial intelligence emphases on biologically inspired methods such as Neural Networks (NN), fuzzy systems and evolutionary algorithms (Das *et al*., 2010).

The goal of this SLR is to identify AI-based DDoS detection system used in wireless sensor network, by assessing peer-reviewed published research papers. Specifically, the following research questions are going to address in this SLR:

RQ1: What is the status of the existing techniques for detecting distributed DoS attack in WSN?

RQ2: Which is the most capable and effective artificial intelligence-based detection scheme to detect DDoS?

That paper's structures are as follows. The methods of this SLR are discussed in section 2, and section 3 deliberates on the findings. The results will be discussed in section 4 of the article. Lastly, both the conclusion and possible research are written in section 5.

Materials and Methods

To conduct this SLR, we have followed one of the most popular protocols named Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Moher *et al*., 2009). A four-phase flow diagram and a checklist of 27 items must have to follow as a requirement of PRISMA statement (Panic *et al*., 2013). In addition, an evidence-based SLR was completed by reviewing and evaluating randomized selections available in the electronic database. Moreover, for selecting the most accurate papers to do this systematic literature review, a selection criterion must set with inclusion and exclusion criteria.

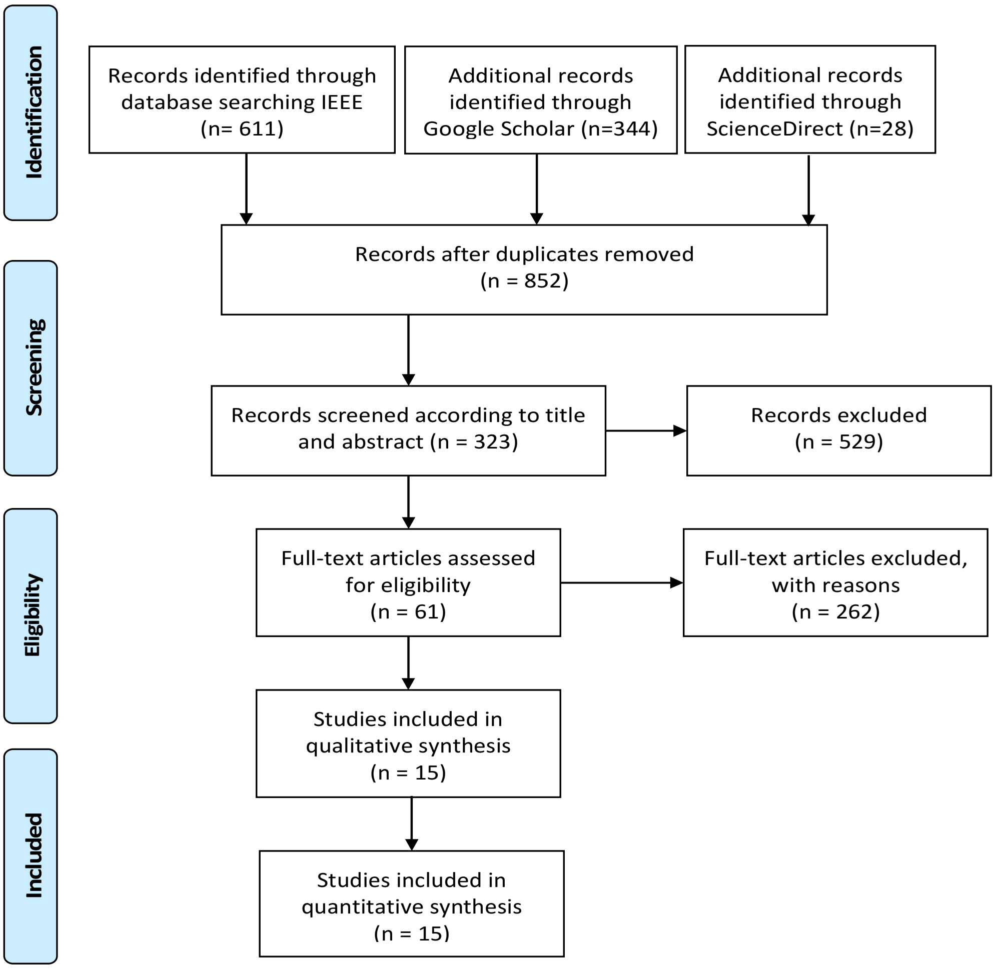
Identification
Records identified through database searching IEEE (n= 611)
Additional records identified through Google Scholar (n=344)
Additional records identified through ScienceDirect (n=28)
Screening
Records after duplicates removed (n = 852)
Records screened according to title and abstract (n = 323)
Records excluded (n = 529)
Eligibility
Full-text articles assessed for eligibility (n = 61)
Full-text articles excluded, with reasons (n = 262)
Included
Studies included in qualitative synthesis (n = 15)
Studies included in quantitative synthesis (n = 15)

Fig. 1: PRISMA diagram for SLR

According to PRISMA guidelines, the full process of four-phase flow diagram illustrates in Fig. 1. The first step of SLR is to search for relevant papers from the electronic database on wireless sensor network, for example, IEEE, ScienceDirect and Google Scholar. The searching terms were like the following:

- ((("Full Text and Metadata": Distributed denial of service) AND "Full Text and Metadata": Wireless sensor network) AND "Full Text and Metadata": Artificial intelligence)

The key terms were 'distributed denial of service', 'wireless sensor network' and 'artificial intelligence'. Furthermore, not only key terms but also the mesh words of key terms are used to search in online databases. In the first phase, 983 scientific papers were found from multiple databases during searching. Subsequent, we omitted 131 articles due to repetition.

The following two criteria were used when choosing the correct articles as inclusion criteria, which are as follows:

- Papers published from January 2013 to March 2019
- We also involved papers that were related to artificial intelligence to detect DoS/DDoS

Meanwhile, the following exclusion criteria are defined to exclude irrelevant papers:

- The published papers were not peer-reviewed articles
- Exclude those papers which were published in other languages except English
- Papers are not associated with the Wireless Sensor Network

In the second phase, after checking the title and abstract, 529 papers were excluded because of the selection criteria. In the third phase, 61 scientific papers were fulfilled the inclusion criteria after studying 323 research papers. The fourth phase is data extraction. For data extraction, 15 research papers were selected. Rest of the 46 articles were excluded from this systematic literature review. The references of the finalized papers were also used for further investigation but never contacted with authors.

Results

In this systematic literature review, we used two inclusion criteria and three exclusion criteria for selecting papers. As per the first inclusion criteria of this SLR, Papers were selected from the year 2013 to 2019. 33.33% of the Papers were selected from the year 2016. 20.0% of papers were published in the year 2013. From the year 2014, 2017 and 2019, each year, 13.33% of articles were included after following inclusion criteria. Only one paper was selected for 2015, which is 6.67. No paper was chosen from the year 2018 (Fig. 2).

Table 1 and 2 represents the answer to the second inclusion criteria.

In the single paper, multiple techniques were used and compare their performance. Table 1 shows the used methods for detecting distributed DoS attack, and Table 2 shows the used techniques for detecting denial of service attack.

In this research, 15 papers were included where 40% of articles were selected from the Institute of Electrical and Electronics Engineers (IEEE). Meanwhile, rest of the papers were published in 9 different international journals such as Engineering Applications of Artificial Intelligence, Security and Communication Networks, International journal of electronics and wireless personal communications, International Journal of Application or Innovation in Engineering and Management, Neurocomputing, International Journal of Computer Science and Network Security, Journal of Electrical and Computer Engineering and International Journal of Distributed Sensor Networks. Figure 3 presents the source of the selected paper.

After analysing 15 selected papers in this systematic literature review, 40.0% of the studies used Artificial Neural Network (ANN) to detect distributed DoS attack in the wireless sensor network. Second highest used artificial intelligence-based technique is Support Vector Machine (SVM) which is 33.33%. Decision Tree (DT), K Nearest Neighbor (KNN) and Naive Bayes algorithms are also popular techniques used to detect DDoS 13.33% both. Other AI-based techniques like fuzzy learning and K-Means are also used in WSN. Mostly used machine learning technics statistics are presented in Fig. 4.

Table 1: AI-based detection system for DoS attack

Detection	AI techniques	Selected Papers
DoS	ANN	Alrajeh and Lloret (2013)
	SVM	Al-Issa *et al.* (2019; Sharma and Parihar, 2013)
	KNN	Li *et al.* (2014)
	Hybrid	Gunasekaran and Periakaruppan (2017)
	Decision tree	Al-Issa *et al.* (2019)

Table 2: AI-based detection system for DDoS attack

Detection	AI techniques	Selected papers
DDoS	ANN	Ahanger (2018; Aljumah and Ahamad, 2016; Khan *et al.*, 2016; Saied *et al.*, 2016; Tang *et al.*, 2016)
	SVM	Mohd and Singh (2019; Wang and Lin, 2016)
	K means	Barki *et al.* (2016)
	KNN	Barki *et al.* (2016)
	Naive Bayes	Barki *et al.* (2016)
	GSA	Jadidi *et al.* (2013)
	Fuzzy Q learning	Shamshirband *et al.* (2014)

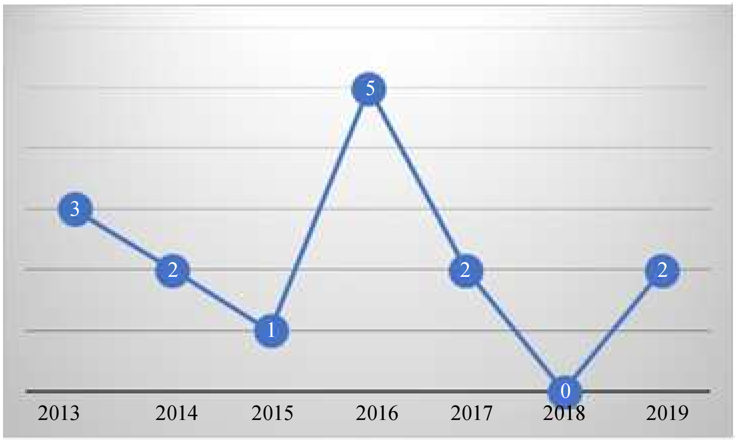

Fig. 2: Published year for selected papers

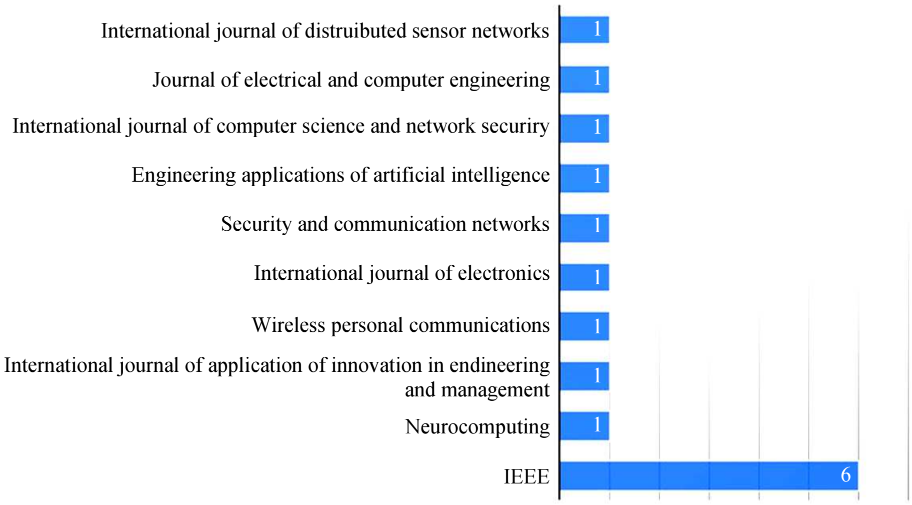

Fig. 3: Journals for selected papers

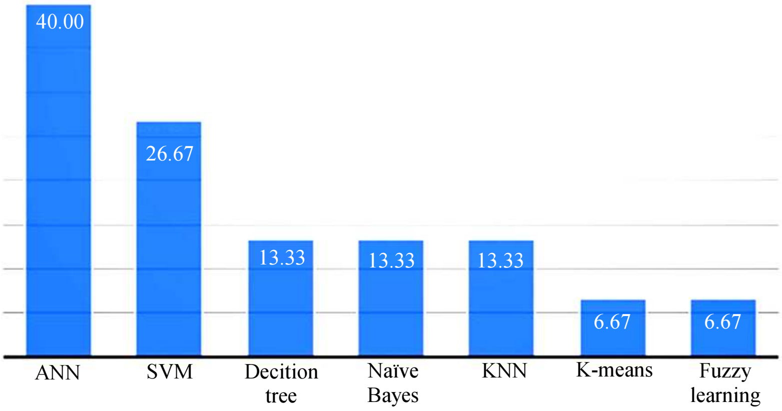

Fig. 4: Current status of AI-based detection system

Table 3: Summary table of data

Author	Year	Detection techniques	Attack	Accuracy
Mohd and Singh	2019	SVM	DDoS	97.49
Al-Issa *et al.*	2019	DT SVM	DoS	99.80
				99.60
Ahanger	2018	ANN	DDoS	99.90
Gunasekaran and Periakaruppan	2017	Hybrid Model	DoS	98.10
Khan *et al.*	2016	ANN	DDoS	99.90
Wang and Lin	2016	Improved SVM	DDoS	97.55
Saied *et al.*	2016	ANN	DDoS	98.00
Aljumah and Ahamad	2016	ANN	DDoS	95.00
Tang *et al.*	2016	DNN	DDoS	75.70
		DT		74.00
		SVM		70.90
		NB		45.00
Barki *et al.*	2016	NB	DDoS	94.00
		KNN		90.00
Li *et al.*	2014	KNN	DoS	99.00
Shamshirband *et al.*	2014	Q-Learning	DDoS	62.30
Sharma and Parihar	2013	SVM	DoS	95.00
Jadidi *et al.*	2013	GSA		99.40
Alrajeh and Lloret	2013	ANN	DoS	90.00

According to Table 1, most of the research conducted using simulated data. All the papers were focused on distributed denial of service attack. Tang *et al.* (2016) applied multiple techniques, for example, Naive Bayes, support vector machine, decision tree and deep neural network on KDD'99 dataset to detect DDoS attack and test the accuracy. They also compared the performance among those intrusion detection techniques. Among these machine learning techniques, DNN performs better than others. Barki *et al.* (2016) applied supervised and unsupervised learning techniques on simulated datasets and supervised learning techniques outperforms than unsupervised learning techniques. Many types of research were conducted using the support vector machine, and the accuracy rate was remarkable to detect DDoS attack. Artificial neural network on simulated data has been applied in multiple research (Ahanger, 2018; Aljumah and Ahamad, 2016; Alrajeh and Lloret, 2013; *et al.*, 2016; Saied *et al.*, 2016). ANN was capable of detecting DDoS attack with 99.98% accuracy rate. Table 3 also represents the accuracy rate of detection of DDoS attacks.

Discussion

ANNs are artificial intellect approaches wherein the biological traits of nerve cells have imitated the use of scientific models from the strategies that permit machines to make deductions and verdicts like an individual (Nelson and Wang, 2003). An SVM is a scientific element, an algorithm for augmenting a specific mathematical function regarding a given variety of data (Noble, 2006).

The objective of this research is to find the most capable and effective techniques to detect DDoS attack in the wireless sensor network. Researchers used many techniques to detect DDoS attack in recent years. From this systematic literature review, it is found that the accuracy rate of DDoS detection using the ANN technique was 99.98% in multiple research (Ahanger, 2018; Khan *et al.*, 2016). In addition, 98.0% and 95.0% accuracy were founded by Saied *et al.* (2016; Aljumah and Ahamad, 2016; Saied *et al.*, 2016). Apart from ANN, the performance of SVM is remarkable which is also more than 95.0% (Al-Issa *et al.*, 2019; Mohd and Singh, 2019; Sharma and Parihar, 2013; Wang and Lin, 2016). DDoS detection using Other techniques like Naive Bayes, decision tree or fuzzy Q-learning etc. varied in different researches.

Meti *et al.* (2017) conducted research to test the accuracy of machine learning algorithms like Naive Bayes, support vector machine and neural network. In that research, they identified that both ANN and SVM provide superior accuracy (approx. 80%) to detect DDoS attack. In addition, researchers calculate precision values where the precision value for ANN was 100%, SVM was 80%, and NB was 75% (Meti *et al.*, 2017).

Another research was conducted on utilisation of AI in WSN in 2017 by. Authors worked DDoS attack, quality of service, to monitor energy efficiency etc. From their findings, AI techniques can be used to improve performance and reliably for detection attacks in WSN (Matlou and Abu-Mahfouz, 2017).

Qian Mao *et al.* also published a comprehensive survey in 2018 that deep learning techniques perform better than other techniques. Authors found that deep learning algorithms can work in different network layers like data link and physical layer (Mao *et al*., 2018). In the wireless sensor network, Artificial neural network and support vector machine techniques can be used instead of other techniques.

Conclusion

WSNs are getting progressively popular currently due to their vast territory of utilisation. Since WSNs are different from other networks, it required innovation solution for security. The corresponding designs and method of arrangement of WSNs exposed to many different types of attacks. Distributed Denial of Service (DDoS) attacks are rising in frequency and becoming more complicated since it can take place in a different layer in the network. This SLR identifies that artificial intelligence techniques are most capable and effective techniques to identify and shield against the DDoS assaults in WSNs. Because of the accuracy rate of AI techniques to detect DDoS attack, artificial intelligence can be used to detect and safeguard against DDoS attacks in WSNs. In a future study, we will propose an intrusion detection system using AI and make a comparison with other existing detection systems for DDoS in WSNs. Further studies will continue to propose a novel AI-based algorithm to detect DDoS attack in WSN.

Funding Information

The authors acknowledge the Deanship of Scientific Research at King Faisal University for the financial support under RAE’D Track (Grant No. 187011).

Authors Contributions

Mohammed Al-Naeem: Contributed in reseach plan, organized the study and reviewing it critically for significant intellectual cotent, give final approval of the version to be submitted and any revised version.

Mohammed Ashikur Rahman: Make considerable contributions to conception and design and/or acquisition of data and/or analysis and interpretation of data.

Adamu AbuBakar Ibrahim: Contributed in drafting th article or reviewing it critically for significant intellectual content.

M.M. Hafizur Rahman: Contributed in drafting the article or reviewing it critically for significant intellectual content.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Ahanger, T.A., 2018. An effective approach to detecting DDoS using artificial neural networks. Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking, Mar. 22-24, IEEE Xplore Press, Chennai, India. DOI: 10.1109/WISPNET.2017.8299853

Al-Issa, A.I., M. Al-Akhras, M.S. Alsahli and M. Alawairdhi, 2019. Using machine learning to detect dos attacks in wireless sensor networks. Proceedings of the Jordan International Joint Conference on Electrical Engineering and Information Technology, Apr. 9-11, IEEE Xplore Press, Amman, Jordan, pp: 107-112. DOI: 10.1109/JEEIT.2019.8717400

Aljumah, A. and T. Ahamad, 2016. A novel approach for detecting DDoS using artificial neural networks. Int. J. Comput. Sci. Network Security, 16: 132-132.

Alrajeh, N.A. and J. Lloret, 2013. Intrusion detection systems based on artificial intelligence techniques in wireless sensor networks. Int. J. Distributed Sensor Networks.

Alsheikh, M.A., S. Lin, D. Niyato and H.P. Tan, 2014. Machine learning in wireless sensor networks: Algorithms, strategies and applications. Commun. Surveys Tutorials, 16: 1996-2018. DOI: 10.1109/COMST.2014.2320099

Ashikur, M. and S. Maruful, 2017. Intrusion detection system for wireless ADHOC network using time series techniques. Int. J. Comput. Applic., 162: 1-5. DOI: 10.5120/IJCA2017913408

Baig, Z.A., M. Baqer and A.I. Khan, 2006. A Pattern recognition scheme for Distributed Denial of Service (DDoS) attacks in wireless sensor networks.

Barki, L., A. Shidling, N. Meti, D.G. Narayan and M.M. Mulla, 2016. Detection of distributed denial of service attacks in software defined networks. Proceedings of the International Conference on Advances in Computing, Communications and Informatics, Sept. 21-24, IEEE Xplore Press, Jaipur, India. DOI: 10.1109/ICACCI.2016.7732445

Cheng, B., L. Cui, W. Jia, W. Zhao and P.H. Gerhard, 2016. Multiple region of interest coverage in camera sensor networks for tele-intensive care units. Trans. Industrial Inform., 12: 2331-2341. DOI: 10.1109/TII.2016.2574305

Das, S., A. Abraham and B.K. Panigrahi, 2010. Computational intelligence: Foundations, perspectives and recent trends. Comput. Intell. Patt. Anal. Biol. Inform.

Di, M. and M.J. Er, 2007. A survey of machine learning in wireless sensor networks-from networking and application perspectives. Proceedings of the 6th International Conference on Information, Communications and Signal Processing, Dec. 10-13, IEEE Xplore Press, Singapore. DOI: 10.1109/ICICS.2007.4449882

Dwivedi, R.K., S. Pandey and R. Kumar, 2018. A study on machine learning approaches for outlier detection in wireless sensor network. Proceedings of the 8th International Conference on Cloud Computing, Data Science and Engineering, Jan. 11-12, IEEE Xplore Press, Noida, India, pp: 189-192. DOI: 10.1109/CONFLUENCE.2018.8442992

Gavrić, Ž. and D. Simić, 2018. Overview of dos attacks on wireless sensor networks and experimental results for simulation of interference attacks. Ingenieria e Investigacion, 38: 130-138. DOI: 10.15446/ING.INVESTIG.V38N1.65453

Gunasekaran, M. and S. Periakaruppan, 2017. A hybrid protection approaches for Denial of Service (DoS) attacks in wireless sensor networks. Int. J. Electron.

Jadidi, Z., V. Muthukkumarasamy, E. Sithirasenan and M. Sheikhan, 2013. Flow-based anomaly detection using neural network optimised with GSA algorithm. Proceedings of the International Conference on Distributed Computing Systems, Jul. 8-11, IEEE Xplore Press, Philadelphia, PA, USA, pp: 76-81. DOI: 10.1109/ICDCSW.2013.40

Khan, M.A., S. Khan, B. Shams and J. Lloret, 2016. Distributed flood attack detection mechanism using artificial neural network in wireless mesh networks.

Li, W., P. Yi, Y. Wu, L. Pan and J. Li, 2014. A new intrusion detection system based on KNN classification algorithm in wireless sensor network. J. Electrical Comput. Eng.

Mallikarjunan, K.N., 2016. A survey of distributed denial of service attack. Proceedings of the 10th International Conference on Intelligent Systems and Control, Jan. 7-8, IEEE Xplore Press, Coimbatore, India, pp: 1-6. DOI: 10.1109/ISCO.2016.7727096

Mao, Q., F. Hu and Q. Hao, 2018. Deep learning for intelligent wireless networks: A comprehensive survey. Commun. Surveys Tutorials, 20: 2595-2621. DOI: 10.1109/COMST.2018.2846401

Matlou, O.G. and A.M. Abu-Mahfouz, 2017. Utilising artificial intelligence in software defined wireless sensor network. Proceedings of the 43rd Annual Conference of the IEEE Industrial Electronics Society, Oct. 29- Nov. 1, IEEE Xplore Press, Beijing, China, pp: 6131-6136. DOI: 10.1109/IECON.2017.8217065

Mazur, K., B. Ksiezopolski and R. Nielek, 2016. Multilevel modeling of distributed denial of service attacks in wireless sensor networks. J. Sensors.

Meti, N., D.G. Narayan and V.P. Baligar, 2017. Detection of distributed denial of service attacks using machine learning algorithms in software defined networks. Proceedings of the International Conference on Advances in Computing, Communications and Informatics, Sept. 13-16, IEEE Xplore Press, Udupi, India, pp: 1366-1371. DOI: 10.1109/ICACCI.2017.8126031

Mohd, N. and A. Singh, 2019. A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks. Wireless Personal Commun.

Moher, D., A. Liberati, J. Tetzlaff and D.G. Altman, 2009. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. Phys. Therapy, 89: 873-880. DOI: 10.1136/BMJ.B2535

Nelson, D. and J. Wang, 2003. Introduction to artificial neural systems. Neurocomputing, 4: 328-330. DOI: 10.1016/0925-2312(92)90018-K

Noble, W.S., 2006. What is a support vector machine? Nature Biotechnol., 24: 1565-1567. DOI: 10.1038/NBT1206-1565

Ogbodo, E.U., D. Dorrell and A.M. Abu-Mahfouz, 2017. Cognitive radio based sensor network in smart grid: Architectures, applications and communication technologies. Access.

Panic, N., E. Leoncini, G. De Belvis, W. Ricciardi and S. Boccia, 2013. Evaluation of the endorsement of the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) statement on the quality of published systematic review and meta-analyses. PLoS ONE.

Patel, K., 2013. Security survey for cloud computing: Threats and existing IDS/IPS techniques. Proceedings of the 24th International Conference on Control, Communication and Computer Technology, (CCT' 13).

Patil, A. and R. Gaikwad, 2015. Comparative analysis of the prevention techniques of denial of service attacks in wireless sensor network. Proc. Comput. Sci., 48: 387-393. DOI: 10.1016/J.PROCS.2015.04.198

Pelechrinis, K., M. Iliofotou and S.V. Krishnamurthy, 2011. Denial of service attacks in wireless networks: The case of jammers. Commun. Surveys Tutorials, 13: 245-257. DOI: 10.1109/SURV.2011.041110.00022

Saied, A., R.E. Overill and T. Radzik, 2016. Detection of known and unknown DDoS attacks using artificial neural networks. Neurocomputing, 172: 385-393. DOI: 10.1016/J.NEUCOM.2015.04.101

Shamshirband, S., A. Patel, N.B. Anuar, M.L.M. Kiah and A. Abraham, 2014. Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks. Eng. Applic. Artificial Intell., 32: 228-241. DOI: 10.1016/J.ENGAPPAI.2014.02.001

Sharma, A.K. and P.S. Parihar, 2013. An effective DoS prevention system to analysis and prediction of network traffic using support vector machine learning. Int. J. Applic. Innov. Eng. Manage., 2: 249-256.

Shiaeles, S.N., V. Katos, A.S. Karakos and B.K. Papadopoulos, 2012. Real time DDoS detection using fuzzy estimators. Comput. Security.

Tang, T.A., L. Mhamdi, D. McLernon, S.A.R. Zaidi and M. Ghogho, 2016. Deep learning approach for network intrusion detection in software defined networking. Proceedings of the International Conference on Wireless Networks and Mobile Communications, Oct. 26-29, IEEE Xplore Press, Fez, Morocco, pp: 258-263. DOI: 10.1109/WINCOM.2016.7777224

Wang, P. and W. Lin, 2016. An Efficient flow control approach for SDN-based network threat detection and migration using support vector machine. Proceedings of the International Conference on E-Business Engineering, Nov. 4-6, IEEE Xplore Press, Macau, China, pp: 56-63. DOI: 10.1109/ICEBE.2016.10

Yu, Z. and J.J.P. Tsai, 2008. A framework of machine learning based intrusion detection for wireless sensor networks. Proceedings of the International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, Jun. 11-13, IEEE Xplore Press, Taichung, Taiwan, pp: 272-279. DOI: 10.1109/SUTC.2008.39