New Approach to Determine DDoS Attack Patterns on SCADA System Using Machine Learning

Fahd A. Alhaidari
College of Computer Science and Information Technology,
Imam Abdulrahman Bin Faisal University,
P.O. 1982, Dammam, Saudi Arabia
faalhaidari@iau.edu.sa

Ezaz Mohammed AL-Dahasi
College of Computer Science and Information Technology,
Imam Abdulrahman Bin Faisal University,
P.O. 1982, Dammam, Saudi Arabia
emaldahasi@iau.edu.sa

***Abstract* — Recently, the importance of Supervisory Control and Data Acquisition (SCADA) systems has grown for many industries around the world. These systems are controlling many vital infrastructures such as grids of power, plants, and water treatment systems. In fact, nowadays SCADA systems cannot be isolated from the public and thus being more vulnerable and exposed to many malicious attacks. Several studies have reviewed the latest developments in cyber-security risks for SCADA systems and found that many factors are responsible for increasing the amount and the level of risks on modern control systems. Among such factors are the network architecture and the reliance on standard technologies that have known vulnerabilities. In this paper, we attempt to improve a framework of SCADA system against Distributed Denial of Service (DDoS) attacks using three machine learning algorithms (i)J48; (ii) Naive Bayes; (iii) Random Forest to determine the attack patterns. These algorithms were trained and evaluated on KDDCup'99 dataset. The preprocessing phase of the dataset was conducted based on the goal of the paper and the obtained results showed that the best classification is obtained using Random Forest classifier (RF) with 99.99% accuracy rate, while Naïve Bayes classifier has the lowest accuracy rate of 97.74%.**

Keywords— SCADA, Cybersecurity, Denial of Service Attack, DoS, DDoS, Cyberattack, Simulation, Computer Network Attack.

I. INTRODUCTION

SCADA refers to Supervisory Control and Data Acquisition which is a system that concentrates on the supervisory level. It is a pure software package that is placed over the devices that are connected to it generally through Programmable Logic Controllers (PLCs) or other commercial devices [1]. The most important usage of SCADA systems is to monitoring the vital national infrastructure such as intelligent networks, power transmission, generation, networks of transport, and also is used to manage public facilities such as controlling building [2]. SCADA systems are known as electronic physical systems with wired (wireless) networks which interfere with several controlling systems and devices, hence providing a large attack surface [2][3].

In general, a SCADA system has the following components as it is shown in Fig. 1.

1) Tools influenced by transactions of the processes.
2) Equipment that being connected to the devices.
3) Local processors that gather the data and are connected with the sites tools such as PLCs, Remote Terminal Units (RTUs), Intelligent Electronic Device (IED), or Process Automation Controller (PAC).
4) Communication media of short-range that carries out the data and signals between local processors and the other equipment of operating.
5) Host computers that work as a central point of human censoring and control processes. Actually, it is also known as Master Terminal Unit (MTU), the server of SCADA, or PC with Human Machine Interface (HMI).
6) Communication media of Long-range among local processors and host computers via network connections [4].

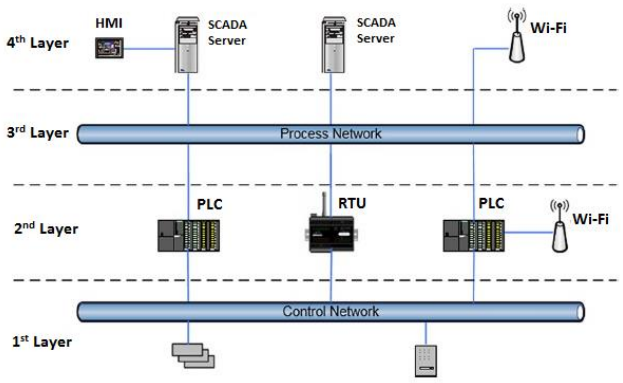

Fig. 1. A general architecture for SCADA system adopted from [2]

The communication among components in the older systems was done through their own dedicated networks and own protocols, thus it was assumed the security of SCADA systems can be achieved via isolation [5]. However, SCADA systems are becoming more open, due to the rapid growth of these systems and their usage of ready-made components, as well as the development of hybrid protocols such as (Modbus / TCP, Omron, ISO-TSAP). The SCADA system is accessible through the Internet, which means that it is exposed to several different cyber-attacks [6].

Several researches have presented several methods of assessing the risks of cyber security on SCADA systems. Also, there are many comprehensive surveys in the literature on SCADA considering simulation studies, modeling, and related techniques [2][7][8].

To ensure the protection of vital assets in SCADA systems, it is required to identify vulnerabilities and gaps in the defenses and control mechanisms seeking for possible violations that might led to compromising systems [9] [10]. In fact, this can be achieved by: 1) Techniques for detecting weaknesses in the system and determining the level of protection against any potential attack. 2) Using tools to gather information related to the intended target system.

978-1-5386-8125-1/19/$31.00 ©2019 IEEE

Several mitigation and detection techniques have been proposed in the literature to protect SCADA systems from being attacked by DDoS attacks. Among such techniques are the Machine Leaning techniques that showed a high accuracy in detecting different sorts of attacks in the real time including DDoS attacks [11] [12][13][14].

In this paper, we attempt to provide a possible security solution via a simulation framework that utilizes the Machine Learning techniques to detect Distributed Denial of Service (DDoS) attacks on SCADA systems. Mainly, we consider three Machine learning algorithms (i) J48; (ii) Naive Bayes; (iii) Random Forest to determinate the attack patterns. In addition, the paper presents literature review and background about SACDA systems issues as well as about DDoS attacks.

The rest of the paper is organized as follows. The background and literature review on SCADA and DDoS attacks are presented in Section 2. Section 3 presents the experimental work and proposed technique. The results along with the corresponding discussion are shown in Section 4. Finally, the Conclusion and future work are given in Section 5.

II. BACKGROUND AND LITERATURE REVIEW

Internet connectivity offers many useful services such as remote connection and scalability, but on the other hand it also makes systems such as SCADA more vulnerable to the global threats of cybersecurity. Therefore, number of vulnerabilities, security issues, and security case studies were accounted and reported in the literature. Few examples of such case studies that show actual threats and attacks targeted SCADA systems are:

1) The "water breach" incident, an incident lasting more than three months with controlling more than 150 sewage pumping stations [9].
2) Accident of "Nuclear power plant" where the Slammer worm closed the safety control system in Ohio [5][10].
3) The "Stuxnet worm" attack, it was discovered in June 2010, targeting Iranian nuclear facilities. It has been considered as the latest high-level attack on the SCADA systems [15].
4) The "Wastewater Infrastructure" attack happened in Australia resulting in a leak of around 212000 gallons of raw sewage. The perpetrator of the attack was an insider, Mr. Vitek Boden, who spread unauthorized commands of radio to the SCADA system [16].

Moreover, other incidents listed by several studies in the database of industrial security accidents illustrate the vulnerability of SCADA systems and confirm that these attacks have devastating consequences on the environment and the human safety.

One of the continuing attacks facing the Internet is the DDoS attack. It is a constant cyber-threat and usually rises major concerns for the computer and information security. There are many kinds of DDoS attacks such as SYN Flooding, ICMP Flooding, and UDP Flooding [17][18]. In fact, there are many different studies aim to detect DDoS attacks for example: 1) Commercial Hardware appliances. 2) Machine learning techniques. 3) Partial Rank Correlation-based Detection (PRCD) scheme to detect both low-rate and high-rate DDoS attacks [19]. 3) Metric named "Mean Inter-Packet Delay Variation" (MI-PDV) to distinguishing LDDoS attacks and benign TCP flows [19]. 4) Deep Learning techniques [20].

A. Cyber security methods and techniques for SCADA systems

A group of researchers in [7] reviewed the latest developments in the cybersecurity risk assessment applied to SCADA systems using a well-established institutional research methodology. Their work covered a range of security and risk related studies on SCADA where about 24 risk assessment methods were applied in the context of the SCADA systems. They suggested an intuitive categorization for the studied methods as follows. First class: Activity-specific methods and Elaborated guidelines. Second class: Formula-based methods and Model-based methods. Third class: Qualitative and Quantitative.

In [2], authors offered a comprehensive survey on techniques that can be used for detecting weaknesses in the system and determining the level of protection against potential attacks. Examples of such techniques presented in the study are: Simulation frameworks, Test beds, Simulating SCADA attacks, Mathematical modelling, Probabilistic modelling, and Risk modelling and assessment. This helps both developers of system and service providers to evaluate their systems before commissioning, and helps users to understand provisions of security and comply with all regulatory requirements. The authors also described tools that can be used to collect information about the intended system including Scanning tools, Penetration testing, Machine learning, Network intrusion detection systems (IDS), Intrusion prevention systems (IPS), Honeypots, Security information and event management (SIEM), Ethical or white-hat hacking, and Forensic science.

B. SCADA system in different sectors

SCADA systems are used in different sectors such as chemical production plants which are a combination of electromechanical systems comprised of giant silos, conveyors, mixers, rotating heads, dust absorption units, and packaging units.

A study in [17] presented an application of SCADA systems on construction chemicals production plants in Turkey that used to use traditionally manual methods to obtain the finished product. They monitored a medium sized construction chemical plant with SCADA system called Reliance Design 4 and PLC program called ABB Control Builder Plus. The study compared between the automated system and the traditional manual system in term of the amount of product produced in an hour considering the following factors: a daily slice of the facility, the amount of electricity consumed, and the number of workers in the facility. The outcomes of such comparison showed that the automated system is %75 faster with an average of 800 packages product produced in a month in automated system compared to about 450 packages in the non-automated system.

In [15], authors presented some modern statistics on cyber-attacks and the possible caused damages. The water and sanitation facilities should implement countermeasures for preventing or minimizing damage of such attacks targeting their controlling systems. The study presented the main challenges of the water and sanitation industry as follows. 1) The high interdependence of their business systems and control systems. 2) The wide variation in the

equipment of industrial control. 3) Many cybersecurity standards across sectors. 4) Differences in resource equipment approaches to achieve security standards. In addition, they explained the possible countermeasures that can be used to defeat such challenges such as selecting safety standards, analyzing gaps, and analyzing vulnerabilities/risks. Finally, they emphasized that the facilities should utilize their limited resources for developing and implementing the necessary programs which are designed to increasing security over the years. The implementation of cyber-security must not be costly, and the improvements can be achieved through policies, procedures, training, and awareness-raising.

C. *Detection of DDoS Attacks*

Authors in [18] sought to analyze DDoS attacks and develop the technologies to counter their influences. To achieve that aim, they used commercial hardware for demonstrating and measuring the effectiveness of DDoS attacks on a victim. As a result of their analysis of weaknesses, they suggested the following recommendations:

1) There is a need for a collaborative cybersecurity mitigation strategy involving individual users of networks, leadership within organizations, and the network security experts.
2) Governments should provide support through international legislation, research, development, and participation.

The two-layer filtering approach is developed in [19] for detecting both high and low rate attacks. In order to assess the performance of proposed methods, the researchers used ns-2 simulation tool. The first layer, named average filter with the metric1, is used for detecting the high-rate DDoS attacks. The second layer, named Discrete Fourier transform (DFT) with the metric2, is used for detection low-rate DDoS attacks. The proposed methods are distinguished as easy for implementing and can detect high and low rate DDoS attacks at the same time. However, when the high-rate and low-rate attacks are close to each other, the accuracy of detection is low.

A study in [20] proposed a detection model of DDoS based on deep learning in network environment and the results showed much better performance compared with traditional machine learning techniques. The model consists of 1) Input layer, 2) Forward recursive layer, 3) Reverse recursive layer, 4) Fully connected hidden layer and 5) Output layer. They used the Recurrent Neural Network (RNN), long short-term memory (LSTM), and convolutional neural network (CNN). All attack packets are mixed with a random number of legitimate packets to get input data for the training model.

In [21], authors proposed an automatic defense model for detecting DDoS attacks using a supervised learning model, Support Vector Machines (SVM). The selection process was in a random way, 60% of the dataset, 809 normal, and 809 anomalous. The results showed a significant improvement (approximately 10 %) in the classification accuracy.

In [22], they presented and discussed a variety of different solutions and methods for detecting DDoS attacks. Some of those methods used continuously in the network environment to detect and mitigate DDoS attacks as presented in Fig. 2.

IP Traceback technique is used as an integrated defense against DDoS attacks by identifying the origin or the source of packets transmitted through the Internet. The methods of traceback are supported by "Packet Marking" and the major techniques used to mark the packets are PPM and DPM. The Entropy method is used to distinguish the difference between the traditional movement and the movement of the DoS attacks where the difference is defined as the change in random flows on the router. Intrusion Detection and Prevention System (IDS/IPS) is a system in the appearance of an application that censoring the network for any suspicious state; and then sends a report to the administrator for taking an action. Examples of traditional IDS/IPS technologies are Signature-based detection and Anomaly-based detection [22].

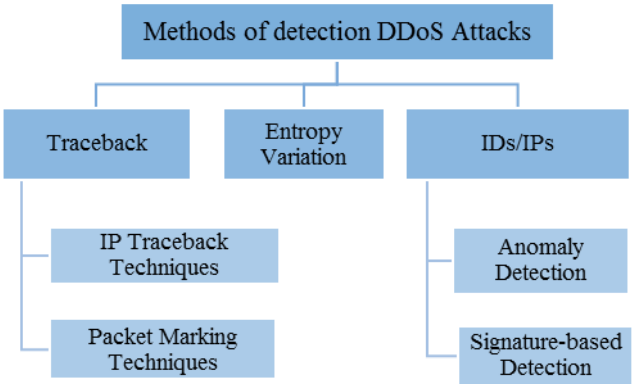

Fig. 2 Methods for detecting DDoS attacks

D. *SCADA System with DDoS Attacks*

In [23], they examined the weaknesses in the SCADA system in hydroelectric power stations and looked for securing the infrastructure of wireless information systems. The study provided a simulation-based analysis of the SCADA system vulnerabilities, particularly related DDoS attacks, using the OPNET (Optimized Network Engineering Tool) [24]. They carried out two scenarios: 1) A model without an attack on the infrastructure of the network. 2) A model with DDoS attacks.

The aim of the study in [25] is to tackle both the fault detection and the time synchronization of the data flow in smart power grid environment. They considered the most two popular and common cyber-attacks which are DoS attack and Man-In-The-Middle attack (MIM). The OMNeT++ simulator was used with NED (Network Description) file and programming logic. The strength of the proposed framework is reflected by its containment of various attack scenarios and its capability to provide a very real and exact behavioral analysis during cyber-attacks in the simulated environment.

In [26], they analyzed the behavior of the smart power grid with both the presence and absence of cyber-attacks. They used several simulators and tools to conduct the experiments including an Objective Modular Network Testbed in C++ (OMNeT++) and Open-source Distributed System Simulator OpenDSS. The integration between the network simulator and the power generation simulator was done using Phasor Measurement Units (PMU) used as a data exchange bridge moving the data from the power generation toward the network simulator. The data center collects the data from the sensors and converts it to any connected

gateway. However, the main challenge of the proposed framework is the issue of combining two dissimilar simulators and the concerns of time synchronization.

III. Experimental Work and Proposed Technique

DDoS attacks can compromise SCADA systems by targeting and breaking down either the PLC or the HMI through sending too many packets within a very small time frame [5]. Fig. 3 shows a simple SCADA system along with the attacker hitting the system components.

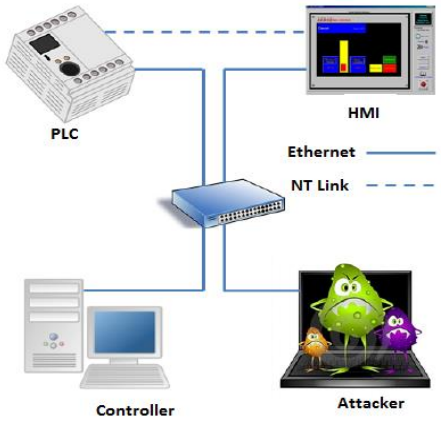

Fig. 3. Simple SCADA system

A. Classifier Types

The aim of our paper is to provide an improvement for security framework of SCADA systems against DDoS attacks using Machine Learning techniques. To achieve such goal, we used the following techniques: Decision tree, Random Forest algorithm (RF), and Naive Bayes method (NB). The dataset used for evaluating the performance of such techniques is the KDD'Cup99 dataset which has been preprocessed to tune the available attack classes keeping only six attack types related to DDoS attacks.

A decision tree is a decision supported tool, commonly used in research especially in decision analysis, and it can be used as either a descriptive means for countering the conditional probabilities or for solving multi-class classification problems. The main idea of a decision tree is to divide the dataset into minimal datasets based on the given features until reaching a small set that consists of points of data falling under one label. One of advantages of Decision Trees is that it is easy to be interpreted and it requires a little preparing of the data from the user (No need to normalizing data). Decision Tree based learning algorithms generate decision trees from the training data for solving classification and regression problems.

Random forest (or random forests) is a technique of ensemble and supervised learning that consists of various decision trees. It can be used for both classification and regression problems. It produces various decision trees and then it merges the obtained decision trees together to get an accurate decision or prediction. In such learning model, decision trees considered as individual learners involving greedy and recursive partitioning [27] [28].

The Advantages of random forest are: 1) It is a high-resolution algorithm. 2) It works with large databases efficiently. 3) It can handle a large number of input variables. 4) It can grant estimating the critical variable in the classification. 5) When data is lost, it works to maintain accuracy and to estimate the lost data in an effective manner. 6) It can balance the dataset and can calculate prototypes that provide information on the relationship between variables and classifications. 7) It can be used to detect changing interactions. One of the disadvantages of random forest technique is that it is not reliable with random data which contains variables with different levels of quantity [28].

Naive Bayes method (NB) is a probabilistic classifier technique adopted from Bayes theorem and particularly is suitable when having a high dimensionality of the input data [29].

B. Dataset Description

We applied J48, NB, and RF algorithms for detecting DDoS attacks on KDDcup dataset which is available online and commonly used for intrusion detection systems [30]. The procedure we followed to evaluate these models is as follows. First, we collected the data from KDDCup'99 dataset. Then, we selected a portion of training dataset from KDDCup'99 for the experimentation. In fact, the dataset contained records for several types of attacks listed in Table 1, but due to the aim of our research, we kept only the DDoS attack classes and dropped others from the dataset. The original dataset contains 493732 instances and after applying the prepressing step it holds only 488807 instances. Table 2 shows the features used to train the three learning models used in this study. Finally, we trained the models using the refined dataset by Waikato Environment for Knowledge Analysis (Weka).

Table 1. Attack classes and its types [25]

Attack Class	Attack Type
DoS	Back, Smurf, Neptune, teardrop, Pod, Land.
Probe	Satan, Ipsweep, Portsweep, Nmap.
R2L	Warezclient, Warezmaster, Guess_passwd, Imap, Ftp_write, Multihop, Phf, Spy.
U2R	Buffer_overflow, Rootkit, Loadmodule, Perl.

Table 2. Dataset Collection

Variable No	Features
1	Duration
2	Protocol_type
3	Service
4	Flag
5	Src_bytes
6	Dst_bytes
7	Land
8	Wrong_fragment
9	Logged_in
10	Count
11	Srv_Count
12	Dst_Host_Count
13	Dst_Host_Srv_Count
14	Dst_Host_Same_Source_Port_Rate
15	Attack

IV. Results and Discusion

The results of our work show that RF classifier is the best algorithm for detecting DDoS attacks compared to the other two models (J48 and NB). In addition, the three algorithms

were compared and evaluated in terms of the accuracy and errors related to the classification as shown in Table 3. Fig. 4 and Fig. 5 show the corresponding confusion matrix and margin curve of the classification done by J48 classifier, respectively. Similarly, Fig. 6 and Fig. 7 demonstrate the corresponding confusion matrix and margin curve for NB; Fig. 8 and Fig. 9 show the corresponding confusion matrix and margin curve for RF, respectively. All of these figures are consistent with the numerical values presented in Table 3.

Comparing our paper with the evaluation study in [31], they evaluated only RF and J48 for securing wireless nodes inside the network, mainly by detecting different kinds of attacks including the DDoS attacks. They used the same dataset we used in our study which is KDDCup'99. Based on their results, the J48 algorithm showed the most preferable accuracy and thus being considered as the best classifier for detecting DDoS attacks. However, in our paper we focused only on the DDoS attacks and based on our results the best performance is of RF but not of J48. Actually, the preprocessing step implemented in our paper enhanced the accuracy of the classification and ranked RF as the best classifier for DDoS attacks. In addition, our framework included the evaluation of a non-decision tree model which is NB. The overall results of our paper show that for detecting DDoS attacks, RF takes place the first rank followed by J48 which is in the second rank and finally NB has the lowest accuracy compared to the FR and J48.

Table 3. Comparison between J48, NB and RF algorithms

Classifier	J48	NB	RF
Correctly Classified Instances	488786	477793	488806
Incorrectly Classified Instances	21	11014	1
Correctly Classified Instances accuracy (%)	99.9957%	97.7468%	99.9998%
Incorrectly Classified Instances accuracy (%)	0.0043%	2.2532%	0.0002%
Kappa statistic	0.9999	0.9616	1
Absolute error	0	0.0054	0
Squared error	0.0032	0.0676	0.0012
Relative absolute error	0.014%	3.7154%	0.0076%
Root relative squared error	1.1831%	25.0489%	0.4498%
Total Number of Instances	488807	488807	488807

=== Confusion Matrix ===

a	b	c	d	e	f	g	h	<-- classified as
97264	9	1	2	0	1	1	0	a = normal.
3	107198	0	0	0	0	0	0	b = neptune.
0	0	280790	0	0	0	0	0	c = smurf.
0	0	0	264	0	0	0	0	d = pod.
0	0	0	0	979	0	0	0	e = teardrop.
0	3	0	0	0	18	0	0	f = land.
0	0	0	0	0	0	2203	0	g = back.
1	0	0	0	0	0	0	70	h = warezclient.

Fig. 4. Confusion matrix for J48 Decision tree

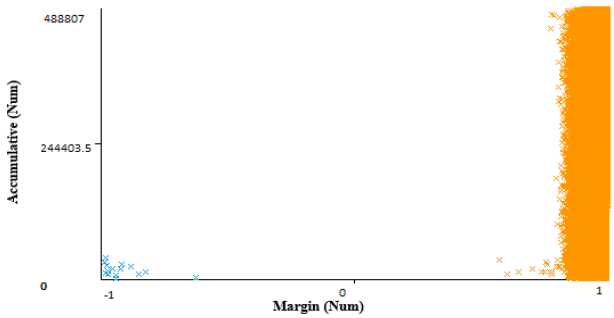

Fig. 5. Visualizes margin curve for J48 algorithm

=== Confusion Matrix ===

a	b	c	d	e	f	g	h	<-- classified as
86713	21	72	4	244	47	0	10177	a = normal.
22	107117	0	0	45	16	0	1	b = neptune.
170	0	280475	143	2	0	0	0	c = smurf.
0	0	0	259	0	0	0	5	d = pod.
0	0	0	0	979	0	0	0	e = teardrop.
0	2	0	0	0	19	0	0	f = land.
43	0	0	0	0	0	2160	0	g = back.
0	0	0	0	0	0	0	71	h = warezclient.

Fig. 6. Confusion matrix for NB

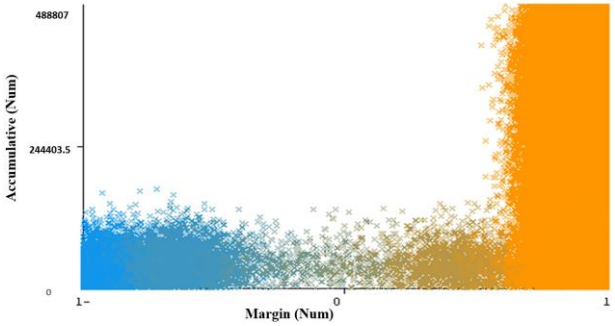

Fig 7. Visualizes margin curve for NB

=== Confusion Matrix ===

a	b	c	d	e	f	g	h	<-- classified as
97277	0	0	1	0	0	0	0	a = normal.
0	107201	0	0	0	0	0	0	b = neptune.
0	0	280790	0	0	0	0	0	c = smurf.
0	0	0	264	0	0	0	0	d = pod.
0	0	0	0	979	0	0	0	e = teardrop.
0	0	0	0	0	21	0	0	f = land.
0	0	0	0	0	0	2203	0	g = back.
0	0	0	0	0	0	0	71	h = warezclient.

Fig. 8. Confusion matrix for RF

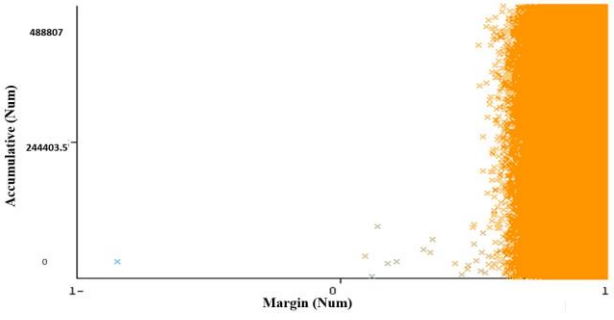

Fig. 9. Visualizes margin curve for RF

V.ⁿ CONCLUSION

In order to improve the security framework of SCADA system against DDoS attacks, in this paper we used three machine learning algorithms (i)J48; (ii) Naive Bayes; (iii) Random Forest classifiers to detect the DDoS attacks based on the training done on KDDCup'99 dataset. Random Forest classifier produces the best performance with an accuracy of 99.9998%, while J48 and NB get accuracies of 99.9957% and 97.74%, respectively. As a future work, we do suggest doing an evaluation on these algorithms using different datasets including a dataset that fits with SCADA systems. In addition, other models of machine learning can be evaluated based on different configuration parameters and datasets.

REFERENCES

[1]ⁿ A. Daneels and W. Salter, "What is SCADA?," 1999.

[2]ⁿ S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," Comput. Secur., vol. 70, pp. 436–454, 2017.

[3]ⁿ X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges," in Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, 2015, pp. 61–68.

[4]ⁿ M. Hentea, "Improving security for SCADA control systems," Interdiscip. J. Information, Knowledge, Manag., vol. 3, no. 1, pp. 73–86, 2008.

[5]ⁿ N. Sayegh, A. Chehab, I. H. Elhajj, and A. Kayssi, "Internal security attacks on SCADA systems," in Communications and Information Technology (ICCIT), 2013 Third International Conference on, 2013, pp. 22–27.

[6]ⁿ E. Byres and J. Lowe, "The myths and facts behind cyber security risks for industrial control systems," in Proceedings of the VDE Kongress, 2004, vol. 116, pp. 213–218.

[7]ⁿ Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," Comput. Secur., vol. 56, pp. 1–27, 2016.

[8]ⁿ W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," Int. J. Crit. Infrastruct. Prot., vol. 9, pp. 52–80, 2015.

[9]ⁿ J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in International Conference on Critical Infrastructure Protection, 2007, pp. 73–82.

[10]ⁿ R. J. Turk and others, Cyber incidents involving control systems. Citeseer, 2005.

[11]ⁿ M. A. Teixeira, T. Salman, M. Zolanvari, R. Jain, N. Meskin, and M. Samaka, "SCADA system testbed for cybersecurity research using machine learning approach," Futur. Internet, vol. 10, no. 8, 2018.

[12]ⁿ Y. Cui, P. Bangalore, and L. B. Tjernberg, "An Anomaly Detection Approach Based on Machine Learning and SCADA Data for Condition Monitoring of Wind Turbines", 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Boise, ID, USA, 2018.

[13]ⁿ L. Zhoua, Ch. Sua, Zh. Lib, Zh. Liuc, and G. P. Hancked "Automatic fine-grained access control in SCADA by machine learning", Jurnal of Future generation computer systems, In Press, Available online 23 July 2018.

[14]ⁿ A. Almalawi, X Yu, Z Tari, A. Fahad, "An unsupervised anomaly based detection approach for integrity attacks on SCADA systems", Computers & Security, vol. 46, pp. 94–110, 2014.

[15]ⁿ S. Panguluri, W. Phillips, and J. Cusimano, "Protecting water and wastewater infrastructure from cyber attacks," Front. Earth Sci., vol. 5, no. 4, pp. 406–413, 2011.

[16]ⁿ M. Abrams and J. Weiss, "Malicious control system cyber security attack case study--Maroochy Water Services, Australia," McLean, VA MITRE Corp., 2008.

[17]ⁿ R. Ozdemir, "A SCADA System in a Construction Chemicals Manufacturing Plant," vol. 2, no. 1, pp. 16–23, 2016.

[18]ⁿ R. J. Gordon, "DDoS Attack Simulation to Validate the Effectiveness of Common and Emerging Threats," J. Inf. Warf., vol. 16, no. 1, pp. 49–63, 2017.

[19]ⁿ S. Toklu and M. Şimşek, "Two-Layer Approach for Mixed High-Rate and Low-Rate Distributed Denial of Service (DDoS) Attack Detection and Filtering," Arab. J. Sci. Eng., 2018.

[20]ⁿ C. Li et al., "Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN," Int. J. Commun. Syst., vol. 31, no. 5, pp. 1–15, 2018.

[21]ⁿ M. S. H. L. Author, G. A. I. E, J. I. Vélez, and L. C. O, "Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype," in Distributed Computing and Artificial Intelligence, 13th International Conference, vol. 474, pp. 33–41.

[22]ⁿ P. Kamboj, M. C. Trivedi, V. K. Yadav, and V. K. Singh, "Detection techniques of DDoS attacks: A survey," 2017 4th IEEE Uttar Pradesh Sect. Int. Conf. Electr. Comput. Electron. UPCON 2017, vol. 2018–Janua, pp. 675–679, 2018.

[23]ⁿ J. D. Markovic-Petrovic and M. D. Stojanovic, "Analysis of SCADA system vulnerabilities to DDoS attacks," in Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2013 11th International Conference on, vol. 2, pp. 591–594, 2013.

[24]ⁿ "(OPNET) Optimized Network Engineering Tools: Simulate your network topologies easier: Information Technology Education Academy: 9781981214112: Amazon.com: Books." [Online]. Available: https://www.amazon.com/OPNET-Optimized-Network-Engineering-Tools/dp/1981214119. [Accessed: 11-Dec-2018].

[25]ⁿ K. A. K. M. S. Dhananjay Bhor, "Network and power-grid co-simulation framework for Smart Grid wide-area monitoring networks," Netw. Comput. Appl., vol. 59, pp. 274–284, 2016.

[26]ⁿ O. Tran, T. Kim, V. Nguyen, and C. S. Hong, "Which network simulation tool is better for simulating Vehicular Ad-hoc network ?," Winter Conf. Proc., pp. 2–4, 2014.

[27]ⁿ B. de Ville, "Decision trees," Wiley Interdiscip. Rev. Comput. Stat., vol. 5, no. 6, pp. 448–455, 2013.

[28]ⁿ L. Breiman, "Random forests," Mach. Learn., vol. 45, no. 1, pp. 5–32, 2001.

[29]ⁿ U. Shardanand, "Social Information Filtering: Algorithms for Automating "Word of Mouth"," Chi'95 Mosaic Creat. , pp. 210–217, 1995.

[30]ⁿ T. Dalgleish et al., "KDD Cup 1999 Data," Journal of Experimental Psychology: General, 2007. [Online]. Available: https:kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. [Accessed: 17-Nov-2018].

[31]ⁿ S. Lakshminarasimman, S. Ruswin, and K. Sundarakantham, "Detecting DDoS attacks using decision tree algorithm," 2017 4th Int. Conf. Signal Process. Commun. Networking, ICSCN 2017, pp. 0–5, 2017.