DOI: http://dx.doi.org/10.26483/ijarcs.v13i5.6912

Volume 13, No. 5, September-October 2022

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

HYBRID INTRUSION DETECTION METHOD BASED ON IMPROVED ADABOOST AND ENHANCED SVM FOR ANOMALY DETECTION IN WIRELESS SENSOR NETWORKS

Mohammad Sirajuddin
Research Scholar, Department CSE
JNTU, Hyderabad, Telangana, India
ORCID ID: 0000-0003-1180-3813

Dr.B. Sateesh Kumar
Professor, Department of CSE
JNTUH- College of Engineering Jagitial
Telangana, India.

Abstract: The utilisation of Wireless Sensor Networks is quickly rising due to the fast progress of wireless sensor technologies. Due to limited resources, infrastructureless nature, and other factors, it faces major security difficulties. This study describes a hybrid IDS based on an improved AdaBoost and Enhanced SVM strategy for detecting network intrusions and monitoring node activity while classifying it as normal or abnormal. AdaBoost is used in combination with an SVM classifier to identify and classify intrusions. The suggested IDS considerably enhanced the network performance by recognising and eliminating malicious nodes from the network and avoiding DoS and sinkhole attacks. Results oproved that it performes better than other state of art methods in terms of transmission delay, detection rate, energy consumption, packet delivery rate. It also has the advantages of a simple structure and quick computation times.

Keywords: IDS; WSN Security; Improved Adaboost; SVM; Hybrid IDS

I. INTRODUCTION

WSN is made up of a collection of nodes that communicate with one another via wireless connections rather than centralised communication. These infrastructure-free networks are largely employed in tactical warfare and emergency search and rescue operations. Wireless sensor networks incorporate different elements of a wired network; intrusion detection is effective when applied directly to wireless sensor networks. The network is vulnerable to different external assaults due to the open features of the WSN. A node inside the network sends information to other nodes directly via wireless connections. Every node in the network served as both a host and a router. Ad-hoc network features including communication through wireless networks, resource limitations, and changeable topology make it more susceptible to intrusions during transmission. Therefore, current research focuses on identifying and categorizing network intrusions.

A. *Intrusion Detection System*

IDS is responsible for keeping an eye on, evaluating, and identifying suspected occurrences that are against the system's safety policy as unlawful actions by a malicious or authorized entity in a solitary computer network. IDS observes network activity and sends out an alarm when illegal conduct is found[1].

The data collection module is in charge of collecting data from the various WSN nodes. The data pre-processor module uses discrete pre-processors to process the data and transform it into the appropriate form. The reaction module is in charge of setting off the alert if any intrusion is discovered, and the intrusion model is the database of previously known intrusion characteristics[2].

B. *Use of Machine Learning Techniques in WSN Security*

Wireless network security is an important and fundamental parts of QoS. It is defined as the process of creating an activity to protect data from unauthorised users, improve network usability, and assure the integrity of data transported over the network. It is an unmeasurable non-functional QoS parameter[3].

Other security criteria are handled by the SVM approach. The IDS is in charge of monitoring, evaluating, and identifying contradictory occurrences that breach the system's safety policy as illegal behaviour by a malicious or allowed entity. When unlawful behaviour is found, IDS monitors the network, examining information and data to find patterns in encrypted communication that may be used to detect infections. Because of their action, an alarm is sent. Machine learning-based intrusion detection systems (IDS) are used to identify and prevent security breaches in wireless sensor networks[2].

The components typically make up an IDS: data gathering, detection, and response. Each module is constructed in phases, and the data collecting module takes statistical data from The WSN as input to the detection module's data analysis module, then executes the response module based on the detection module's output while considering the needs of the IDS. When nodes send or receive data packets, they use a wireless transmit, receive, transmit buffer, detection module, response module, and routing module[4]. In order to reach the ultimate determination, the output of the The detection module sends IDS to the response module. After reviewing the information, the final answer is created, and the appropriate actions are taken. Before the detection module outputs, the detection module's accuracy and the prospective attack model must be considered in order to make the optimal choicesThe whole method will use the power of the nodes and the computing power of the MCU. Due to the random selection of malicious nodes during the simulation, the malicious node closes the IDS. When the AODV routing module receives the request packet, it ignores the restrictions and sends a large number of response packets.

Since malicious nodes cannot collect data or be used to deploy IDS, when there are DoS attack nodes in the WSN, the target node uses the IDS implementation to determine if the attack took place. and then take the necessary measures to remove the malicious nodes. in WSN to restore network performance back to normal.

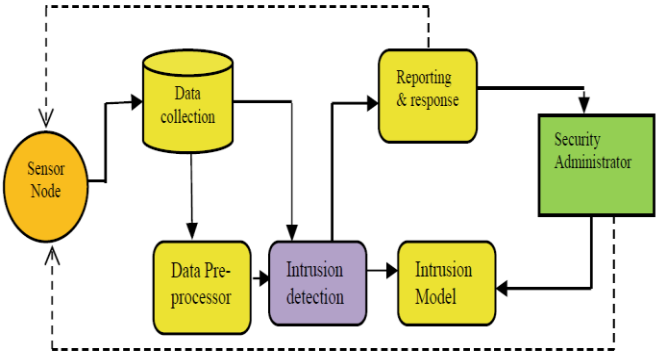

Figure 1. Architecture of IDS

II. Literature Survey

In paper [5], The combinationof SVM classifier with Ada Booster is a powerful anomaly intrusion detection method created for wireless ad hoc networks. The EAB-SVM classifier's major goal is to increase anomalous intrusion detection accuracy while reducing classification time In order to pick the best features for effective intrusion detection, the EAB-SVM classifier first performs optimum feature selection. After that, an intrusion detection model using the chosen ideal features employs an ensemble of AdaBooster with an SVM classifier. The weights of each sample in the hyperplanes are determined by the SVM base classifier. The powerful classifier Ada Booster is derived from weight calculation. Finally, the node is classified as either normal or anomalous using the objective function of the strong classifier. Anomaly intrusion detection accuracy, false positive rate, classification time, and packet delivery ratio are some of the different metrics used in the simulation. The performance results demonstrate that, compared to state-of-the-art approaches, the EAB-SVM strategy improves anomalous intrusion detection accuracy with minimal classification time as well as packet delivery ratio with little false positive rate.

In article [6,] an IDS based on the IABRBFSVM technique is presented, allowing the WSN to defend DoS attacks more successfully. The experiment findings present that including the suggested methodology into the system can enhance overal capability and bring it near to the perfect network. Simulation output proved the presented methodology has a more detection rate for detecting and removing faulty nodes from the system during network attacks..

The paper [7] developed a good traffic anomaly detection mechanism. First, PCA was accustomed scale back knowledge spatiality and scale back the quantity of parameters for additional model coaching. a completely unique DCNN structure is made to suit the model's light-weight and high detection ability wants. The classic convolution layer and depth wise dissociable convolution layer square measure integrated within the creation of DCNN, and also the pooling layer is replaced with associate degree attention methodology for feature extraction whereas avoiding feature loss due by pooling.

In comparison to the current technique, the suggested method [8] increased the sinkhole attack detection ratio by an average of 7%. However, the knowledge-based rules were effectively implemented in the member and leader nodes but significantly less effective in the related nodes when the sinkhole detection ratio for each node of the suggested technique was examined. The guidelines will be expanded upon so that the suggested approach may be used in a variety of settings. Additionally, as was already said, a sinkhole assault is challenging to identify since it is a destructive attack that compromises the accuracy and integrity of data. The proposed technique builds rules based on the knowledge base of the expert system and is based on the specification-based intrusion detection approach, allowing for the identification of just sinkhole attacks.

This study [9] modifies the speed update weight and sigmoid function to provide the particle swarm with several updating options at various phases. The NSL-KDD dataset's feature space was condensed using the improved feature selection method from 41 dimensions to 14 dimensions, and the Adaboost algorithm was used to assess these features. The evaluation's findings demonstrate that, in comparison to previous approaches, our feature selection algorithm delivers more essential characteristics to the Adaboost algorithm, improving its accuracy. This study also suggests an enhanced Adaboost approach that, by employing weight modification techniques, efficiently lessens the impact of noisy samples while training classification models and, to a certain extent, increases sample accuracy overall.

[10] describes a thorough process for preventing infiltration utilizing ML on structured data. The following phases were proposed by this method: input, dataset selection, algorithm application on gathered input, input processing, and final conclusion based on output. The AVISPA tool was used for authenticity verification in this manner. It offers complete risk monitoring and intrusion modelling on anomaly detection and prevention strategies for WSNs through the use of a projected security protocol verification tool. [6]. It keeps track of the encryption pattern and looks for variations that might signal an intrusion.

The technology [11] employs the limited Boltzmann machine learning-based RBC-IDS, a prospective machine learning and deep learning-based intrusion detection methodology utilised for monitoring the crucial components of a wireless sensor network [11]. This technique achieved a 99.91% accuracy rate and a 99.12% detection rate on the examined wireless sensor networks, with the number of concealed layers equal to three intrusive actions [11].

In this paper Hybrid Improved Ada Booster with Enhanced SVM (Hybrid IABESVM) classifier is a powerful anomaly intrusion detection method proposed for wireless sensor networks. The Hybrid IABSVM classifier's major goal is to increase anomalous intrusion detection accuracy while reducing classification time. Anomaly intrusion detection accuracy, packet delivery ratio, classification time, and other metrics are used to evaluate the effectiveness of the proposed approach. Performance results demonstrate that the Hybrid IABESVM methodology outperforms state-of-the-art techniques in terms of anomalous intrusion detection accuracy with the shortest classification time and highest packet delivery ratio.

III. SECURITY ATTACK MODEL BASED ON AODV PROTOCOL

WSNs are made up of many sensor nodes that have high computing, storage, and energy requirements. These sensor nodes can function independently in challenging environments without human involvement. Data collection from the physical world is one of the fundamental aims of WSNs, however, because of its broadcast features, it is open to various network assaults. DoS attacks are the most frequent in WSNs and have a significant impact on QoS factors including transmission latency, energy consumption, packet delivery ratio, throughput, and the restricted capabilities of node resources in WSNs. As a result, security in WSNs has become a major issue. A DoS attack prevents regular nodes from using network resources as they would in the absence of the assault. One of the most popular methods of such assaults is to employ unexpectedly large amounts of data to flood network nodes, using up bandwidth and exhausting the target system's resources. The nodes of the WSNs transmit various sorts of control packets based on the AODV routing protocol to guarantee the topology of the link. A node broadcasts the Hello packet after receiving an RREQ packet, and this process continues until the packet is received by the destination node. A node will transmit RREP packets to the source node when it is aware of the routing path. This procedure creates a routing path for the data transport itself. The QoS characteristics of WSNs are impacted by the RREQ flood DoS attack utilizing the AODV protocol. Malicious nodes that receive such packets produce numerous routing request packets, exhaust the limited resources of wireless sensor nodes, and significantly impede the functioning of the network. Additionally, malevolent nodes continuously emit RREQ signals, preventing neighboring nodes from responding to requests from other nodes.

A. Energy Consumption Model

The most critical matter is how to lower energy usage and extend the lifespan of WSNs due to the restricted resource characteristics. Currently, The consumption of power in WSNs, the REDM model, which assumes that the distance between transmitting and receiving nodes is d and that the default threshold is d0, is widely employed. The amount of energy required to transmit one bit:

$$E_{TX}(k) = E_{elec} \times k + X$$

Energy consumed by receiving 1 bit:

$$E_{RX}(k) = E_{Elec} \times k$$

B. DoS attack model based on AODV Protocol

The control packets of the AODV routing protocol are Hello, R_Req, and R_Rep packets. R_Req packets are used by the AODV routing system to determine the best path to the destination, whereas broadcast HELLO packets tell nodes about neighbouring nodes. Flooding assaults launch DoS attacks using R_Req packets and Hello packets, it can disturb in ways that violate the AODV protocol's retransmission mechanism, preventing ordinary nodes from receiving the R_Req packet scan and forcing middle routing nodes to broadcast R_Req packets constantly, wasting their resources.

IV. PROPOSED MODEL: IDS BASED ON IMPROVED ADABOOST AND E-SVM (HYBRID IABESVM)

AdaBoost is an iterative method that repeatedly updates the sample weight using the lifting concept. The next training will focus more attention to error samples and improve classification effect by raising the weights of past classification error samples. Finally, a strong classifier is paired with a weak classifier that is trained repeatedly.

The kernel function of the SVM is selected to meet the AdaBoost training criteria. The kernel function translates eigenspace to kernel space to create nonlinear separation in eigenspace. In kernel space, SVM finds a hyperplane with the greatest geometric space

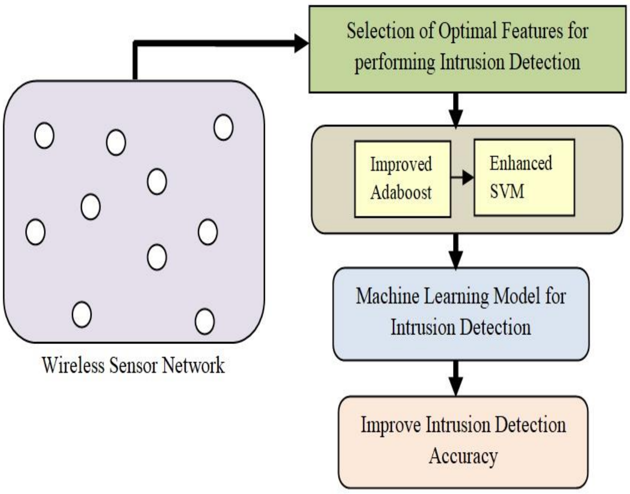
Selection of Optimal Features for performing Intrusion Detection
Improved Adaboost
Enhanced SVM
Machine Learning Model for Intrusion Detection
Improve Intrusion Detection Accuracy
Wireless Sensor Network

Figure. 2 Hybrid IABESVM

Algorithm IABESVM

```
1. **Initialize**: the weights of training data
2. For the Maximum number of iterations in $T$
     Step 1: Train weak classifier by distribution $W1$
     Step 2: Get weak classifiers $ft(\boldsymbol{x})$ of IABESVM
               by the $\sigma$, Calculate training error$e_t$ , and
               Model error $e_m$ of $f_t(\boldsymbol{x})$
     Step 3: If $e_t >$ 0.5, decrease $\sigma$ by its initial value
                  and go to Step 1
     Step 4: Update the weights
3. Output the Hypothesis
```

.

Three components typically make up an IDS: data gathering, detection, and response. Each module is constructed in phases, and the data collecting module takes statistical data from The WSN as input to the detection module's data analysis module, then executes the response module based on the detection module's output while considering the needs of the IDS. When nodes send or receive data packets, they use a wireless transmit, receive, transmit buffer, detection module, response module, and routing module. The whole method will use the power of the nodes and the computing power of the MCU. Due to the random selection of malicious nodes during the simulation, the malicious node closes the IDS. When the AODV routing module receives the request packet, it ignores the restrictions and sends a large number of response packets. Since malicious nodes cannot collect data or be used to deploy IDS, when there are DoS attack nodes in the WSN, the target node uses the IDS implementation to determine if the attack took place. and then take the necessary measures to remove the malicious nodes. in WSN to restore network performance back to normal.

A. *Data Collection Module*

The data collection module plays important roll in receiving the data through the simulation of nodes in the case of unattacked and attacked under various operating factors. behavior of the network, such that attacked nodes can perceive that there is an obvious increase in traffic and other features. The number of packets that are received or sent by the destination node and its neighbors within each unit of time may significantly rise as a result of hostile nodes attacking the target node, exceeding the bandwidth limit and frequently causing packet losses.

B. *Detection Model*

The detection module, which is at the heart of the IDS, significantly affects network performance. The eigenspace discovered above is taken from the trace files produced by the simulation model, and it is tallied. The training set, validation set, and test sets are created by randomly dividing the obtained data set. To train the Improved Adaboost and E-SVM algorithms, create the final classifier, and deploy it as a module to the node, the ratio is 0.6:0.2:0.2.

C. *Response Model*

In order to reach the ultimate determination, the output of the The detection module sends Hybrid IABESVM IDS to the response module. After reviewing the information, the final answer is created, and the appropriate actions are taken. Before the detection module outputs, the detection module's accuracy and the prospective attack model must be considered in order to make the optimal choices. Adjusting the alarm threshold can improve the detection accuracy of the module because the false alarm rate and false alarm rate of the hybrid IABESVM can reduce the detection module's accuracy.

V. RESULT ANALYSIS

A. *Packet Delivery Ration*

Figure 3 depicts the examination of the packet delivery ratio in relation to the number of packets transmitted. The chart makes it quite obvious that as the number of packets increases, the packet delivery ratio increases across all modalities. However, the Hybrid IABESVM classifier algorithm outperforms the current approaches in terms of packet delivery ratio. This is due to the fact that each feature in the dataset has its optimum feature selection assessed.

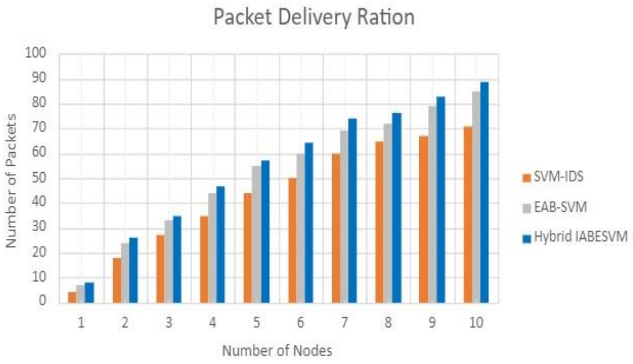

Figure 3. Packet Delivery Ratio Analysis

B. *Classification Time*

The classification time is the length of time needed to categorize the incursion as routine or abnormal. Milliseconds are used to measure the classification time. The graphic makes it quite evident that, for all methods, the classification time increases as the number of nodes increases. The suggested Hybrid IABESVM strategy, however, takes less time than the current approaches to categorize a normal or anomalous node, as shown in the figure. This is due to the employment of an Ada boost ensemble with an SVM classifier for effective classification. AdaBoost trains the SVM classifier to provide a powerful classifier that can categorize the incursion. The weak classifiers are combined into a single strong classifier using the AdaBoost method

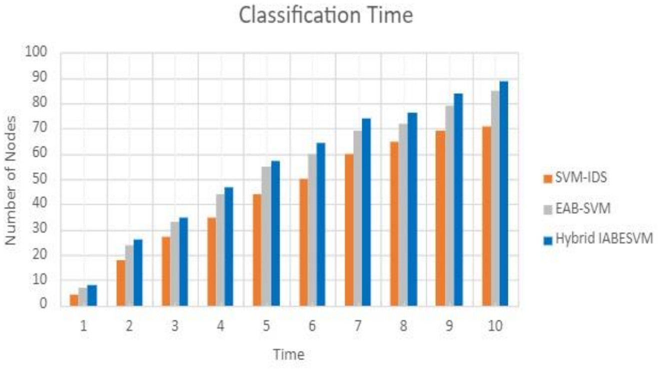

Figure 4. Classification Time Analysis

C. *Intrusion Detection Accuracy*

The accuracy of anomaly intrusion detection is calculated by dividing the number of nodes correctly detected as anomalous by the total number of nodes in the network. The graphic makes it very obvious that the Hybrid IABESVM approach increases the accuracy of anomalous intrusion detection.

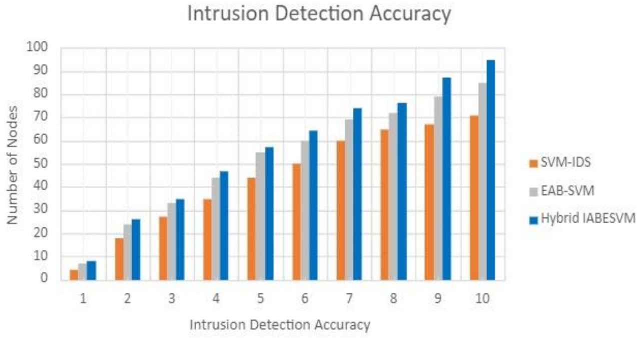

Figure 5. Intrusion Detection Accuracy Analysis

VI. CONCLUSION

In this paper Hybrid Improved Ada Booster with Enhanced SVM (Hybrid IABESVM) classifier is a powerful anomaly intrusion detection method proposed for wireless sensor networks. The Hybrid IABSVM classifier's major goal is to increase anomalous intrusion detection accuracy while reducing classification time. Anomaly intrusion detection accuracy, packet delivery ratio, classification time, and other metrics are used to evaluate the effectiveness of the proposed approach. Performance results demonstrate that the Hybrid IABESVM methodology outperforms state-of-the-art techniques in terms of anomalous intrusion detection accuracy with the shortest classification time and highest packet delivery ratio.

References

[1] N. Tran, H. Chen, J. Bhuyan and J. Ding, "Data Curation and Quality Evaluation for Machine Learning-Based Cyber Intrusion Detection," in IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3211313.

[2] Sirajuddin, M., Sateesh Kumar, B. (2022). Collaborative Security Schemes for Wireless Sensor Networks. In: Kumar, A., Mozar, S. (eds) ICCCE 2021. Lecture Notes in Electrical Engineering, vol 828. Springer, Singapore. https://doi.org/10.1007/978-981-16-7985-8_36

[3] H. Kawaguchi, Y. Nakatani and S. Okada, "IDPS signature classification based on active learning with partial supervision from network security experts," in IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3211651.

[4] M. Sirajuddin and B. S. Kumar, "Efficient and Secured Route Management Scheme Against Security Attacks in Wireless Sensor Networks," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), 2021, pp. 1045-1051, doi: 10.1109/ICESC51422.2021.9532779.

[5] Murugan K, Suresh P. Ensemble of Ada Booster with SVM Classifier for Anomaly Intrusion Detection in Wireless Ad Hoc Network[J]. *Indian Journal of Science and Technology*, 2017, 10(21):1-10.

[6] Dai Jianjian, Tao Yang, Yang Feiyue, A Novel Intrusion Detection System based on IABRBFSVM for Wireless Sensor Networks,
Procedia Computer Science, Volume 131, 2018, Pages 1113-1121, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2018.04.275.

[7] Y. Yang, K. Yin and J. Yang, "Traffic Anomaly Detection in Wireless Sensor Networks Based on Principal Component Analysis and Deep Convolution Neural Network," in IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3210189.

[8] Ga Hyeon An, Ta Ho Cho, Improving Sink hole attack detection rate through knowledge based specification Rule for a sink hole attack Intrusion detection technique for IoT, International Journal of Computer Networks and Applications (IJCNA), Volume 9, Issue 2, March – April (2022), DOI: 10.22247/ijcna/2022/212333.

[9] Quanmin Wang,Xuan Wei, The Detection of Network Intrusion Based on Improved Adaboost Algorithm ICCSP 2020: Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy,https://doi.org/10.1145/3377644.3377660

[10] P. R. Chandre, P. N. Mahalle and G. R. Shinde, "Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification," 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2018, pp. 135-140, doi: 10.1109/GCWCN.2018.8668618.

[11] S. Otoum, B. Kantarci and H. T. Mouftah, "On the Feasibility of Deep Learning in Sensor Network Intrusion Detection," in IEEE Networking Letters, vol. 1, no. 2, pp. 68-71, June 2019, doi: 10.1109/LNET.2019.2901792.

Authors Profile

Mr. Mohammad Sirajuddin, is a Research JNTU Hyderabad, Learning, IoMT Telangana, India. His current research interest includes Machine, and Scholar, CSE, WSNs. He has published more than 15 refereed academic papers/ articles.. He attended conferences and published papers in reputed journals like Springer, IEEE.

Dr. B. SateeshKumar, is a Professor of CSE, JNTUHCEJ, Jagitiyal, Telangana, India. He is the recipient of many national and international awards, including The VishistaSevaPuraskar-2011, BharathJyoti Award, IIFS Delhi, 2011, Best Teacher Award, JBREC, 2006 for Remarkable Contributions, Accomplishments, Distinguished Services, and Impressive Role in Education and Support. He serves as a Governing Body Member to the Boards of studies of various Professional and service-oriented organizations, including the ISTE, which has accepted him as a life member. He attended conferences and, published papers and wrote book chapters in reputed publishers like Springer, IEEE, CRC Press.