ISSN 2278-3091

Volume 8, No.1.1, 2019

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse4781.12019.pdf

https://doi.org/10.30534/ijatcse/2019/4781.12019

# Daniel of Service Attack Detection using Classification Techniques in WSNs

**Manal A. Abdullah[1], Bdoor M. Alsolami[2], Hana M. Alyahya[3], Maha H. Alotibi[4]**

Department of Computer Science, King Abdul Aziz University,
KAU Jeddah, Saudi Arabia
[1]maaabdullah@kau.edu.sa
[2]bdoor.alsolami@yahoo.com
[3]hana.alyahya@gmail.com
[4]mahahotiby@gmail.com

## ABSTRACT

Wireless Sensor Networks (WSNs) are comprised of a large number of sensor nodes that are low in cost and smaller in size. The sensor nodes are usually placed in open areas and used in many applications. The nature of WSNs makes it threatened by many security attacks, one of them is the Denial of Service (DoS) attack which is defined as any activities that prevent the network to perform its expected functions. Intrusion Detection System (IDS) is a mechanism used to detect the malicious nodes in the network. In this paper, classification techniques are used as a tool to detect intruder node. These techniques are Naives Bayesian, Support Vector Machine (SVM), Random Forest and J48. Four types of DoS attacks are considered in this study, they are: Blackhole, Grayhole, Flooding and Scheduling attacks. The detection performance evaluation is measured by different metrics such as True Positive Rate (TP), Precision (P), Recall, False Positive Rate (FP) and ROC area. A specialized dataset for WSNs is used as an input file. Using WEKA data mining tool. The results show that the SVM classifier outperforms the other classifiers with high detection rate of 96.7%.

**Key words :** Wireless sensor networks; Denial of Service attack; Intrusion Detection System; WSN-DS; WEKA

## 1. INTRODUCTION

Wireless Sensor Networks (WSNs) has a huge number of nodes distributed over a large space with one or multiple nodes works as the base station BS. The sensor nodes work together in order to collect information and send them to the BS for analysis. WSN has become an integral part of today's applications. It can be used in various applications such as environmental, healthcare, traffic control, industry, home automation, military and other commercial applications [1]. The sensor node differs from the normal nodes in terms of their resources. Sensor nodes are small in size and low in cost. They have limited energy and memory capacity [2]. The computation of the node is affected by the communication with other nodes and the bandwidth. Due to the limited resources of the sensor nodes, the data measured by these nodes are sometimes unreliable and incorrect. A high percentage of unreliable data comes when battery power of the node is very low.

Security is a major issue of WSNs. Because of the large use of WSNs and its nature which makes it used in unattended environments, the sensor nodes become attractive to different type of attacks such as Denial of Service (DoS), Sinkhole, Sybil and Wormhole attacks. These attacks will allow the advertiser to make changes to the collected data and that may destroy the whole network. DoS attacks considered to be one of the most dangerous attacks that negatively affects the security of WSNs. In DoS attacks, the services provided by WSNs are often interrupted or stopped from work.

There are various solutions that can be used to secure WSNs such as key management, authentication, or cryptography. However, these solutions do not guarantee a full prevention of all existing attacks. As a result, an intrusion detection system (IDS) is introduced to work as a second line defense [3]. The objective of the IDS is to detect the malicious nodes and alert the administrators about that[4].

The aim of this paper is to provide a comparative evaluation study of different classification techniques used in IDS for WSNs such as Naives Bayesian, Support Vector Machine (SVM), Random Forest and J48. A specialized dataset for WSNs is used as an input and WEKA tool is used for analysis purpose. Because the dataset doesn't have information about all types of Dos attacks, only four types of DoS attacks are considered in the study. The attacks are: Blackhole, Grayhole, Flooding and Scheduling attacks. Different metrics are used to evaluate the performance of each classifier like precision, recall, true negative rate, false positive rate and ROC curve.

The rest of the paper is structured as follows: In Section 2 an overview of WSNs, classification of attacks in WSNs, DoS attacks and IDSs are presented. Section 3 introduces the system model. Section 4 shows the results and analysis of the proposed model based on the performance metrics. Section 5 concludes the paper.

## 2. BACKGROUND

### A. *An Overview of WSNs*

The improvements that have done in recent years in different types of technologies like wireless communications, digital electronics and micro-electro-mechanical systems (MEMS) technology allows to create a new kind of network called Wireless Sensor Networks. These types of networks have large number of sensor nodes that has limited resources. The sensor nodes are placed in a large area in order to collect data and process them for analysis purposes.

Due to its high capabilities, WSNs can be used in many applications such as home automation, military, healthcare, environment and other commercial applications. There are many features of WSNs, one of them is that the sensor nodes are self-organized. The other one is that the sensor nodes work cooperatively. Each node has a processor which makes it able to process the data and recognize the needed data and ignore unwanted data, so it will be easy for them to transmit the data to the base station [6].

However, WSNs can be threatened by different security attacks because of its nature and its restricted resources. In the following section a detailed information about the security attacks in WSNs will be shown.

### B. Classification of Attacks in WSNs

The nature of WSNs makes it threatened by different types of attacks. In [7], authors show two models of attacks, one is called the mote-class attack and the other is called laptop-class attacks. The attacker uses a few nodes that are inside the WSNs in the mote-class attacks. Whereas, in the laptop-class attacks, there is multiple devices that can be controlled by the attacker. Attackers can use these powerful devices to create threats that work against the WSNs. In [8], authors classified the attacks against WSNs as an active and passive attacks.

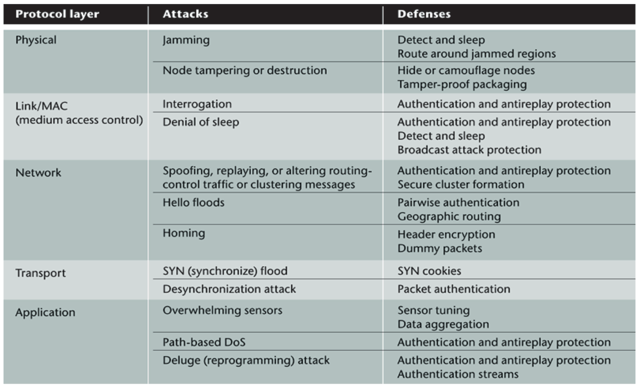
Passive attacks are attacks that listen to the messages which are transmitted between nodes. Passive attacks don't do anything to destroy the networks or its resources, it only takes the information that obtained from exchanging the messages between the nodes without changing or modifying it. Attacks against Privacy are the most common passive attacks in WSNs. It can be categorized into three types: Monitor and Eavesdropping, Traffic Analysis and Camouflage Adversaries.

However, the attacks that listen to the data exchanged between nodes and that modify and change them, are considered to be as an active attack. Active attacks have different types such as Routing attacks, Denial of service (DoS) attacks, Node outage, Physical attacks, Message corruptions, Node subversion, False node, Passive information gathering and Spoofed, Node replication Attacks, altered and replayed routing information and Node malfunction [11].

### C. DoS Attacks

Denial of service attack is defined as an event that harm the network by preventing it from performing its tasks [9].. There are many techniques used to prevent the DoS attacks but the problem with WSNs is that these techniques have heavy computation which makes it difficult to implement in WSNs as it has limited resources.

Since WSNs used in many applications and some of them are very critical and has sensitive data, DoS attacks form a real problem for WSNs. For example, an application that is used for alarming people in case of fire could be highly threatened by DoS attacks [9]. In addition, DoS attacks could also result in deaths of people or buildings. Because of that, researchers spent much of the time looking for these attacks trying to know their type and find a way to avoid them. According to [12] DoS attacks can be categorized into 5 categorizes based on the protocol layers. Figure 1 shows the attacks on protocol layers and the defense mechanisms.



| Protocol layer | Attacks | Defenses |
|---|---|---|
| Physical | Jamming | Detect and sleep<br>Route around jammed regions |
| | Node tampering or destruction | Hide or camouflage nodes<br>Tamper-proof packaging |
| Link/MAC (medium access control) | Interrogation | Authentication and antireplay protection |
| | Denial of sleep | Authentication and antireplay protection<br>Detect and sleep<br>Broadcast attack protection |
| Network | Spoofing, replaying, or altering routing-control traffic or clustering messages | Authentication and antireplay protection<br>Secure cluster formation |
| | Hello floods | Pairwise authentication<br>Geographic routing |
| | Homing | Header encryption<br>Dummy packets |
| Transport | SYN (synchronize) flood | SYN cookies |
| | Desynchronization attack | Packet authentication |
| Application | Overwhelming sensors | Sensor tuning<br>Data aggregation |
| | Path-based DoS | Authentication and antireplay protection |
| | Deluge (reprogramming) attack | Authentication and antireplay protection<br>Authentication streams |

**Figure 1:** Denial of Service attacks and defenses by protocol layers [12]

### D. IDS

The multihop distributed environments of the WSNs make it difficult for a new detection or prevention mechanisms to be designed. The difficulty comes from the unknown position of the attackers or the abnormal nodes. There are many methods designed for detecting or preventing security attacks in WSNs but none of them can find all of the security attacks. For example, many routing protocols that considered to be secure are only able to detect fewer attacks [7].

In addition, the mechanisms of media access only work with few problems like hidden-node or selfishness. A data protection from the passive attacks can be handled by the encryption techniques. However, there is a need for detection and prevention mechanisms for WSNs instead of only protecting the data itself. An IDS is one of these mechanisms.

An intrusion is defined as any events that made by the attackers in order to destroy the network resources or the sensor nodes. An IDS is used to detect the abnormal behavior of the nodes [13]. The IDS works with different layers of the network and able to control the activities of the user and the network as well. The main feature of IDS is that it makes the administrators aware about the abnormal activities, so they can stop the attack or even reduce the damage that comes from the attack.

The IDS has three main components which are monitoring, analysis and detection and alarming. The monitoring is used for internal monitoring which includes node itself or neighboring nodes. The main component is the analysis and detection which are responsible for detecting the network behavior and the activities on it and then analyze them to decide if there is an abnormal behavior or not. The alarm component is responsible for alerting the administrator when an intrusion is detected. The IDSs are only able to detect the intrusion as they are passive in nature. It only alarms the administrators without taking any further actions.

IDS can be either a signature-based IDS or an anomaly-based IDS. The signature-based IDS stores the signatures of different types of attacks in a database. This type works effectively with the well-known types of attacks, but the problem is that the new attacks are difficult to be detected because their signatures are not stored in the database.

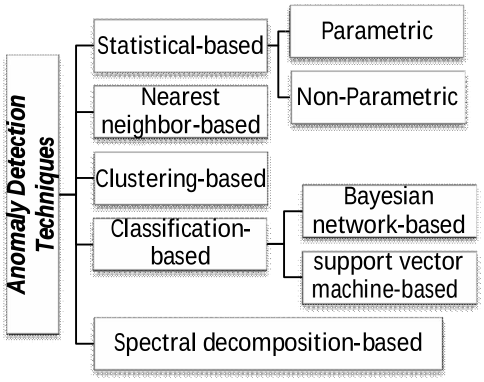


**Figure 2:** Organization of anomaly detection techniques for Wireless Sensor Networks

The anomaly-based IDS solves this problem as it can detect the new attacks. However, the well-known attacks are sometimes not detected because it doesn't use a database, instead it monitors the user's activities and the network behavior in a continuous manner. According to [14], a statistical-based, nearest neighbor-based, clustering-based, classification-based, and spectral decomposition-based approaches are the different types of anomaly detection techniques. Anomaly Detection Techniques for WSN are summarized in Figure 2.

## 3. RELATED WORK

ElMourabit and Bouirden, 2015 [15], used the well-known KDD'99dataset and provided a comparative assessment of the well-known anomaly detection techniques in IDS for WSNs. They determined additional to the normal class, 4 types of attacks. Attacks was classified as Probe, DOSS, U2R and R2. They used WEKA tool and apply several classification and clustering classifiers such as K-means, SVM, Naïve-bayes and Random Forest. The results show that the random forest classifier had the highest detection rate compared to other techniques.

Almomani, 2016 [16], created a new dataset especially for WSNs WSN-DS. The dataset has four classes of DoS attacks in addition to the normal class. It can detect the Scheduling, Grayhole, Blackhole, and Flooding attacks. In the simulation, authors used LEACH protocol which is considered to be one of the most used hierarchical routing protocols in WSNs. Network Simulator 2 (NS-2) scheme has been defined to collect data. The dataset has 23 features and it has been trained using Artificial Neural Network (ANN) to classify and detect different DoS attacks. They used WEKA toolbox with holdout and 10-Fold Cross Validation for splitting the data. The results show that the specialized dataset makes a great improvements to the IDS as it gives higher accuracyrate.

Sumitha and Kalpana, 2015[17] have focused on DoS attack, as it is popular and affects the environment severely. MATLAB software is used to simulate a WSN based on LEACH protocol. In this work, a new hybrid technique has been proposed by combining Ant Colony Optimization with Hidden Markov Model (ACO +HMM) which provides better performance than other techniques. The results were compared with earlier algorithms such as ACO and HMM.

Horng *et al.*, 2011 in [18], proposed a new system to detect WSNs attacks. The new IDS uses SVM technique and the KDD Cup 1999 dataset to evaluate the performance. The authors compared their new system with other detection systems that uses the same dataset. The results show that their system gives higher detection rate in Probe and Denial of Service attacks compared to the other systems. Also, the performance in overall accuracy is the best.

In [19],Wazid and Das have used hybrid k-means clustering with anomaly detection technique. OPNET simulator was used to simulate the WSN and to collect the dataset. The resulted dataset contains analysis of traffic data and the end to end delay is also performed. The data has been clustered using WEKA 3.6. Two types of anomalies attacks (blackhole and misdirection) are activated in the network.

## 4. PROBLEM STATMENT

As WSNs used in critical and sensitive applications, WSNs are highly vulnerable to different type of attacks which may threats the system security and performance. DoS attacks form a real problem for WSNs as explained earlier. As a sequence, several IDS have been designed with the aim of detecting or reducing the effect of such attacks and a lot of research works have been done to handle the Dos attacks specially. However, there was no previous work that uses the WSN-DS dataset to perform intrusion detection of Dos attacks in WSNs. In this work, the authors show how different classification techniques can be used with the WSN-DS dataset to detect the Dos attacks specifically. Therefore, knowing the best classifier among the other will help in reducing the impact of those attacks in the WSNs. The next sections will explain the system model and the classification techniques used in more details.

## 5. IDS MODEL

In this section, authors will present detailed presentation of the proposed IDS model. It will provide an information about the dataset, the types of attacks and finally, the classification methods used in this paper.

### A. WSN-DS Dataset

In this paper, the classification and evaluation process are done using a specialized dataset for WSNs called WSN-DS [16]. The dataset can detect four types of DoS attacks in addition to the normal behavior (no attack). The dataset used the Low Energy Aware Cluster Hierarchy (LEACH) routing protocol to collect the dataset. The network area was 100 m x100 m and the number of nodes were 100 divided into 5 clusters. The dataset collected using the Network Simulator 2 (NS-2) and the collected data has 23 features.

A sample of this dataset contains 32 records and an additional 72 records added to form a total of 104 records by following the same algorithms that used in [16]. A subset of features is selected to create the final dataset used by this paper. The final dataset contains 104 records and 19 features. The dataset divided into five classes; Blackhole, Grayhole, Flooding, Scheduling and Normal.

## B. Attacks Model

This paper focuses on four type of DoS attacks: Flooding, Scheduling, Grayhole, and Blackhole attacks. In this section, a flowchart of the processes followed to detect the attack is shown in figure 3. To guarantee suitable distribution of the attacker nodes, we divide the network terrain into 10 areas. Thus, the attackers' ratios per the simulation scenario were distributed arbitrarily within these areas.

*Flooding Attack*: is a kind of DoS attack by which the attacker affects LEACH protocol by multiway. Flooding attack work by sending huge number of advertising Cluster Head CH massages with high broadcast energy. Accordingly, once sensors receive this messages, it will expend sensors energy also it will waste time to decide which CH to join. Furthermore, the attacker tries to cheat sensors node to choose it as a CH specially the nodes that are located on a remote distance from it to consume their energy[16].

*Scheduling attack:* happens throughout the setup phase of LEACH protocol, when CHs establish Time Division Multiple Access (TDMA) schedules for the data transmission time slots. Here the attacker works as a CH. Also, it will allocate all sensor nodes the same time slot to send data. To do this the attacker modifying the behavior from broadcast to unicast TDMA schedule. Such convert will cause packets collision which leads to data loss.

## C. Intrusion Detection Techniques

*Naive Bayes algorithm:* is the regulated learning strategy. Probabilities of each ascribe which has a place with each class are considered for an expectation. This calculation expect that the likelihood of each ascribe having a place with a given class esteem does not rely upon every other quality. In the event that the estimation of the quality is known the likelihood of class esteem is called as the restrictive probabilities. Information examples likelihood can be discovered by increasing all qualities contingent probabilities together. Forecast can be made by computing each class occurrence probabilities and by choosing the most astounding likelihood class esteem [15].

Naive Bayes classifier is typically worked in WSNs since it is elegance, robustness, and simplicity. Many changes have been presented, by the data mining, statistical, machine

*Blackhole Attack:* is a type of attacks that affects LEACH protocol. It causes DoS by advertising itself as a CH for other nodes at the beginning of the round. Therefore, several nodes that have joined the fake CH through this round will send the data packets to it in order to send them to the Base Station. The attacker will keep dropping these data packets and not sent them to the Base Station.

*Grayhole Attack:* is a type of attacks that affects LEACH protocol. It causes DoS by advertising itself as a CH for other nodes. Then, when the fake CH receives from other nodes, it drops some packets either randomly or selectively. Also, it prevents data packets from reaching the Base Station. To apply Grayhole and Blackhole attack in the simulation environment, some attackers' intensities (10%, 30%, and 50%) have been added arbitrarily. These attackers which act as CHs will drop all the packets (blackhole) or some packet (Grayhole) relayed through them in their way to the Base Station learning, and pattern recognition together make it more flexible. New method was suggested in [15] to classify the faulty nodes by Naïve Bayes classifier. This Naïve Bayes outline was arranged for performing WSN faulty sensor(s) detection. By using Naïve Bayesian classifier, a new attribute, the end-to-end transmission time of each packet arrived at the sink is examined for deciding the network status. This procedure doesn't include any extra protocol and additional resource consumption of sensor, it proposes a catalogue of suspicious faulty nodes to the user.

*Support Vector Machine SVM Classifier:* Mainly for characterization issues. N-dimensional component space is considered to plot every datum thing as a point with the estimation of each element as a specific facility. At that point, grouping is made by finding the hyper-plane that separate the two classes great. Bolster Vectors are the co-ordinates

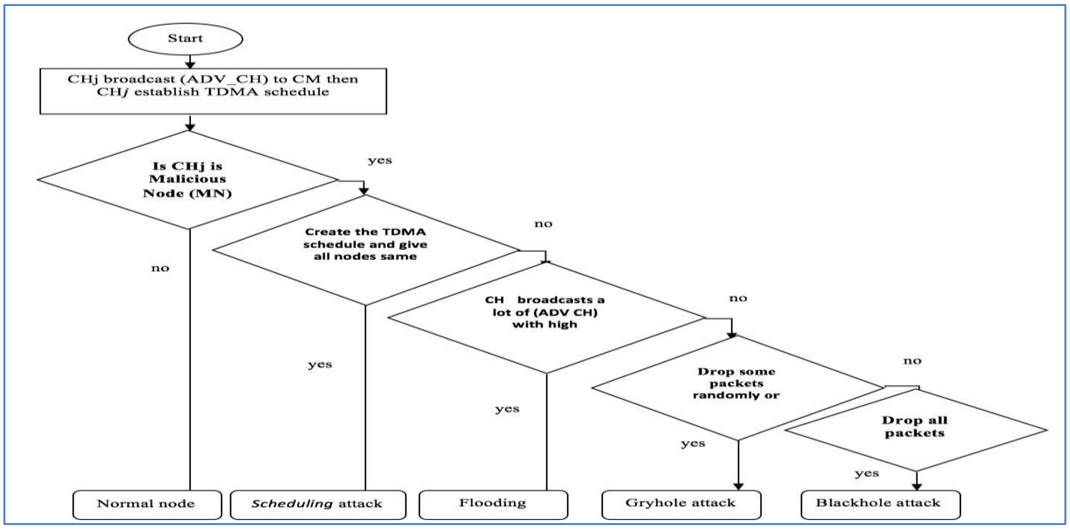

Start
CHj broadcast (ADV_CH) to CM then CHj establish TDMA schedule
Is CHj is Malicious Node (MN)
yes
no
Create the TDMA schedule and give all nodes same
no
yes
CH broadcasts a lot of (ADV CH) with high
no
yes
Drop some packets randomly or
no
yes
Drop all packets
yes
Normal node
Scheduling attack
Flooding
Gryhole attack
Blackhole attack

**Figure 3:** Flowchart of the proposed Intrusion Detection System

of explicit perception that lies nearest to the fringe. If there should arise an occurrence of SVM, preparing tests are partitioned into various subsets called as help vectors, the choice capacity is determined by these help vectors [13].

*J48:* is a basic C4.5 choice tree for grouping. This strategy produces a parallel tree which is made to show the grouping procedure. At the point when the tree is built, it is useful to all tuple in the database and results in grouping for that tuple.

*Random forests classifier*: uses a collection of data mining techniques which works the way as the decision trees. It builds a variety of decision trees at training time and resulting the class, that is the mode of the classes result by separate trees. The Random tree, then again, includes building of several random decision trees.

Another information mining approach concentrated on arbitrary woods was proposed to arrange and portray an extensive scale physical condition in [20]. The recommended information mining detailing, gives better act access terms of exchange off among precision and vitality effectiveness. Contrasted with a solitary choice tree calculation, Random Forests run successfully on enormous datasets with an improved act.

## 6. RESULTS AND ANALYSIS

A set of experiments were applied on WSN-DS dataset using different classification methods such as naïve bayes, j48, random forest and SVM. Different performance metrics are used for evaluation like True Positive Rate (TP), Precision (P), Recall, False Positive Rate (FP) and ROC area. WEKA tool was used in the experiments to prepare the dataset and calculate the detection rate for each classifier. WEKA is open source software implemented using java programming language. It can be used for data preprocessing, clustering, classification, association rules, regression, and visualization [21]. The main goal of these experiments was to evaluate each classifier and find out the method that best achieve high detection rate.

To identify how each classifier correctly detect the attacks, the True Positive Rate (TPR), and False Positive Rate (FPR) were used where TPR is used to show the percentage of attacks that correctly identified by each classifier and FPR used to represent rate of normal cases that identified as attacks by each classifier. Figures 4, 5, 6 and 7, summarize TPR and FPR for each method. Figures 4 show the TPR and FPR when using naïve Bayes method. It correctly classified all type of attacks but it incorrectly classified some Normal instances. Figure 5 shows the TPR and FPR when using J48 method. It correctly classified all attacks type except Grayhole attack. Figure 6 shows the TPR and FPR when using Random forest method. It correctly classified all attacks type except Scheduling attack. Figure 7 shows the TPR and FPR when using SVM method. It correctly classified all attacks types but it incorrectly classified some Normal instances. Table 1 shows number of records.

**Table 1:** Number of Records

| Class | Instances Number |
|---|---|
| Normal | 75 |
| Grayhole | 8 |
| Flooding | 7 |
| Blackhole | 8 |
| Scheduling | 6 |

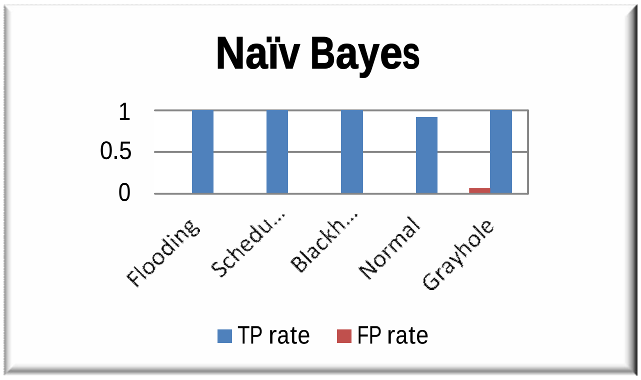


**Figure 4:** True Positive and False Positive rates with Naïvc Bayes

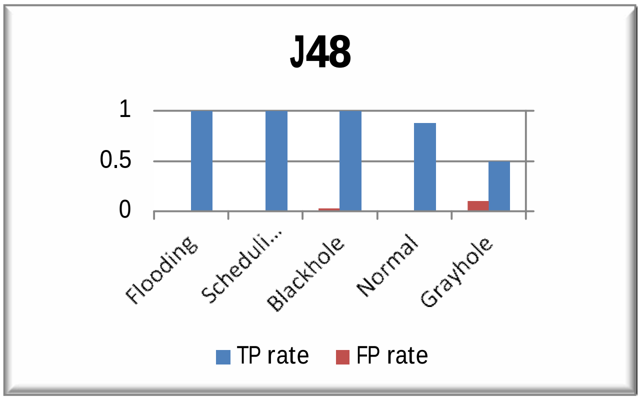


**Figure 5:** True Positive and False Positive result with J48

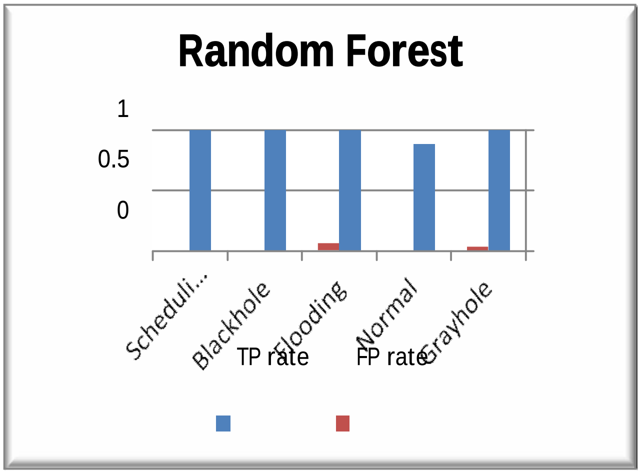


**Figure 6:** True Positive and False Positive rates with random forest

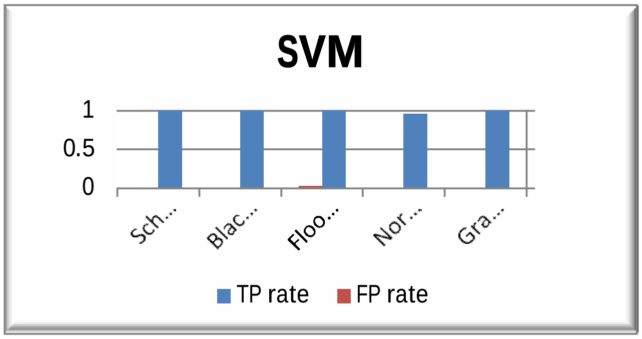


**Figure 7:** True Positive and False Positive rates with Support Vector Machine

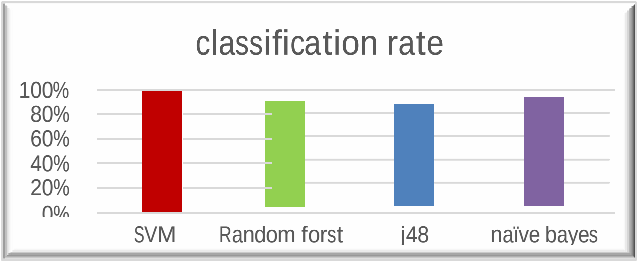


**Figure 8:** Classification rate

A comparison between all methods are shown in figure 8. It can be clearly seen that among all the classification methods, SVM is the best one as it has high detection rate compared to the other. The Naïv Bayes and Random Forest classifiers come next. However, j48 is the worst as it has the lowest detection rate.

## 7. CONCLUSION AND FUTURE WORK

This paper evaluates and compares different data mining techniques for intrusion detection systems applied for WSNs. From the obtained results, it can be concluded that SVM classifier outperforms the other classifiers. Among the four classification methods used in the experiments, SVM is the best technique for detecting the abnormal behavior of the node as it can detect 96% of the DoS attacks.

Because of the constrained dataset utilized in this work, another total dataset for WSNs will be made as future work. There is no online dataset available for IDS in WSNs. We will try to apply other data mining techniques such as clustering using k-means algorithm. In addition, we will try to add more attacks that considered as DoS attacks such as Sybil, Sinkhole and Wormhole.

## REFERENCES

[1] N. Marriwala and P. Rathee, “An approach to increase the wireless sensor network lifetime,” in *2012 World Congress on Information and Communication Technologies*, 2012, pp. 495–499. https://doi.org/10.1109/WICT.2012.6409128

[2] R. Mitchell and I.-R. Chen, “A survey of intrusion detection in wireless network applications,” *Comput. Commun.*, vol. 42, pp. 1–23, 2014. https://doi.org/10.1016/j.comcom.2014.01.012

[3] H. Y. Lin and T. C. Chiang, “Intrusion Detection Mechanisms Based on Queuing Theory in Remote Distribution Sensor Networks,” *Adv. Mater. Res.*, vol. 121–122, pp. 58–63, Jun. 2010. https://doi.org/10.4028/www.scientific.net/AMR.121-122.58

[4] A. Abduvaliyev, A. S. K. Pathan, Z. Jianying, R. Roman, and W. Wai-Choong, “On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks,” *Commun. Surv. Tutorials, IEEE*, vol. 15, no. 3, pp. 1223–1237, 2013. https://doi.org/10.1109/SURV.2012.121912.00006

[5] M. M. N. Aldeer, “A summary survey on recent applications of wireless sensor networks,” in *2013 IEEE Student Conference on Research and Developement*, 2013, pp. 485–490. https://doi.org/10.1109/SCOReD.2013.7002637

[6] S. Meenatchi and S. Prabu, “www.ijptonline.com A CLUSTER BASED LOAD BALANCING TECHNIQUE FOR INCREASING THE WIRELESS SENSOR NETWORK LIFE TIME,” *Int. J. Pharm. Technol. IJPT*|, vol. 8, no. 3, pp. 4716–4727, 2016.

[7] N. A. Alrajeh, S. Khan, and B. Shams, “Intrusion detection systems in wireless sensor networks: A review,” *International Journal of Distributed Sensor Networks*, vol. 2013. Hindawi Publishing Corporation, 2013.

[8] H. Sedjelmaci and M. Feham, “Novel Hybrid Intrusion Detection System For Clustered Wireless Sensor Network,” *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 4, pp. 1–14, Jul. 2011. https://doi.org/10.5121/ijnsa.2011.3401

[9] G. Padmavathi and M. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” *IJCSIS) Int. J. Comput. Sci. Inf. Secur.*, vol. 4, no. 2, 2009.

[10] K. Pongaliur and L. Xiao, “Sensor node source privacy and packet recovery under eavesdropping and node compromise attacks,” *ACM Trans. Sens. Networks*, vol. 9, no. 4, pp. 1–26, Jul. 2013. https://doi.org/10.1145/2489253.2489267

[11] K. Kaushal and V. Sahni, “DoS Attacks on different Layers of WSN: A Review,” *Int. J. Comput. Appl.*, vol. 130, no. 17, pp. 975–8887, 2015.

[12] D. R. Raymond, S. F. Midkiff, A. Wood, and J. Stankovic, “Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses,” pp. 74–81, 2008.

[13] M. C. Belavagi and B. Muniyal, “Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection,” *Procedia Comput. Sci.*, vol. 89, pp. 117–123, 2016. https://doi.org/10.1016/j.procs.2016.06.016

[14] Y. Zhang, N. Meratnia, and P. Havinga, “Outlier Detection Techniques for Wireless Sensor Networks: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 12, no. 2, pp. 1–12, 2010. https://doi.org/10.1109/SURV.2010.021510.00088

[15] Y. El Mourabit and A. Bouirden, “Intrusion Detection Techniques in Wireless Sensor Network using Data Mining Algorithms: Comparative Evaluation Based on Attacks Detection,” *IJACSA) Int. J. Adv. Comput. Sci. Appl.*, vol. 6, no. 9, 2015.

[16] I. Almomani, B. Al-kasasbeh, and M. Al-akhras, “WSN-DS : A Dataset for Intrusion Detection Systems in Wireless Sensor Networks,” vol. 2016, 2016.

[17] S.Sumitha Pandit and Dr.B.Kalpana, “Hybrid Technique for Detection of Denial of Service (DOS) Attack in Wireless Sensor Network,” *Int. J. Adv. Netw. Appl.*, vol. 7, no. 2, pp. 2674–2681, 2015.

[18] S.-J. Horng *et al.*, "A novel intrusion detection system based on hierarchical clustering and support vector machines," *Expert Syst. Appl.*, vol. 38, no. 1, pp. 306–313, 2011.
https://doi.org/10.1016/j.eswa.2010.06.066

[19] M. Wazid and A. K. Das, "An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol. 90, no. 4, pp. 1971–2000, Oct. 2016.

[20] B. C. P. Lau, E. W. M. Ma, and T. W. S. Chow, "Probabilistic fault detector for Wireless Sensor Network," *Expert Syst. Appl.*, vol. 41, no. 8, pp. 3703–3711, Jun. 2014.
https://doi.org/10.1016/j.eswa.2013.11.034

[21] A. Tesfahun and D. L. Bhaskari, "Intrusion Detection Using Random Forests Classifier with SMOTE and Feature Reduction," in *2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies*, 2013, pp. 127–132.
https://doi.org/10.1109/CUBE.2013.31

[22] R. R. Bouckaert *et al.*, "WEKA---Experiences with a Java Open- Source Project," *J. Mach. Learn. Res.*, vol. 11, pp. 2533–2541, 2010.