Date of publication MAR-31, 2024, date of current version JAN-19, 2023.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.23.1.3442

A Hybrid Particle Swarm Optimization and C4.5 for Network Intrusion Detection and Prevention System

K.NANDHA KUMAR[1], D.UDAYA SURIYA RAJKUMAR[2],G.VISWANATH[3], J.MAHALAKSHMI[4]

[1]Associate Professor,Department of Computer Science and Engineering (Data Science), Sri Venkateswara College of Engineering and Technology(Autonomous), Chitoor, Andhra Pradesh, India, e-mail: nandha.k07@gmail.com

[2] Associate Professor, Department of Computer Science and Engineering, GLOBAL Institute of Engineering and Technology, Ranipet District, Tamil Nadu, India, e-mail: u_suriya@yahoo.com

[3] Associate Professor, Department of Computer Science and Engineering, Sri Venkatesa Perumal College of Engineering & Technology, Puttut, Chitoor District, Andhra Pradesh, India, e-mail: viswag111@gmail.com

[4] Associate Professor, Department of Information Technology, MLR Institute of Technology, Hyderabad, Telangana, India, e-mail: mahalakshmi1203@gmail.com

Corresponding authors: K.Nandha Kumar, D.Udaya Suriya Rajkumar (e-mail: nandha.k07@gmail.com, u_suriya@yahoo.com)

ABSTRACT Network Intrusion Detection and Prevention systems (NIDPS) ensure network security and used to effectively detect various attacks and completely stop them from intruding over a network. Since, securing sensitive information carried by various organizations is much more significant, developing enhanced security models become inevitable. To meet the growing demand in safeguarding the network from various known and unknown attacks. In this paper, a Hybrid Particle Swarm Optimization and C4.5 (HPSOCM) method is proposed to network based intrusion prevention system to detect unknown attacks and a signature based SNORT method to detect the known attacks in NIDS. In the hybrid method, we use data mining approach to mine the unknown attacks. Hence, we develop an anomalous detection model and train it using the data mining rules. The trained network is capable of detecting various unknown attacks. The conventional signature based SNORT method detects the known attacks by matching the detected threats from the KDD99 dataset. The proposed HPSOCM method is demonstrated using simulation and the performances were evaluated in terms of Accuracy, Specificity, Detection Rate and False Alarm Rate. The proposed method had produced better efficiency compared to various other existing methods.

KEYWORDS Intrusion Detection System; Intrusion Prevention System; Particle Swarm Optimization; Detection Rate.

I. INTRODUCTION

THE emergence of Network Intrusion Detection Prevention Systems established a high level of protection compared to the conventional firewalls and IDS. The level of security that IPS provides will be higher than the security offered by IDS and firewalls. IPS is a novel technology which furnishes enhanced security for networked systems powered with the latest effective features to face threats. The evolution of IPS technology can be treated as the next level of IDS emergence [1]. IPS systems can be implemented both in hardware or software which has the potential to identify known as well as unknown threats and completely stop the attack. IPS can be defined as a device for network security which supervises the activities of a system or a network and detects the anomalous behavior and starts interacting to avoid such abnormal activities in a system or a network. In order to defend any IT networks, IPS will be a better choice and can be much more fruitful than IDS or firewalls. IPS safeguards the system or a network from DoS (Denial of Service) attacks and also identifies the weaker sections in software and protects them. The popularity of IPS let many leading organizations to employ them and even individuals also started utilizing IPS to protect their systems/network [2].

IPS integrates the functionalities found in firewalls and IDS and performs higher level of monitoring to prevent all possible threats. Since IPS includes the functions of IDS, they can be called as Intrusion Detection and Prevention Systems (IDPS). These IDPS are passive systems which monitor network congestions and threat blocking reports thus evaluating them and delivering actions automatically over the

flow of traffic which are entering into the network. Such automated actions are issuing alarm notifications to the admin, descending the anomalous packets, stopping congestions from the source address and establishing connection reset [3, 4].

II. LITERATURE REVIEW

In [5], various recent intrusion detection systems were summarized as per their categorization and various algorithms utilized to identify malicious activities. Authors strived to juxtapose several intrusion methods. Several techniques and the role of intrusion detection system in network security were studied. In [6, 7], a review of different security attacks categorization methods belonging to TCP/IP protocol stack was presented. The author concentrated on earlier IDS methods employed for detecting intrusions and the advantages of Network IDS and IPS tools both open source and commercial. These IDPS tools and methods which are used to identify and stop the security threats were compared and their performance characteristics were evaluated to effectively identify the network attacks. In [8, 9], an intrusion detection system and an automatically responding system were considered. An automatically responding system was studied along with IDS because conventional IDS seemingly does not respond properly to several attacks on time when it comes to real-world practice. Hence, an automatic response system is necessary to respond as per the type of the network threat. The authors devised various IDS systems and Intrusion Response systems (IRSs) and put forward techniques to effectively handle various types of network attacks using recent technologies.

In [10, 11], an in-depth evaluation of Intrusion Prevention Systems (IPS) which is an extension of IDS systems was performed. The authors utilized an IPS system to completely detect, prevent and stop threats which could easily pass via conventional firewall devices and IDS systems which detect only known attacks. They summarized various IPS evasion methods that could effectively and smartly stop various attacks. In [12], adaptive IDPs (Intrusion Detection and Prevention Systems) for IoT systems (IDP-IoT) were discussed to improve the security of network based and host based functions by analyzing the prevailing IDS methodologies. The presented IDP-IoT model gets the data packet and traces the behavior of the packet. If it is found suspicious, the model stops or drops the packet completely. The presented model is found to be effective in securing IoT ecosystem. In [13, 14], intrusion detection system utilizing Snort rules was presented. The devised system scans every packet that passes through the network. Once a suspicious activity is detected, an alarm notification is instantly raised. Security rules were deployed in IDS by Snort for each packet passing through the network. Snort captures any information of the arriving packet that passes through the network and issues an alert once the packet is matched with the signature allotted by the organization. In this study, signature based network attacks were detected.

In [15, 16], an improved IDS system with the application of Snort rules to detect the network probe attacks was proposed. The authors devised a novel method to enhance the rules of snort IDS to effectively detect the network probe attacks. Hence, they employed a dataset from MIT DAPRA 1999 that contains both normal and abnormal traffic to experiment the performance of the proposed system. Initially, they considered snort rules from earlier methods, improvised and deployed those rules. Further, they used Wireshark tool to evaluate the data packets to detect attacks by comparing them with the considered dataset. Then, the improved Snort rules were used to effectively detect the network probe attacks. In [17, 18], the performance assessment of the proposed intrusion detection and prevention system (IDPs) in real-time were carried out by employing Snort. This study determined network congestion captures; the reports and performance characteristics produced by Snort were evaluated as well as the corresponding signature alert ratio for a specific attack.

In [19, 20], a swarm intelligence technique was presented in the context of agent-based models to identify eavesdroppers. Artificial bee colony attack detection can determine the difference between the eavesdropper and the node IDs described in the ruleset. Collectively, the nodes that produce a warning about the characteristic of an intruder are constructed. A voting procedure is developed in order to identify the intrusion. Artificial bee colony Boolean signing the expect list to consent on the intruder are sent to the groupings through Boolean sign generation. In [21], recently presented research on Intrusion Detection Systems (IDS) in WSNs was analyzed, and categorization of various IDS approaches based on the used detection methods was given. This study focuses on three major categories: Protocols for anomaly detection, protocols for abuse detection, and protocols for specification based detection. We describe the security attacks that have already occurred in WSNs and the related suggested IDS techniques to stop them. We evaluate the works in light of the WSNs network architecture.

An analysis of IDS research initiatives for IoT was shown in [22]. Our goal is to recognize emerging trends, unresolved problems and promising areas for future study. According to the following characteristics detection techniques of IDSs deployment strategy, security threat and validation approach we categorized the IDS suggested in the literature. The many options for each characteristic were also discussed with details of works that either suggest particular IDS schemes for IoT or create attack detection methodologies for IoT threats that might be included in IDSs. The main theme of energy efficient intrusion detection in WSNs was covered in [23]. The survey study covers subjects like the fundamentals of intrusion detection methods and the numerous energy saving approaches employed in diverse building models. The early successes in WSN intrusion detection that used less energy are also outlined and current issues are mentioned. By emphasizing open research topics, we also provide a glimpse in to the potential pathways for future work in intrusion detection.

A technique for wireless sensor networks intrusion detection was presented in [24, 25]. Our intrusion detection method creates a model of a typical traffic behavior using a clustering technique then analyzes that model to find abnormal traffic patterns. Our method's ability to identify previously unseen attacks is a significant benefit. Additionally, the foundation of our detection method is a collection of traffic characteristics that may be used to counter a variety of routing attacks. We have modified a sensor network simulator to mimic routing attacks in wireless sensor networks so that our intrusion detection system may be evaluated.

III. PROPOSED METHODOLOGY

We propose a Hybrid Particle Swarm Optimization and C4.5 (HPSOCM) method. Applying this HPSOCM method, the traffic congestions in the complete network can be analyzed by evaluating the activities of the protocol in order to decide necessary actions. We also analyze the network behavior by monitoring the traffic congestion to detect attacks which produce abnormal flow of traffic, namely malware, DDoS attacks and violation of policies. In the presented hybrid approach, several detection techniques such as traffic anomalies, protocol anomalies and signature based detection methods are combined together to detect attacks and stop traffic congestions arriving from an inline router device. NIDPS systems are usually appliance based which appear in-line and stops abnormal traffic congestions once identifying a threat. These systems employ various detection techniques aforementioned such as detection of anomalies, signature based detection and few other conventional detection methods to completely stop some particular attacks. In this hybrid approach, the below mentioned methods are integrated to efficiently detect and block an attack [18, 19].

Protocol based detection of anomalies: In this technique, the packet data from a network will undergo complete analysis of data packets with the protocol decoding mechanisms to make sure that the packets match the specifications of the protocol. Here, normalization of traffic is established to separate the protocol uncertainties and assure that congestions have been defined by the presented HPSOCM model. We present a hybrid data mining approach along with SNORT to effectively detect various types of attacks. Hybrid data mining approach will help detect unknown attacks where the SNORT approach will detect known attacks. Hence, to construct anomaly based detection, we have combined Particle Swarm Optimization Technique and C4.5, proposed as HPSOCM method, which helps in detecting both known and unknown attacks.

Signature Based Detection: In this technique, the NIDPS model monitors all the information of the state of an activity in which the system participates. It takes care of the applicable areas of traffic congestions from where the attack is executed. This is made possible by tracing the state and on the basis of conditions mentioned by the user to detect a threat. In this context, the user should possess earlier understanding of the threat since the detection is not entirely automated. The proposed HPSOCM model is illustrated below. We adopted Snort methodology along with HPSOCM model for effective prevention of various attacks over a network. Snort is a most prominent method, available open source that can be utilized in intrusion detection and prevention systems. Snort can establish traffic evaluation in real-time. Snort is a light weight, smaller tool which is capable of performing network intrusion detection (NIDS) as well as Network intrusion prevention (NIPS). Snort can perform logging of packets and evaluation of traffic congestion in real-time over internet protocol (IP) networks. The main reason behind adopting this Snort method in our HPSOCM method is that Snort has the capability of supporting both anomaly based methods and signature based methods. Hence, we have introduced a hybrid model using Snort to support these two methods together. Snort can assess protocols and also does content based matching or searching and they are generally utilized to stop or detect various attacks, threats, probes and many more. This method operates on the basis of the available signatures in order to actively identify and stop intrusions. These signatures were commonly available in the packet payload or packet header.

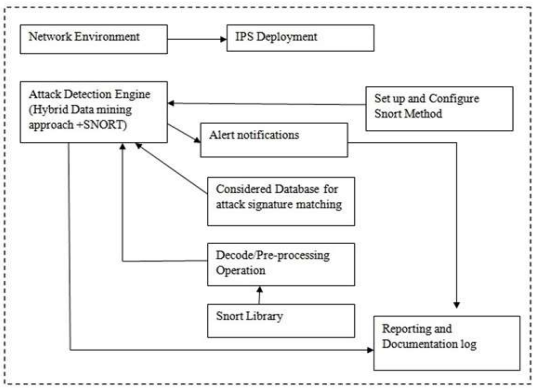

Figure 1. Proposed HPSOCM Method Process implementation

Snort fetches coarse data packets along with the library. It further undergoes decoding operation followed by pre-processing. Then, the pre-processed data is sent to the attack detection engine. In the pre-processing section, it contains categorization, premature dropping of packets, IP layer regrouping of fragments, TCP session rebuilding and many more. The attack detection engine follows the hybrid attack detection mechanism and effectively detects various types of attacks and compares with the stored database, where the defined attack signatures have been already saved. Once an attack has been detected after a match with the database, the HPSOCM method immediately alerts notifications (alarms) and reports in the log file. The Snort based HPSOCM method pro-actively detects various attacks and completely stops them.

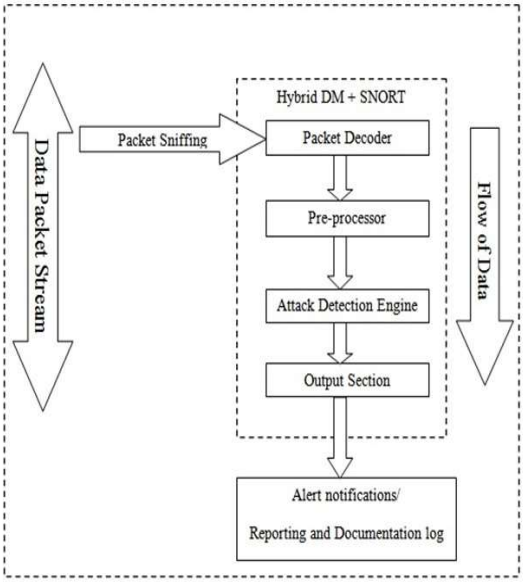

Figure 2. Proposed HPSOCM method with SNORT

The proposed method contains the following four stages, namely: Packet decoder, pre-processor, attack detection mechanism engine and the output section that carries alert notifications and reports log whenever an attack is detected. The data packet stream that flows over a network has been

sniffed before it is decoded. The decoded data is pre-processed and further it is taken to the attack detection mechanism where the attack is compared with the pre-defined database for matching. In this hybrid NHIPS model, we have adopted anomaly detection method to detect unknown attacks. In case of anomaly detection method, it detects threats on the basis of notable changes from the normal activities.

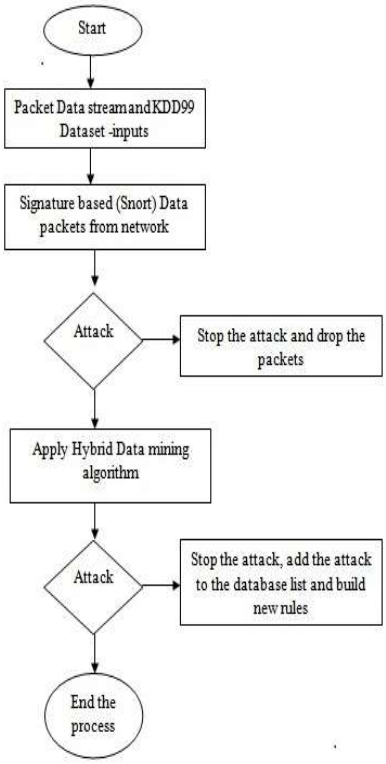

Figure 3. Process Flow diagram of the proposed HPSOCM method

Anomaly detection method has the ability to detect unknown threats as well. Anomaly detection method has the advantage of higher false alarm rate. Signature based detection along with Snort is used to detect known attacks. Hence, we combined these two methods to get the advantage of detecting both known and unknown attacks using a hybrid approach. The HPSOCM method is aimed to prevent various types of attacks posed threat to the network security. Though there are various prevention techniques available in IPS such as signature technique, state protocol technique and profile technique. We made use of the conventional signature technique in this HPSOCM model to detect both known and unknown attacks. In this signature technique, the HPSOCM model scans every data packet byte by byte with the real-time dataset of pre-defined attack patterns. To detect and stop unknown attacks, anomaly detection method is used to detect unknown attacks through hybrid data mining approach.

We considered KDD99 dataset in this HPSOCM method. In this hybrid technique, we combined the PSO and C4.5 algorithm together to detect the global and local optimal values to get the best solution for n iterations. Hence, to obtain the best solution, the training dataset effective features were taken along with the calculated average value. The entire distinct values of are chosen to identify the distinct values which are part of the same class label for every attribute of a. If distinct values of n are also part of it, then segregate them into m number of intervals where n should not be greater than m. If the distinct values of n belong to some other class label, consider examining them to check whether the probability of that value be part of the same class label. If the match is found, then modify the values in the class label to the largest probability class values. Divide the distinct values for each value in the considered dataset. Identify the standard gain for every attribute. The node which is responsible for decision builds the optimal attribute with the largest normalization gain. These nodes are responsible for constructing child nodes. These operations will remain in process till the dataset intersects. Conclusively, train the presented model. The trained model will be responsible to detect unknown attacks in real time.

Table.1. Simulation Parameters

SIMULATION PARAMETERS	
Symbol	Description
D	dataset considered
Atr	Attribute
N	distinct values set
M	number of ordered intervals
$Cl_{1,2,.....n}$	Class labels where Cl_1, Cl_2, Cl_3.....Cl_n are the child nodes and different/same class labels
dec_n	node responsible for decision
O_a	Optimal attribute

Proposed HPSOCM algorithm

OriginalData = KDDDataset
PreprocessingOrginalDataset
Input: TrainingDatasetasKDD99 DatasetM
Step 1: IdentifyingtheoptimalattributesO throughinformationgain and distinct value set n
Step 2: If($n \epsilon cl_1$)then
DivideM
Elseif($n \epsilon Cl2$)
LargestProbabilityϵCl
DivideC1
Step 3: Update
divideM
$M < n$
End
Step 4: $Dec_n = atr + LargestOptimal$ Informationgain
RepeatO_a
$Cl_n = O_a$
Repeattillall$O_{aisidentified}$
Step 5: EndProcess
Output: AttackTypes (DDoS, Probe, R2L, Normal)

IV. EXPERIMENTS AND RESULTS

The proposed HPSOCM method is simulated by installing the proposed model in a networked computer for detecting and preventing various types of attacks. The proposed method has proven to be effective in identifying and stopping various known and unknown attacks in a networked environment while compared to various other existing approaches. The

following table shows different attacks under various categories.

Table 2. Various types of attacks detected and prevented

Attack type	Attack name
DDoS attack (Distributed Denial of Service)	Neptune, Smurf, Pod, Land, Back, teardrop
Probe attack	Ip sweep, port sweep, nmap and satan
R2L attack (Remote to Local)	Imap, phf, warezclient, multihop, ftp_write
Normal attack	Perl, rootkit, load module, buffer_overflow

The proposed HPSOCM method adopts data mining technique to detect and stop both known and unknown attacks. We considered around 5000 random logs of the KDD99 dataset to evaluate the performance characteristics of the proposed HPSOCM method and various other existing approaches. Table 2 shows the number of attacks which are detected and prevented using the proposed HPSOCM method. The presented system is capable of identifying and stopping 20 attacks stated in Table 2. The attacks were compared with the rule structure of the KDD99 dataset. If the attack has already been presented (known attack) in the dataset, it is simply noted and stopped. If any new attack (unknown attack) has been detected, it is also stopped and updated in the rule list of KDD99 dataset. The performance characteristics of the proposed HPSOCM method have been demonstrated and compared with various other existing approaches. The performance parameters considered are accuracy, specificity, sensitivity and false alarm rate. The following tables illustrate the performance parameters of the proposed HPSOCM method and various other existing approaches.

Selection of dataset for these experiments is significant task suitable to the systems performance which is based on the excellence of the data. The effectiveness of the proposed system could be better if an accurate dataset was provided. Numerous difficulties arise when using large amounts of data which are additionally complex and challenging. These difficulties can be overcome using KDD dataset to validate the proposed method for the detection of intrusion. The following KDD Cup99 dataset is provided by:

- Subjective results are not known by the classifier due to its non-redundant data is offered in training set.
- As data is not cyclical, the decrease in ratio could be lesser for the test set.
- The number of selected-records from all level clusters, which is complicated, is comparable to the records percentage of KDD dataset.

Therefore, 41 attributes are enclosed in the dataset that unfolds different flow features and each data is assigned one label that is defined as usual or attack type. The attack types are confidential into four groups and these are DDoS, Probe, R2L, and Normal. The normal KDD99 dataset is used for estimating the proposed system which is given and alienated into four parts and these are DDoS, Probe, R2L, and Normal. Furthermore, here are 65454 samples included in DoS, 32,877 samples in Probe, 18,437 samples in P2L and 9,256 samples in U2R. The evaluation metrics used in these methods are Accuracy, Sensitivity, Detection Rate, and False Alarm Rate. The explanation of these metrics is defined as follows:

Accuracy: It is determined as the prediction of two correct instances from a total amount of data.

$$Accuracy = \frac{TruePositive + TrueNegative}{\left(\begin{matrix} TruePositive + TrueNegative \\ +FalsePositive + FalseNegative \end{matrix}\right)}.$$

Sensitivity: It is calculated as the amount of correctly predicted positive class proportion to the total number of positive predictions.

$$Sensitivity = \frac{TruePositive}{TruePositive + FalsePositive}.$$

Detection Rate: It is defined as the confusion matrix that allows expressing the performance metrics such as the detection rate and False Alarm Rate. It is also called as true positive rate (TPR).

$$Detection\ Rate = \frac{True\ Positive}{TruePositive + False\ Negative}.$$

False Alarm Rate: It is defined as the proportion of benign instances that have triggered a false alarm, while the FDR measures the proportion of the alerts that are irrelevant.

$$Specificity = \frac{False\ Positive}{False\ Positive + True\ Positive}.$$

Table 3. Accuracy Measure for KDD99 Datasets

Attacks Methods	DDoS	Probe	R2L	Normal
SVM	82.32	62.34	82.10	73.50
Naive Bayes	89.03	80.45	85.08	81.92
Random Forest	90.3	87.90	91.86	85.90
HPSOCM	98.5	94.3	98.23	90.11

These results specify that the hybrid method shows better performance when comparing with other existing attacks. Table 2 and Figure 4 show the overall Accuracy for the proposed method and comparison with existing methods.

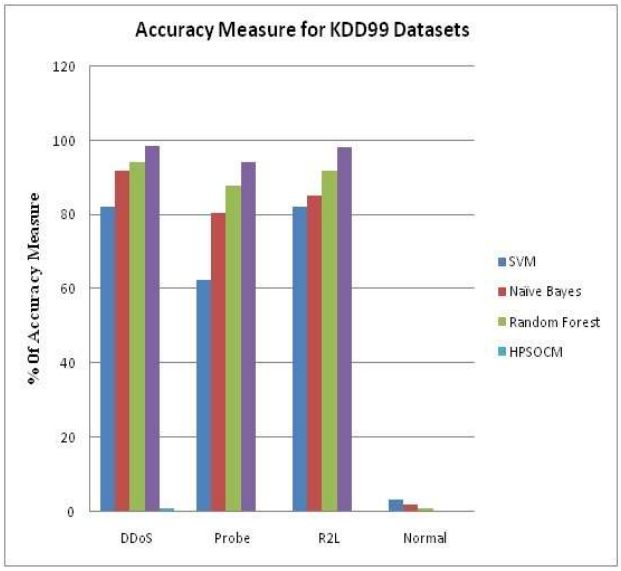

Figure 4. Accuracy Measure for KDD99 Datasets

Table 4. Specificity Measure for KDD99 Datasets

Attacks Methods	DDoS	Probe	R2L	Normal
SVM	72.32	65.35	72.15	73.55
Naive Bayes	79.35	82.45	80.08	80.55
Random Forest	88.35	87.90	86.25	84.35
HPSOCM	**98.50**	**94.85**	**98.23**	**94.10**

Table 4 and Figure 5 show better performance specificity for the proposed method compared to the existing methods.

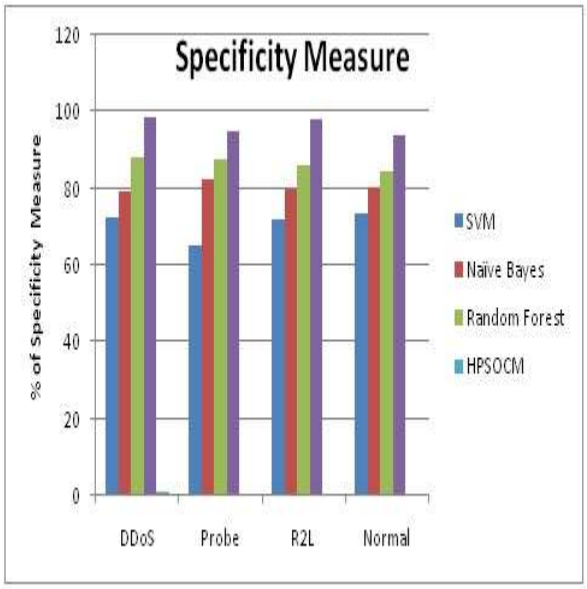

Figure 5. Specificity Measure

Table 5. Detection Rate Measure for NSL-KDD Datasets

Attacks Methods	DDoS	Probe	R2L	Normal
SVM	78.55	75.30	80.45	76.50
Naive Bayes	81.60	84.20	83.50	80.80
Random Forest	87.35	89.75	91.00	86.45
HPSOCM	**97.50**	**94.90**	**98.75**	**96.10**

Table 5 and Figure 6 show better performance Detection Rate for the proposed method in comparison with the existing methods.

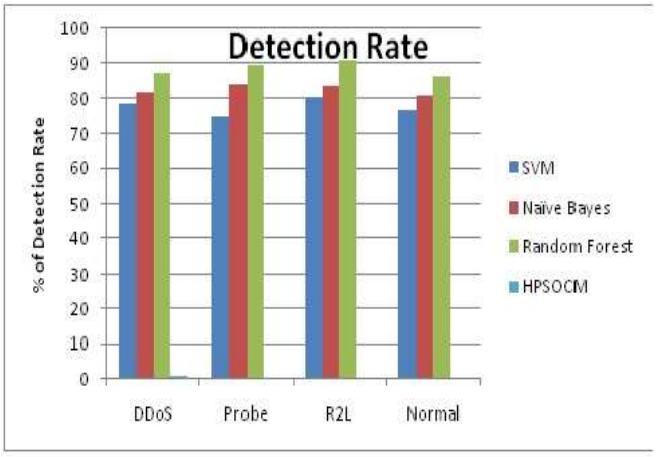

Figure 6. Detection Rate

Table 6. False Alarm Rate Measure for NSL-KDD Datasets

Attacks Methods	DDoS	Probe	R2L	Normal
SVM	4.35	5.10	4.65	4.45
Naive Bayes	3.03	3.50	4.05	3.20
Random Forest	2.75	2.35	2.90	2.55
HPSOCM	**1.50**	**1.60**	**1.20**	**1.10**

Table 6 and Figure 7 show better performance False Alarm Rate for the proposed method in comparison with the existing methods. Each and every attack is performed based on the data samples.

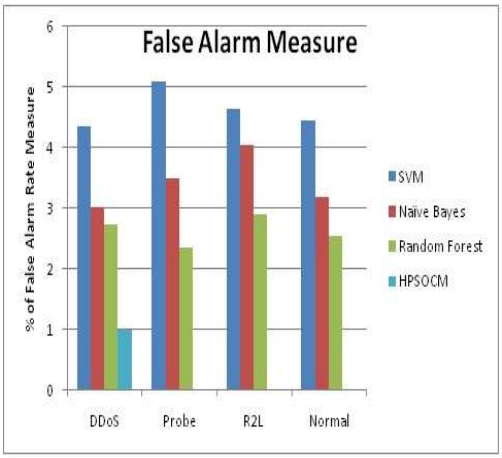

Figure 7. False Alarm Measure

From the above tables, it is evident that our proposed HPSOCM method has achieved better accuracy, specificity, Detection Rate, and lesser False Alarm Rate while compared to various other existing approaches.

V. CONCLUSIONS AND FUTURE WORK

Network security is an integral part of the secure network environment in order to protect valuable information of organizations. Several hackers make use of various new techniques to intrude into the network to edit, delete or modify the sensitive information stored in the network environment. Hence, we present a secure HPSOCM method that employs hybrid approach using data mining technique and signature based SNORT approach to detect both known and unknown attacks. Snort approach is a robust method to detect known attacks. Since signature based Snort approach is not much effective in detecting unknown attacks, we use hybrid data mining approach that constructs anomalous detection module to detect known attacks. The hybrid HPSOCM method has shown less false alarm rate, higher accuracy, sensitivity and sensibility while compared to other existing approaches. The performance parameters of the proposed HPSOCM method and other existing systems are evaluated and tabulated.

References

[1] Y. Uhm and W. Pak, "Real time network intrusion prevention system using incremental future generation," *Computers Materials &Continua*, vol.70, issue 1, pp.1631-1648, 2022.https://doi.org/10.32604/cmc.2022.019667.

[2] A. H. Farooqi and F. A. Khan, "Intrusion detection systems for wireless sensor networks: A survey," *Proceedings of the International Conference on Future Generation and Communication Networking*

FGCN'2019, CCIS, 2019, volume 56, pp. 234-241.https://doi.org/10.1007/978-3-642-10844-0_29.
[3] A. Ghosal and S. Halder, "Intrusion detection in wireless sensor networks: Issues, challenges and approaches," *Wireless Networks and Security*, vol.10 (1007), pp. 329-367, 2013. https://doi.org/10.1007/978-3-642-36169-2_10.
[4] I.Butun,S. D. Morgera and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 16, issue 1, pp. 266–282, 2013.https://doi.org/10.1109/SURV.2013.050113.00191.
[5] Y. Maleh, A. Ezzati, Y.Qasmaoui and M. Mbida, "A global hybrid intrusion detection system for wireless sensor networks,"*Procedia Computer Science*, vol.52, issue 10, pp.1047-1052, 2015.https://doi.org/10.1016/j.procs.2015.05.108.
[6] S. T. Bakhsh, S. Alghamdi, R. A.Alsemmeari and S. R. Hassan, "An adaptive intrusion detection and prevention system for Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 15, issue 11, pp.1-9, 2019.https://doi.org/10.1177/1550147719888109.
[7] B. B.Zarpelão, R. S. Miani and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things,"*Journal of Network and Computer Applications*, vol. 84, issue 10, pp. 25–37, 2017.https://doi.org/10.1016/j.jnca.2017.02.009.
[8] A. Ghosal and S. Halder, "A survey on energy efficient intrusion detection in wireless sensor networks,"*Journal of Ambient Intelligence and Smart Environments*, vol. 9, issue 2, pp. 239–261, 2017.https://doi.org/10.3233/AIS-170426.
[9] X. Xiao and R. Zhang, "Study of immune-based intrusion detection technology in wireless sensor networks,"*Arabian Journal for Science and Engineering*, vol. 42, issue 8, pp. 3159–3174, 2017. https://doi.org/10.1007/s13369-017-2426-1.
[10] W. Guo, Y. Chen, Y. Cai, T. Wang and H. Tian, "Intrusion detection in WSN with an improved NSA based on the DE-CMOP,"*KSII Transactions on Internet and Information Systems*, vol. 11, issue 11, pp. 5574-5591, 2017.https://doi.org/10.3837/tiis.2017.11.022.
[11] G. Creech and J. Hu, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns,"*IEEE Transactions on Computers*, vol.63, issue 4, pp. 807–819, 2014.https://doi.org/10.1109/TC.2013.13.
[12] S. Aljawarneh, M. Aldwairi and M. B.Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *Journal of Computational Science*, vol. 25, issue 10, pp. 152–160, 2018.https://doi.org/10.1016/j.jocs.2017.03.006.
[13] V. Kelli, V. Argyriou, and T.Lagkas, "IDS for industrial applications: A federated learning approach with active personalization,"*Sensors*, vol.21, issue 20, pp. 1-17, 2021.https://doi.org/10.3390/s21206743.
[14] I. Almomani, B. Al-Kasasbeh and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *Journal of Sensors*, Article Id. 4731953, pp.1-15, 2016.https://doi.org/10.1155/2016/4731953.
[15] S.Otoum, B.Kantarci, H. T Mouftah, "On the feasibility of deep learning in sensor network intrusion detection,"*IEEE Networking Letters*, vol.1, issue 2,pp. 68–71, 2019.https://doi.org/10.1109/LNET.2019.2901792.
[16] Md. E. Haque and T. M. Alkharobi, "Adaptive hybrid model for network intrusion detection and comparison among machine learning algorithms," *International Journal of Machine Learning and Computing*, vol. 5, issue 1, pp. 17-23, 2015.https://doi.org/10.7763/IJMLC.2015.V5.476.
[17] R. Zhang and X. Xiao, "Intrusion detection system in wireless sensor networks with an improved NSA based on space division," *Journal of Sensors*, vol.10, no. 1155, pp.1-21, 2019.https://doi.org/10.1155/2019/5451263.
[18] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks,"*IEEE Communications Surveys & Tutorials*, vol. 16, issue 1, pp. 266–282, 2014.https://doi.org/10.1109/SURV.2013.050113.00191.
[19] U. S. R. Dhamodharan et al., "A centralized mechanism for preventing DDOS attack in wireless sensor networks,"*Wireless Personal Communication*, vol.10, no. 1007, pp.1-18,2021.
[20] U. S. R. Dhamodharan et al., "Artificial bee colony method for identifying eavesdropper in terrestrial cellular networks,"*Transaction on Emerging and Telecommunications Technologies*, vol.32, issue 7, pp.1-17, 2019.https://doi.org/10.1002/ett.3941
[21] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks,"*IEEE Communications Surveys & Tutorials*, vol. 15, issue 3, pp. 1223–1237, 2013.
[22] E. Gyamfi and A. Jurcut, "Intrusion detection in Internet of Things: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets," *Sensors*, vol. 22, issue 3744, pp. 01–33, 2022. https://doi.org.10.3390/s22103744.
[23] U. S. R. Dhamodharan, P. Shanmugaraja, K. Arunkumar, R. Sathiyaraj and P. Manivannan, "A HSEERP – Hierarchical secured energy efficient routing protocol for wireless sensor network," *Peer-to-Peer Networking and Applications*, vol. 17, issue 1007, pp. 163-175, 2024. https://doi.org/10.1007/s12083-023-01575-w.
[24] C. E. Loo, M. Y. Ng and M.Palaniswami, "Intrusion detection for routing attacks in sensor networks,"*International Journal of Distributed Sensor Networks*, vol. 2, issue 4, pp.313-332, 2006.https://doi.org/10.1080/15501320600692044.
[25] S. Misra, V. Krishna, and K. I. Abraham, "A simple learning automata-based solution for intrusion detection in wireless sensor networks,"*Wireless Communications and Mobile Computing*, vol. 11, issue 3, pp.426-441,2011.https://doi.org/10.1002/wcm.946.

K. Nandha Kumar received his MCA degree from Dr.MGR University, Tamilnadu, India in 2009 and He obtained his MTech degree in Computer Science from VelTech University, Tamilnadu, India in 2012. He received the Ph.D. Degree in Computer Science from the Bharathiyar University, Tamilnadu, India in 2022. He has 13 years of teaching experience starting from Lecturer to Associate Professor. At present he is working as Associate Professor of Computer Science in Sri Venkateswara College of Engineering and Technology (Autonomous), Andhra Pradesh.

DR. UDAYA SURIYA RAJKUMAR Dhamodharan He received Ph.D. from Department of Computer Science and Engineering from Sathyabama University, Chennai. He has been working as an Associate Professor and Head in the Department of Computer Science and Engineering at Global Institute of Engineering and Technology, Ranipet District, Tamil Nadu. His research interest includes Wireless Sensor Network, Theory of Computation, Data Mining and Machine Learning. He has published Nine papers in International Journal and Four in National Journals. He has attended Ten international and national conferences.

Dr. G. VISWANATH working as Associate Professor in the Department of computer science & engineering Sri Venkatesa Perumal college of Engineering and Technology, Puttur, Andhra Pradesh, India. His research interest Includes Wireless Sensor Network, Theory of Computation, Data Mining and Machine Learning. He has published nine papers in International Journal and four in National Journals. He has attended ten international and national conferences.

Dr. J. MAHALAKSHMI, an Associate Professor in the Department of Information Technology in MLR Institute of Technology, Hyderabad, Telangana. Her research interest includes Wireless Sensor Network, Theory of Computation, Data Mining and Machine Learning. She has Published nine papers in International Journal and four in National Journals. She has attended ten international and national conferences.