MultiCraft

International Journal of Engineering, Science and Technology
Vol. 14, No. 4, 2022, pp. 30-45

INTERNATIONAL JOURNAL OF ENGINEERING, SCIENCE AND TECHNOLOGY

www.ijest1-ng.com
www.ajol.info/index.php/ijest

Computational intelligence paradigms for automata based secured energy efficient routing inwireless sensor network - A technical survey

S. Prithi [1], S. Sumathi [2]*

[1] Department of Computer Science and Engineering, Sri Rajalakshmi Engineering College Chennai, INDIA
[2] Department of Electrical and Electronics Engineering, PSG college of Technology, Coimbatore, INDIA
**Corresponding Author: e-mail: ssi.eee@psgtech.ac.in, Tel. No.: +99947 59330*
ORCID iDs: http:/orcid.org/0000-0001-5165-0212 (Sumathi)

Abstract

Wireless Sensor Network (WSN) has been deployed in several areas of interest for controlling the region, automation of mundane tasks due to features such as smart sensor nodes, low cost, and small-scale factors. Earlier, the sensory units were costly and deficient in the computational and communicational capabilities which were overcome by sensing, processing, storing, and forwarding the data powered by a battery. There predominates diverse applications which affects the low-cost solutions of WSNs in numerous specialties such as observing patients in health care, target exposure, and tracking purposes, examining the atmosphere and climate, home applications, contributing protection for vehicular networks Owing to the diversity of the applications of Wireless Sensor Network, it needs to impose varying design, implementation, and performance requirements on the Wireless Sensor Network to have deep knowledge about the characteristics of WSNs. The pervasiveness of designing and optimizing WSN appeared to be a surplus to several application fields which influenced countless researchers to pay attention to several issues such as routing, mobility of nodes, coverage, and security. In recent years, designing of WSN becomes the leading domain for many researchers. A WSN is bounded with a collection of devices that are associated in the network to communicate the information collected from the field through the wireless links that have been establishedin the network. The data thus collected is transmitted through multiple nodes and also, the data is communicated to other networks through the gateway. During the design and deployment of WSNs, more attention is required at various levels like routing, coverage, and security. A complete system could be designed so that it could resolve the problems such as energy exhaustion, network lifetime, throughput, end-to-end time, routing, and intrusion detection could also monitor and keep control of the network environment. Therefore, this proposed technical research survey work has been carried out by devising an automaton system that can learn, monitor and control the dynamic behaviour of the network environment as well as can obtain an optimal route using Computational Intelligence Techniques. Besides, it detects the malicious activities that occur in the network using Hybrid Intrusion Detection System (IDS) model to enhance the throughput, lifetime of the network, utilization of the energy, end-to-end delay, accuracy, detection rate, computational time and recall rate.

Keywords: Wireless sensor networks, finite state automata, energy efficient routing, classification IDS, hybrid intrusion detection system, computational intelligence, PSO, GWO, support vector machine, random forest, decision tree

DOI: http://dx.doi.org/10.4314/ijest.v14i2.4

Cite this article as:
Prithi S., Sumathi S. 2022. Computational intelligence paradigms for automata based secured energy efficient routing inwireless sensor network - A technical survey. *International Journal of Engineering, Science and Technology*, Vol. 14, No. 2, pp. 30-45. doi: 10.4314/ijest.v14i2.4

Received: August 4 2022; Accepted: August 8, 2022; Final acceptance in revised form: December 8, 2022

1. Introduction

In this section, the various facts that motivated to perform this research survey work are highlighted. Based on the understanding given by (Elshakankiri 2008), the sensor nodes tend to sense, numerate, and communicate data and therefore a large amount of energy has been utilized among the battery-operated sensor nodes. To maintain an energy-efficient network greater attention has to be delivered in designing the networks as well as to sustain the epoch of the network. The key aspect in designing the wireless sensor network which reduces energy and limits the network period is clustering. Therefore, the process of selecting cluster head has to be done very effectively, flexibly and efficiently in comparison with certain existing approaches such as LEACH (Low-Energy Adaptive Clustering Hierarchy), HEED (Hybrid Energy - Efficient Distributed clustering) suggested by Ossama Younis & Sonia Fahmy (2004), Ossama Younis *et al.* (2006), EECS (Energy Efficient Clustering Scheme) stated by Mao Ye *et al.* (2005), Recluster-LEACH proposed by Gao Yi *et al.* (2009), SecLEACH (Secure LEACH) as mentioned by Schaffera *et al.* (2012), Qi Dong & Liu (2009), Leonardo B Oliveira *et al.* (2007), Thandar Thein *et al.* (2008), Shujuan Jin &Keqiu Li (2009), Sasikumar & Sibaram Khara (2012), Akila *et al.* (2017), andYahia *et al.* (2019).

To efficiently design wireless sensor networks, the next foremost factor which has to be considered to reduce the utilization of energy among nodes is the routing process. While transmitting messages across the path the packets might be transferred through the other intermediary nodes. Choosing the most suitable and appropriate path for traffic in a network is known as routing which is one of the most preponderant tasks of the sensor node. The foremost focus of the routing technique is to obtain the optimal route that helps in maintaining the network period to a maximum level as well to efficiently utilize the power. Consequently, Hui Zhou *et al.* (2012), Michael *et al.* (2016) and Abhishek *et al.* (2018) put forth Computational Intelligence Techniques such as Ant Colony Optimization (ACO) algorithm, Genetic Algorithm (GA), Firefly Algorithm and Particle Swarm Optimization (PSO) algorithm to obtain the optimal route. The researchers used these optimization algorithms to find the optimized route in the network for data communication to ensure that the lifetime of the network could be improvised very considerably and the energy is dissipated competently.

Next, according to the ideas obtained from Sohrabi *et al.* (2000), Matt Bishop (2004), and Mohammad Ilyas & Imad Mahgoub (2005), the network's epoch can be estimated by computing the time taken from starting the activity of the network to the time taken till the senor nodes initial energy gets exhausted. As per this thought, there can be an improvement in network performance by determining the dead node ahead of time i.e. identifying the alive node that completely exhausts energy in advance to ensure that the deadnode is restricted from the routing process. In view of this, a motivation occurred to design an automata-based system that tracks the node's energy and in case the remaining energy of a node becomes zero the automaton considers the node as dead and restricts it from taking part in routing. Consequently, with this method, the sensor nodes that exhaust its energy can be easily identified and ignored in the routing process which enables the network lifetime to be extended to a maximum level and the consumption of energy could be minimized in the network.

Owing to the shortcoming of physical protection of wireless sensor networks and also because of its operating behavior, there is a huge possibility for the attacker to destroy, damage, seize, and interrupt the sensor nodes. Consequently, WSNs are susceptible to numerous attacks like wormhole attack, Sybil attack, sink attack, selective forwarding attack, black hole attack, and gray hole attack as mentioned by Karlof (2003), Butun *et al.* (2014), and Fatemeh Barani (2014). These attack nodes interrupt the data transmission and block the node from transmitting data packets to other nodes as well as the attackers evacuates the energy and resources and damages the network environment. To overwhelm the operating chaos of the sensor network, a need occurs to continuously monitor the sensor nodes to identify the affected node and the affected nodes must be restricted from taking part in routing. Misra *et al.* (2009), Amir Hosein *et al.* (2012), Amir Hosein *et al.* (2013) and Amir Hosein *et al.* (2015) proposed an automaton that was used in WSN to control the malicious node. The role of the automaton is to identify the malicious node and not allow them to take part in routing so that the utilization of the energy of these malicious nodes can be minimized as well as the lifetime of the network can beextended to maximum level.

Furthermore, along with automata an IDS model could be designed which helps to identify and detect the threatful activities that happen in the network. Henceforth, Mrutyunjaya Panda (2014), Mohammad Reza Norouzian, Sobhan Merati (2011), Md. Al Mehedi Hasan *et al.* (2013), Jamal Esmaily *et al.* (2015), and Mouhammd Alkasassbeh *et al.* (2016) carried out several investigations using machine learning algorithms such as Decision Trees (DT), Artificial Neural Network (ANN), Random Forest (RF), Bayesian Belief Network, Naive Bayes (NB), Multi-layer Perceptron (MLP), and Support Vector Machine (SVM) to competently detect the intrusions that happen in the network. Jamal Esmaily *et al.* (2015) and Megha Jain Gowadiya (2016) conducted experiments to hybrid the classifiers by exhibiting the uses of the two detection techniques, namely misuse and anomaly detectors. The biggest challenge in designing a hybrid intrusion detection system in the wireless sensor network is to produce an effective and efficient IDS with high overall accuracy, high precision rate/detection rate, and high true positive rate/recall rate.

From the perspective of the above discussions made, the core motives of the proposed research work are emphasized. The foremost motive is to design an automaton-based system with computational intelligence techniques to provide an energy-efficient and effective secured routing in the wireless sensor networks which optimizes the data transmission process and obtains the optimized route. The next predominant motive is to integrate the automata with a hybrid intrusion detection system that dynamically keeps track and learns the network activities to detect the attacks and malicious activities thereby blocking the attacked nodes in taking part in routing. Thus, this research work is done focusing to solve the issues such as routing and security in WSN by minimizing the energy utilization, improving epoch of the network, detecting the attacks with high precision rate/detection rate and overall accuracy, delivering packets with high throughput and less end-to-enddelay.

The rest of the paper is organized as follows. Section 2 presents the background literature study related work. Section 3 describes the Objectives and Scope. Section 4 elaborates on research outcomes & conclusion and Section 5 deals with future enhancements.

2. Background Literature Study

This section elaborates on the existing literature survey pertaining to the numerous clustering techniques, to the various routing algorithms. The earlier research work on the different automata to detect the intrusions and the optimization techniques to optimize the route to provide energy-efficient routing are detailed in this section. Finally, various classification techniques for hybrid intrusion detection system used in earlier research to classify the attacks are discussed.

2.1 Clustering and Routing Algorithms

The communication protocol feature specified by Wendi Rabiner Heinzelman *et al.* (2000) showed a substantial influence on the overall utilization of energy in the network. As per the outcomes of Wendi Rabiner Heinzelman *et al.* (2000) static clustering, multi-hop routing, direct transmission through conventional based protocols, and transmission of minimum energy was not necessarily optimal for the sensor nodes, and therefore a clustering-based LEACH protocol was proposed by them. This protocol moves the cluster head randomly for broadcasting the energy load amongst the sensor nodes. The outcome of LEACH proves that it can accomplish a reduction of 8 multiples in dissipating the energy in comparisonwith the conventional routing protocols. In addition, the protocol enables to uniformly dispense the energy across the sensor nodes, thus the protocol doubles the system lifetime. The energy among the network distributed is performed effectively in the network by minimizing the dissipation of power and improving the lifetime of the system. Li Han (2010) proposed a cluster-based energy-efficient routing algorithm to investigate and bring out a solution for the hot spot problem that occurs while performing routing between clusters in addition network lifetime is optimized. Further, the authors used Particle Swarm Optimization (PSO) technique to explore the optimum route among the clusters in addition to sustain the epoch of the network. In the proposed approach, the utilization of energy was balanced by applying the local competition mechanism while forming clusters as well as the periodic rotation of the cluster head was done. The result of simulation reveals that the cluster-based energy-efficient routingalgorithm achieves better results than LEACH for the network metrics energy, lifetime of the network, and the procedure's firmness proves the efficiency of the algorithm. Further, Chen Yi-Ping *et al.* (2010) suggested an efficient routing that concentrates on improving the efficiency of energy by balancing the energy moreover sustaining the epoch of the network. In this approach, the formation of the cluster is happened by the approach of local competition and the hot spot problem is solved.

Sheng-Shih Wang & Ze-Ping Chen (2013) devised an algorithm called as Link-aware Clustering Mechanism (LCM) for making the routing path efficient and trustwo rthy. A novel clustering metric has been used by the LCM approach to evaluate the selection of nodes for cluster heads to group the cluster. From the simulation result, it is noticed that LCM performs efficiently in clustering with the help of random selection and shows an improvement in packet delivery ratio, consumption of energy, and delivery latency. Certain amendments were done in the LEACH protocol by the author' s Danish Mahmood et al. (2013) to propose the MODLEACH algorithm. The cluster head was replaced efficiently to sustain the dual transmission power levels. The research outcome proves that the MODLEACH algorithm achieves a better result in terms of data flowrate, epoch of the network, and on forming cluster head. Pratyay Kuila & Prasanta K Jana (2014) proposed two formulations, namely Linear and Non-linear formulations for clustering with low power consumption and routing problems. These two algorithms used the PSO algorithm to provide clustering with efficient energy and routing algorithms. The algorithm was deployed in order to prove a tradeoff between the number of hop count and transmission distance. This approach balances the energy utilization as well as improves the epoch of the network. The experimental result proves that the two formulations outperformed the existing algorithms in regard to the number of inactive sensor nodes, networklifetime as well as total data packets transmitted.

A PSO based clustering and routing algorithm was presented by Md Azharuddin & Prasanta K Jana (2017) for WSNs. The clustering algorithm has been facilitated to efficiently utilize energy among gateways and sensor nodes however the routing algorithm relies on to compensate the energy efficiency and to balance the energy. A particle-encoding method witha multi-objective fitness function was formulated and derived for the proposed clustering and routing algorithm. These algorithms have the ability to tolerate the failure of cluster heads. Various experiments have been performed by the authors and proved that the proposed schemes outperformedepoch of the network , utilization of energy, the count of inactive nodes, residual energy of gateways and count of received data packets in comparisonwith the existing approaches like PSO based clustering proposed by Pratyay Kuila & Prasanta K. Jana (2014), Greedy Load Balanced Clustering Algorithm (GLBCA) presented by Chor Ping Low *et al.* (2008), Least Distance Clustering (LDC) approach suggested by Ataul *et al.* (2008), and Genetic Algorithm based clustering (GA) proposed by Pratyay Kuila *et al.* (2014). However, the authors have noticed that fault tolerance has occurred because of the failure ofthe cluster heads.

Energy-Aware Cluster Based Multi-hop (EACBM) routing algorithm was proposed by Amanjot Singh Toor & Jain (2018) that makes use of the clustering principle and communication pattern based on multi-hop to transfer messages to the base station. When comparing EACBM routing protocol performance with existing algorithms the proposed algorithm has shown betterment with respect to stability among sensor nodes, throughput, the lifetime of network, and statistics of dead nodes for each round for various sizes of the network. It has been observed from the investigational study that the modified LEACH algorithm has been recognized to be better in regard to flow rate, epoch of the network, and formation of cluster head. Therefore, in this literature investigation, the MODLEACH algorithm has been employed to perform clustering among nodes which supports to minimize energy conservation as well as prolongs the network period.

2.2 Optimization Algorithms for Energy Efficient Routing

Enhanced PSO-Based Clustering Energy Optimization (EPSO- CEO) approach was suggested by Vimalarani *et al.* (2016) in which an enhanced PSO algorithm selected the cluster head to minimize the utilizationof the energy in the wireless sensor network. The evaluation of the approach was performed on the various assessment parameters like throughput, the ratio of packet delivery, the period of the network, delay, normalized overhead, remaining energy, and consumption of total energy. The simulation result indicates that the proposed (EPSO-CEO) algorithm shows improvement by minimizing the total power utilization of the nodes and by increasing the network period.

The authors Santar Pal Singh & Subhash Chander Sharma (2017) determined the programming formulation to improvise energy-efficient clustering and proposed PSO algorithm to provide efficient clustering. The proposed algorithm has been experimented and evaluated with various measures such as exhaustion of power, rate of flow, ratio of packet delivery, and number of alive nodes and comparison has been done on existing algorithms. The experimental result indicates that the approach achieves efficient results in comparison with the existing algorithms.

The authors Xiaoqiang Zhao *et al.* (2018) proposed a novel energy-efficient protocol built upon an improved Grey Wolf Optimizer (GWO), which is referred to as Fitness value-based Improved GWO (FIGWO). The fitness value has been considered for improving the searching process of the optimal solution in GWO, which ensures a better distribution of Cluster Head(CH) and a more balanced cluster structure. Based on the Base Station (BS) and CHs distance, sensor nodes transmission distance is recalculated to minimize the utilization of energy. The results of simulation show that the proposed approach can extend the epoch of the network in comparison to other algorithms, namely by 31.5% in comparison to Stable Election Protocol(SEP) suggested by Georgios Smaragdakis *et al.* (2004), and even by 57.8% when compared with LEACH protocol. The result also proves that the proposed protocol performs well over the SEP and LEACH protocols concerning power consumption and throughput of the network.

The Firefly algorithmic rule is implemented by the author Mukhdeep Singh Manshahia (2015) that depends on the firefly attractiveness for improving the energy efficiency in routing. The simulation result of this approach shows an improvement in flow rate and network lifetime. Michael Okwori *et al.* (2016) investigated the effectiveness of Ant Colony Optimization (ACO) and Firefly Algorithm (FA) meta-heuristic algorithms to detect the optimal route in a WSN. The performance of these two algorithms were tested on randomly deployed sensor networks that were placed in a clustered fashion. The results simulated proves that the Firefly algorithm could detect routes with minimum cost when compared with the ACO algorithm in case of short routes while the ACO algorithm performs better forlonger routes.

The authors Al-Aboody *et al.* (2016) used Grey Wolf Optimizer (GWO) to devise clustering and routing algorithm and developed a three-level hybrid approach for wireless sensor network. In Level One, the base station (BS) played a predominant part to elect a cluster head along with a centralized selection. To perform data communication GWO based routing was developed in Level Two and selected the best route towards the base station to save the power. Finally, in Level Three, appertaining to cost function a distributed clustering was designed. The approach has been assessed on various performance measures like network power consumption of the network, period of the network, and the stability period. The simulation results prove that the approach achieves a longer network period, reduced utilization of energy, and longer stability period in comparison with the existing algorithms.

Agnihotri *et al.* (2018) used Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) to develop an energy-efficient routing algorithm. The authors developed four types of routing approaches namely theshortest path approach, GA approach, PSO approach, and Hybrid based PSO- GA approach for both large size as well as small size networks. The outcomesof simulation indicated that the Hybrid based PSO-GA routing approach has increased from 12% to 23% network lifetime in comparison with shortest path approach, 8% to 15% network lifetime when compared with PSO approach and 5% to 13% lifetime in comparison with GA approach for large-sized network. The packet delivery ratio of Hybrid based PSO-GA has increased from 9% to 16% when compared with the shortest path approach, 6% to 11%in comparison with the PSO approach, 5% to 9% when compared with the GA approach.

An energy-efficient routing protocol using a hybrid optimization technique was proposed by Logambigai *et al.* (2018). The author has used hybridized Bacterial Swarm Optimization (BSO) method to optimize the energy in WSN. The hybrid BSO approach combined the Bacterial Foraging Optimization (BFO) and Particle Swarm Optimization (PSO). For each gateway, the optimal next node was identified and the final result was an optimized route. Regarding the gateway's lifetime and distance between the gateway and base station the optimal relay nodes was selected. The experiment result proved that the hybrid BSO method improved the network lifetime by 50 rounds, increased the utilization of energy up to 15%, and the hop count used for routing improved by 2 to 5 than the existing algorithms.

Therefore, in this research work the PSO and Grey Wolf Optimizer (GWO) algorithm has been hybridized to form an hybrid optimization algorithm to obtain an optimal path for transmitting the data packets, to sustain the network lifetime, to increase the flow rate, and to proficiently utilize the energy in the wireless sensor network.

2.3 Classification Techniques for IDS

The main part of the intrusion detection system is accuracy, which helps in improving the rate of precision and to decline the probability of falsedetection. To strengthen the intrusion detection system, machine learning algorithms like Support Vector Machine (SVM), Multi-Layer Perceptron (MLP) have been used frequently in research work. An efficient classification technique should be used to identify and classify the attacks since the intrusion detection system mostly plays a major role in analyzing huge trafficdata. A detailed review of the various classification techniques used for designing the intrusion detection system are discussed in this section.

The authors' Wang Jing-xin, Wang Zhi-ying & Dai Kui (2004) developed and implemented a network intrusion detection model by using artificial neural networks and carried out experiments on it. The experimental result shows that the false alarm rate is reduced by 3% for the renowned assaults and the probability of false detection is almost declined by 13% for unknown intrusions when compared with the existing algorithms as well as comparatively better than the traditional intrusion detection methods.

Mrutyunjaya Panda *et al.* (2014) proposed and used vanous machine learning algorithms to detect the intrusions effectively like Decision Tree J48, Na'.ive Bayes and J48 with AdaBoost (AB), Rotation Forest, Bayesian Belief Network, Hybrid NB with DT, Discriminative multinomial NB, Hybrid J48 with Lazy Locally weighted learning, and Random Forest with NB and J48. These algorithms were assessed using the NSL-KDD intrusion detection dataset. The simulation results were performed and assessments were done on the metrics like probability of false detection, detection rate, and the average rate for misclassification. The results helped the researchers to better understand the domain of network intrusion detection.

The authors Md. Al Mehedi Hasan *et al.* (2013) worked out on the SVM for various kernels using Knowledge Discovery and Data Mining KDDCup' 99 dataset to analyze the assessment of the best kernel. The authors eliminated the redundant records that were available in the KDD' 99 trainingset and KDD ' 99 testing set named KDD99Train+ and KDD99Test+ in order to remove the bias that occurred because of these redundant records. The experimental result shows that the SVM classifier with Radial Basis Function (RBF) kernel achieved better detection rate when compared with Linear and polynomial SVM kernels, as well as the RBF kernel, achieved low false- negative rate in comparison with the polynomial kernel.

The authors Muhammad Shakil Pervez *et al.* (2014) merged the classification and feature selection on the NSL-KDD dataset to develop a newintrusion detection approach by applying SVM. The ultimate intention of the system is to decrease the set of input features of the training dataset by improving the expertise of the intrusion classification. To experiment, the authors have trained the SVM classifier on various input feature subset of thetraining samples of the standard NSL-KDD dataset. The result of simulation signified that the approach achieved 91% classification accuracy for three features, while for 36 features and for all the remaining 41 training features the classifier was able to achieve 99% classification accuracy.

Devaraju Sellappan *et al.* (2014) compared the effectiveness of the intrusion detection system on various neural network classifiers. The proposed system used the Feed Forward Neural Network (FFNN), Probabilistic Neural Network (PNN), Generalized Regression Neural Network (GRNN), and Radial Basis Neural Network (RBNN). The simulation was performed on MATrix LABoratory (MATLAB) software and the various performance metrics were assessed on the KDDCup'99 dataset. The authors have analyzed the performance of the full features with the reduced featured KDDCup'99 dataset. The result of simulation indicated that the performance of the reduced featured dataset has performed better than the full-featured dataset.

Classification techniques such as Random Forest, Support Vector Machine, and Decision Tree has been used in this research work to devise and develop an intrusion detection model to identify and categorize the attacks into various attack classes and the performance of the model is evaluated for the standard KDDCup'99 and the standard NSL-KDD intrusion dataset.

Hybrid Intrusion Detection System

Abduvaliyev *et al.* (2010) designed a Hybrid Intrusion Detection System (eHIDS) by combining the anomaly and misuse detection. The authors reduced computational cost and communication by using cluster- based wireless sensor networks. The effectiveness of the eHIDS model was assessed by conducting simulation and the outcome was compared with related schemes like TEEN (Threshold Sensitive Energy Efficient Sensor Network) and PEGASIS (Power Efficient Gathering in Sensor Information Systems). The experimental results indicated an energy efficient system and achieved a high detection rate.

Kuo-Qin Yan *et al.* (2010) proposed Hybrid Intrusion Detection System (HIDS) to enhance the rate of precision and decline the probability of false detection. The authors used Back Propagation Network (BPN) based decision model to detect and classify the attacks. The outcome of the experiment indicated that the rate of precision, accuracy, and probability of false detection of the proposed model is 99.81%, 99.75%, and 0.57% respectively. When the training samples are not persistent the detection rate of the proposed model was very low hence the authors concluded that the training samples have to be specific in number.

Jamal Esmaily *et al.* (2015) devised a model by combining the Decision Tree (DT) and Multi-Layer Perceptron (MLP) algorithm for detecting attacks. The authors designed an Intrusion Detection System model in accordance with Decision Trees and Artificial Neural Networks which produced a higher precision rate and declined the probability of false detection. A newfangled dataset was created by providing the DT and MLP network classification results based upon the random dataset. Whereas in the next phase the classification in the new dataset was done by MLP network and the results were assessed. They achieved promising outcomes such as a very low false alarm rate and promised reliable results m real-worldapplications.

A two-step method was suggested by Md. Al Mehedi Hasan *et al.* (2016) for selecting features based on Random Forest. This algorithm's effectiveness was evaluated on the KDD'99 intrusion detection dataset but this dataset contained a large volume of redundant records. Henceforth, the authors eliminated the redundant records to derive RRE-KDD dataset, to ensure that the bias occurred because of redundant records will be removed inthe classifiers and feature selection method. The RRE-KDD consisted of the KDD99Train+ and KDD99Test+ dataset to train and test the samples. Through the experimental result, it was noticed that for classification the proposed approach was able to select the relevant and most important features that reduced the time and reduces the count of input features besides improvesthe classification accuracy.

The authors Divyatmika & Manasa Sreekesh (2016) built an intrusion detection system using K-Nearest Neighbors (KNN) classifier. The data packets of Transmission Control Protocol/Internet Protocol (TCP/IP) were categorized as input as the proposed architecture depends on the behavior of the network. The data was preprocessed by the parameter filteringmethod and built a self-supporting model by using hierarchical agglomerative clustering. Additionally, KNN classification categorized the data as an intrusion or normal traffic which reduced cost-overheads. Thus, it provided strong security with an increase in true positive rate and reduction in false positive rate as well as progressively learned to segregate normal data and affected data.

The author Megha Jain Gowadiya (2016) suggested a modified datamining classification technique K-Nearest Neighbor Genetic Algorithm (KNNGA) to solve the processing overhead problem that achieved a higher detection rate. The experimental results of the algorithm indicated that there was a rise of 5% with respect to overall accuracy, the probability of false detection was reduced and there was an improvement in detection rate when compared with existing algorithms. The authors Iftikhar Ahmad *et al.* (2018) performed a comparison on various classifiers such as SVM, random forest, and Extreme Learning Machine (ELM). In comparison with existing classifiers like SVM, RF the technique ELM outperformed the metric overall accuracy, recall rate, and precision rate/detection rate for the full data samples. Besides, the SVM technique outperformed the other algorithms for 1/2 of the data samples and 1/4 of the data samples. Hence the authors concluded that the ELM algorithm can be suggested for classifying the datasetwhich contains a large amount of data.

The authors Kumar Parasuraman and Anbarasa Kumar (2018) investigated and compared various classifiers, precisely, SVM, Multiclass SVM, KNN, and Binary Classification (BC). Multiclass SVM outperforms other approaches such as SVM, KNN, and BC with respect to overall accuracy, precision rate/decision rate, and recall rate on the complete data samples as well as on the I/4th dataset. The authors Yi Yi Aung and Myat Myat Min (2018) combined the K-means algorithm and classification and regression trees (CART) algorithm to obtain a Hybrid model to classify the attacks. The authors evaluated the model for KDD' 99 dataset and were able to perform the classification with good accuracy and improved time complexity. The simulation result indicates that the proposed model performed well on accuracy to classify normal data and attacks, as well as the training time of the proposed model, was adaptable in large intrusion detection dataset.

The authors Sandip Hingane & Umesh Kumar Lilhore (2018) used Improved Random Forest (IRF) with bagging and Average One-Dependence Estimator (AODE) to build a hybrid intrusion detection system. This model resolved the problems of the existing RF approach. The performance measures like overall accuracy, precision rate, and probability of false detection was measured for the HIDS method and comparison was done on the existing approach. The simulation outcomes signified that the proposed HIDS method outperformed the existing approach RF with respect to overall accuracy, rate of detection, and probability of false detection.

Through a thorough background study on the various classifiers, it was clear that the hybrid algorithm obtained better results in regard to accuracy, detection rate, and recall rate. Therefore, in this research work hybridization of the classifier are performed using SVM, RF and DT classifier to detect and classify attacks thereby to enhance the detection rate, accuracy, recall rate, Fl-score and computational time for the standard KDDCup'99 dataset and standard NSL-KDD dataset.

2.4 Automata-based IDS and Routing in WSN

To stabilize the network's lifetime and to reduce the utilization of power in wireless sensor networks, Elham Hajian *et al.* (2010) developed an automaton. The automata obtained the optimized path in accordance with the performance metric node. The authors devised a learning automaton for each sensor node to track the redundant nodes in the sensor nodes by Mostafaei *e*such as energy consumption and the distance among the destination *et al.* (2010). The authors' Yan Sun & Min Sik Kim (2011) proposed an efficient algorithm to implement deep packet inspection using regular expression match in g. By analyzing the performance of Deterministic Finite Automata (DFA), they designed an approach that skipped most of the matching process in the compressed regions of the traffic. The algorithm was evaluated on the most popular and standard open-source intrusion detection system known as Snort rule set. The experimental result of the proposed approach proves that it was able to reduce the state access in a DFA in proportion to the traffic's compression ratio. Matteo Avalle *et al.* (2012) proposed a new algorithm to build mulitstride NFA for inspecting packet with reasonable memory and time.

Pattern Matching algorithms play a central-most component m almost all intrusion detection systems which are usually based on the construction of Deterministic Finite Automata to represent the patterns. The modern intrusion detection system tool deals with hundreds of patterns, therefore a necessity occurs to store huge DFAs which generally does not fit in fast memory. Thus, it stands as a big obstruction on the performance of the power consumption, cost, and throughput. So, the authors Anat Bremler Barr *et al.* (2014) proposed a novel approach to compress DFA to improve throughput and consumption of power. This approach was applied to the various huge classes of automata that are grouped by simple properties. The result proves that the model can achieve a throughput of 10 Gbps with minimum power consumption.

The author Joel W Branch (2003) presented a research work and proposed automata known as Time-dependent Deterministic Finite Automata (TDFA) to detect Denial of Service (DoS) attack and masquerading attack in real-time. The proposed approach recorded and processed sequences of user commands, and for the users' signatures, probabilistic state finite automata were constructed. The signature was used to classify between valid and invalid user sessions. In this work, the author has utilized the interval of time among the event occurrences to detect DoS attack and masquerading attack with improved accuracy in a distributed detection architecture.

The authors' Majid Gholipour & Mohammad Reza Meybodi (2008) proposed a protocol called Learning Automata based Mobicast protocol (LA-Mobicast). The authors used learning automata in an appropriate manner to obtain the outline and position of the forwarding zone in order that a number of wake-up sensor nodes is retained in WSN. An algorithm has been used to obtain the forwarding zone with lesser communication overhead. The simulation result shows that LA-Mobicast protocol has outperformed the existing mobicast routing protocols such as Delivery Zone Constrained (DZC) mobicast routing protocol, Face-Aware Routing (FAR) and Variant-Egg mobicast (VE-Mobicast) with regard to slack time, message conversation, and network period.

The authors Kumar Neeraj *et al.* (2014) proposed a Learning Automata-based Energy Efficient Heterogeneous Selective Clustering (LA- EEHSC) algorithm to obtain energy efficient clustering in WSN. In this model, at each sensor node an automaton is positioned to enable the automaton choose the cluster head and employs the observation of node diversity to elongate the epoch of the network. Hao Sheng *et al.* (2018) recommended a automata-based energy-efficient, stable routing algorithm. They developed an algorithm that focused on the durability of the node and formulated an energy-efficient ratio function to maximize the power consumption.

The emphasis of this proposed research survey work is to present an automaton model to follow up the behavior of the nodes that participate in transferring packets which enables the automaton to identify the dead and attacked nodes and restricts these nodes from taking part in routing. Therefore, these sensor nodes do not utilize energy and data transmission does not occur in these affected nodes. Further, the main emphasis of the automaton is to deliver packets with high throughput, minimize the utilization of the energy and transfer packets with minimum time delay also sustains the network lifetime.

3. Objectives and Scope of the Research

For the past few decades, many investigations were performed on routing algorithms and optimization techniques to competently perform routing, to optimize the route for data transmission as well as to effectively design the intrusion detection system to detect the intruding events, identify malicious node, analyze the packets and classify the attacks in WSN. An automaton system can be used to efficiently utilize the energy by monitoring the network activities to detect the attacks, route the packets to destination without any interruption in the route. Computational intelligence paradigms can also be used with the automaton system to optimize the route for efficient routing. Subsequently, a Hybrid IDS model was designed and integrated with the automaton to carry out secured data transmission in WSN. Therefore, the predominant objective of the research work is to devise an automaton to dynamically keep track of the activities of the network environment, to constantly record the node's energy, detect any intrusions that happen in the node as well as during data packet transmission, and to procure the optimized path for data transmission to ensure that the utilization of energy could be minimized, the epoch of the network could be augmented, throughput could be improved, the end-to-end delay could be reduced with high accuracy and high detection rate. The research work was started keeping these objectives in mind and various model was proposed to satisfy the objectives that are described in this section.

The foremost objective was to suggest a framework with an energy- efficient routing using Learning Dynamic Deterministic Finite Automata (LD^{2}FA) with Particle Swarm Optimization (PSO) Algorithm which monitors the activities of each sensor nodes in WSN dynamically and constantly keeps track of the network environment to explore out the valid paths which exist to transfer data packets across the sensor nodes. PSO algorithm procures an optimal path, as a result, it suggestively saves the energy consumption, extends the epoch of the network, reduces end-to-end-delay, and improves throughput. The sensor nodes must not be exaggerated by the malicious activities and the focus of the network is to improve the consumption of the energy in WSNs. So, detection of two attacks namely Sybil attack and selective forwarding attack was implemented to detect the malicious node affected by these attacks, and the automata restricted these nodes from taking part in routing. Hence, the second intention of this research work is to propose asecure data transmission algorithm using the Hybrid PSO-GWO optimizationalgorithm together with LD^{2}FA that substantially balances the dissipation of energy as well as augments the route among all available paths, extends the network lifetime, improves throughput and reduces end-to-end delay.

The third objective is to propose a new hybrid-based intrusion detection system using SVM, RF, and DT classifiers to detect and classify theattacks in the dataset. The evaluation on the proposed model is carried out on the KDDCup'99 dataset and the NSL-KDD dataset, comprising 41 features, and the analysis has been done on the various performance metrics such as overall accuracy, precision/detection rate, true positive rate/recall rate, FI- score measure and computational time.

The final eminent contribution of this research work was to integrate the automata LD^{2}FA Hybrid PSO-GWO algorithm with a hybrid intrusion detection model to constantly monitor the activities of the network environment and determine the malevolent events and malicious nodes that occur in the wireless sensor network. The integrated model has to procure theoptimal route and the automaton has to investigate the node, route, and packetso as to identify the malicious activities that occur in the network as well as todetect the attacks during data transmission. The evaluation of the integrated model is conducted on the KDDCup'99 dataset and NSL-KDD dataset. The integrated model was suggested to significantly contribute to improve throughput, to minimize the consumption of energy, to reduce end-to-end delay, to enhance network lifetime with nearly cent percent precision rate/detection rate, overall accuracy, true positive rate/recall rate, and computational time. The overall research work has been systematized into four work modules with each module emphasizing the motivation of the research work, implementation of the proposed framework, setup of the experiment, and simulation results besides comparative analysis of the proposed model with the existing algorithms. The overall structure of the proposed research work portrays the proposed framework, approach of the proposed solution, strategies of implementation, verification of the proposed model, and evaluation of performance measures are represented in Figure 1.

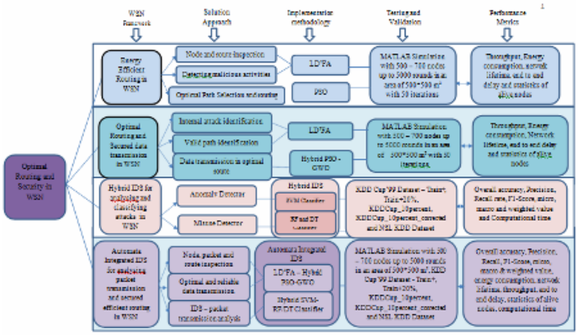

WSN Framework
Solution Approach
Implementation methodology
Testing and Validation
Performance Metrics
1
Optimal Routing and Security in WSN
Energy Efficient Routing in WSN
Node and route inspection
Detecting malicious activities
Optimal Path Selection and routing
LD²FA
PSO
MATLAB Simulation with 500 - 700 nodes up to 5000 rounds in an area of 500*500 m² with 50 iterations
Throughput, Energy consumption, network lifetime, end to end delay and statistics of alive nodes
Optimal Routing and Secured data transmission in WSN
Internal attack identification
Valid path identification
Data transmission in optimal route
LD²FA
Hybrid PSO - GWO
MATLAB Simulation with 500 – 700 nodes up to 5000 rounds in an area of 500*500 m² with 50 iterations
Throughput, Energy consumption, Network lifetime, end to end delay and statistics of alive nodes
Hybrid IDS for analyzing and classifying attacks in WSN
Anomaly Detector
Misuse Detector
Hybrid IDS
SVM Classifier
RF and DT Classifier
KDD Cup'99 Dataset – Train+, Train+20%, KDDCup_10percent, KDDCup_10percent_corrected and NSL KDD Dataset
Overall accuracy, Precision, Recall rate, F1-Score, micro, macro and weighted value and Computational time
Automata Integrated IDS for analyzing packet transmission and secured efficient routing in WSN
Node, packet and route inspection
Optimal and reliable data transmission
IDS – packet transmission analysis
Automata Integrated IDS
LD²FA – Hybrid PSO-GWO
Hybrid SVM-RF/DT Classifier
MATLAB Simulation with 500 – 700 nodes up to 5000 rounds in an area of 500*500 m², KDD Cup'99 Dataset - Train+, Train+20%, KDDCup_10percent, KDDCup_10percent_corrected and NSL KDD Dataset
Overall accuracy, Precision, Recall, F1-Score, micro, macro & weighted value, energy consumption, network lifetime, throughput, end to end delay, statistics of alive nodes, computational time

Fig 1. Overall Framework of the proposed research survey work

The experiment has been evaluated by considering the different set-ups namely Setup 1 and Setup 2. The network parameters such as area of simulation, initial energyof sensor nodes, total number of sensor nodes, simulation rounds and communication rounds are found to be the same in both setups and it only differs in the placement of the base station. The base station is placed at position (500,250) for Setup 1, and for Setup 2, the base station is placed at position (250,250). The performance of LD^{2}FA- PSO, LD^{2}FA-Hybrid PSO-GWO, LD^{2}FA-Hybrid SVM-DT and LD^{2}FA-Hybrid SVM-RF for setup 1 and setup 2 are depicted in Table 1 and Table 2 respectively. The results show that LD^{2}FA-Hybrid SVM-RF has better consumption of energy, network lifetime, throughput but end-to-end delay is slightly higher than the other frameworks.

Table 1 Overall Performance of proposed WSN framework for Setup 1

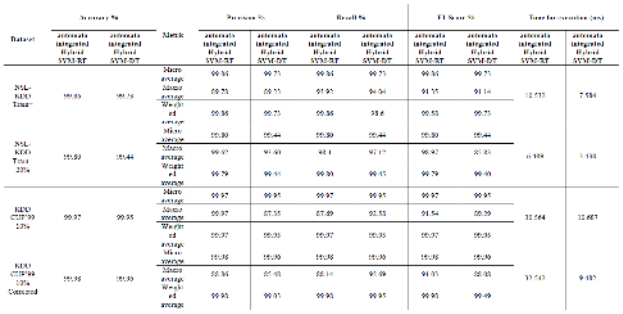
Performance Metric / WSN Framework	Energy Consumption (Joules)	Network Lifetime (rounds)	End-to-end delay (ms)	Throughput (bps)	Statistics of Alive nodes (in number)
LD^{2}FA-PSO	1580	740	0.038	15040	2560
LD^{2}FA-HybridPSO-GWO	1490	800	0.048	16000	2600
LD^{2}FA- Hybrid SVM-DT	1480	830	0.056	16600	2895
LD^{2}FA- Hybrid SVM-RF	1400	855	0.082	17200	2790

The investigational outcomes of the overall performance of automata integrated Hybrid SVM-RF IDS and automata integrated Hybrid SVM-DT IDS is tabulated in Table 3 for the KDDCup'99 and NSL-KDD dataset. It shows the comparison of the two IDS models with respect to accuracy, precision, recall rate, F1-score and computational time.

Table 2 Overall Performance of proposed WSN framework for Setup 2

Performance Metric / WSN Framework	Energy Consumption (Joules)	Network Lifetime (rounds)	End-to-end delay (ms)	Throughput (bps)	Statistics of Alive nodes (in number)
LD^{2}FA-PSO	1980	990	0.0425	18000	2580
LD^{2}FA-Hybrid PSO-GWO	1740	1050	0.0473	18945	2610
LD^{2}FA-Hybrid SVM-DT	1660	1120	0.0845	15800	22810
LD^{2}FA-Hybrid SVM-RF	1640	1210	0.0872	16900	3000

Table 3 Overall Performance of automata integrated Hybrid SVM-RF and Hybrid SVM-DT on various NSL and KDD Dataset



Dataset	Accuracy %		Metric	Precision %		Recall %		F1 Score %		Time for execution (ms)	
	automata integrated Hybrid SVM-RT	automata integrated Hybrid SVM-DT		automata integrated Hybrid SVM-RT	automata integrated Hybrid SVM-DT	automata integrated Hybrid SVM-RT	automata integrated Hybrid SVM-DT	automata integrated Hybrid SVM-RT	automata integrated Hybrid SVM-DT	automata integrated Hybrid SVM-RT	automata integrated Hybrid SVM-DT
NSL-KDD Train+	99.85	99.75	Micro average	99.86	99.73	99.86	99.73	99.86	99.73	12.513	7.584
			Macro average	89.73	89.33	91.93	94.04	91.35	91.14		
			Weighted average	99.86	99.73	99.86	98.6	99.53	99.73		
NSL-KDD Test 20%	99.80	99.44	Micro average	99.80	99.44	99.80	99.44	99.80	99.44	6.189	3.138
			Macro average	99.67	91.60	98.1	97.12	98.92	85.83		
			Weighted average	99.79	99.44	99.80	99.45	99.79	99.40		
KDD CUP'99 10%	99.97	99.95	Micro average	99.97	99.95	99.97	99.95	99.97	99.95	32.564	32.687
			Macro average	99.97	87.35	87.49	92.53	91.54	89.29		
			Weighted average	99.97	99.95	99.97	99.95	99.97	99.95		
KDD CUP'99 10% Corrected	99.98	99.90	Micro average	99.98	99.90	99.98	99.90	99.98	99.90	32.543	9.482
			Macro average	88.86	85.48	88.14	93.49	91.03	88.08		
			Weighted average	99.93	99.05	99.93	99.95	99.93	99.49		

4. Conclusion

This section summarizes the major research outcomes that has beenobtained in this literature study and also highlights the future research directions appliedin the field of wireless sensor networks. As a summary the following contributions are proposed in this paper. The first contribution is proposing an automata-based system to provide an energy efficient routing in wireless sensor networks. The second contribution is designing a hybrid computationalintelligence-based optimization algorithm to optimize the routes as well as to secure the data transmission in wireless sensor networks. As a third contribution designing an efficient hybrid intrusion detection model to detect and classify the attacks. The last and foremost contribution is integrating the automata with the intrusion detection model so that the attacks can be identified and monitored by the automaton system in wireless sensor network.

4.1 Research outcomes

Wireless sensor networks face many challenging issues in designingan efficient network such as consumption of power, clustering, security, scalability, reliability related to WSN domain. The first and foremost factor isto design an energy efficient WSN using automata incorporated computationalintelligence technique with minimum consumption of energy of the network that extends the lifetime of the network. And next is to design an energy efficient routing in wireless sensor network that focuses to provide a better end- to-end delay by improving throughput so that the packet transmission takes place at a faster rate with minimal interruptions. Based on these factors and research objective an automaton-based system integrated with IDS was designed to continuously monitor the network activities in order to improve energy utilization, extend network lifetime, reduce end-to-end delay and to transmit packets at a faster rate without any interruptions.

In the first work module, A Learning Dynamic Deterministic Finite Automata (LD^{2}FA) was proposed that dynamically learns the environment of the networkand also adapts to any changes that occur in the network i.e. if any failure occurs in the sensor nodes the automata handles it faster and does the necessary changes to provide uninterrupted packet transmission. Next, a computational intelligence technique namely PSO algorithm was used along with LD^{2}FA thatobtained the optimal route through which the energy needed for transmitting packets was minimized as well as throughput was improved. The experimentswere evaluated on simulating the network environment for two differentscenarios namely, Network 1 and Network 2. The base station was placed at different locations in these two Networks consequently to evaluate the performance of the proposed work LD^{2}FA-PSO model. The performance metrics such as utilization of energy, lifetime of the network, throughput, statistics of alive nodes and end-to-end delay was evaluated and analyzed for the proposed system LD^{2}FA-PSO which was then compared with the existing algorithms like PSO proposed by PratyayKuila & Prasanta K. Jana (2014), Greedy Load Balanced Clustering Algorithm (GLBCA) presented by Chor Ping Low et al (2008) and Genetic Algorithm based clustering (GA) proposed by Pratyay Kuila et al (2013).

In second work module, LD^{2}FA has been integrated with the Computational Intelligence technique such as Particle Swarm Optimization (PSO) and Grey Wolf Optimizer (GWO) algorithm which provides an optimal route to transmit data as well as detection of sybil attack and selective forwarding attack has beenimplemented to eliminate malicious nodes that affect the network so that the utilization of energy of the sensor nodes can be minimized, improving throughput, reduces end-to-end delay and enhancing network lifetime. The experiment has been simulated for the same two different network setups namely, Network 1 and Network 2. Investigation was done to build an efficient Hybridized IDS model to classify the attacks classes for the standard KDDCup’99 intrusion detection dataset and NSL-KDD intrusion detection dataset. Hybridization of SVM and RF classifiers as well as Hybridization of SVM and DT classifiers were done by applying misuse and anomaly detection approach to improve the overall accuracy, precision/detection rate, recall rate and computational time. The standard intrusion detection NSL-KDD dataset was segregated into three datasets, precisely dataset 1, dataset 2 and dataset 3 and training has been done on 80% samples and the learnt model has been tested on 20% samples. The analysis for NSL- KDD dataset has been performed on the performance metrics such as overall accuracy, detection/precision rate, computational time, recall rate and F1-Score and compared with the existing approaches such as SVM_Linear and SVM_RBF suggested by Iftikhar Ahmad et.al (2018), RF proposed by Iftikhar Ahmad et.al (2018) and DT proposed by (Vaishali Kosamkar 2014).

In third work module, Learning Dynamic Deterministic Finite Automata (LD^{2}FA) Hybrid PSO-GWO model has been integrated with the Hybridized IDS model to secure the data packets during transmission in the wireless sensor network as well as the automaton continuously monitors the activities of the network. The automaton is integrated with IDS so any attacks that occurs during data transmission could be automatically identified as well as sybil attack and selective forwarding attack detection takes place which help the model to transmit packets in an uninterrupted route. The proposed model secures the network and achieves high overall accuracy, detection rate, recall rate as well as improves the utilization of energy, reduces end-to-end delay, improves networklifetime and throughput. The experiment has been simulated for the same two differentnetwork setups namely, Network 1 and Network 2. The overall accuracy, recall rate, precision rate and F1-Score are measured and compared with prior art approaches such as SVM_Linear and SVM_RBF suggested by Iftikhar Ahmad et.al (2018), RF proposed by Iftikhar Ahmad et.al (2018) and DT proposed by (Vaishali Kosamkar 2014) for the NSL-KDD dataset as well as KDDCup'99 data set and the NSL-KDD dataset has beendivided into three datasets and further the model is trained on 90% training samples and tested on 10% testing samples. As well as the automata integrated Hybridized IDS is compared with the existing algorithms such as without automata integrated IDS LD^{2}FA-Hybrid PSO-GWO, PSO proposed by Pratyay Kuila & Prasanta K. Jana (2014), GLBCA deployed by Chor Ping Low et al (2008) and GA proposed by Pratyay Kuila et al (2013).

4.2 Future Enhancement

During the proposed survey research work, few research directions were identified that can enhance or improvise this work for further research and development inthe field of wireless sensor network. In this research work survey, static nodes were used but when compared to static nodes mobile nodes are more versatile and can be deployed in any situation and also adapts to quick topological changes. Therefore, the proposed model can be developed by considering the mobility of sensor nodes for WSNs.

Next, the proposed model in this thesis work have been tested only using simulators it can be further investigated on real sensors or real network environment for small as well as large networks so that there might be significant impact on the performance of the network in the wireless sensor network. Further the proposed model could also be evaluated on the metrics such as packet delivery ratio, packet loss ratio, computation cost and operation cost.

As a future research direction, the WSN could be designed to solve the issues related to scalability, reliability, confidentialityand integrity. In this work, sybil attack and selective forward attack have been implemented. There are various otherattacks such as blackhole attack, wormhole attack, gray hole attack and sink attacks that can also be implemented as future research in WSNs. In the future the proposed model can be further investigated onreal world network traffic as well as can be used on specific simulator or real time network deployment instead of open source network simulator.

References

Agnihotri A. & Gupta I. K. 2018, A hybrid PSO-GA algorithm for routing in wireless sensor network, *IEEE 4th International Conference on Recent Advances in Information Technology*, Dhanbad, India, 15-17 March, pp. 1-6. DOI: 10.1109/RAIT.2018.8389082

Abhishek Maity 2016, ‘Supervised Classification of RADARSAT-2 Polarimetric Data for Different Land Features’, (arXiv:1608.00501v1), [1 Aug2016].

Abduvaliyev A., Lee S. and Lee Y.-K. 2010, Energy efficient hybrid intrusion detection system for wireless sensor networks, *International Conference on Electronics and Information Engineering*, Vol. 2, pp. V2-25-V2-29.

Sharifi A., F.F. Zad, F. Farokhmanesh, A. Noorollahi, J. Sharifi 2014, 'An Overview of Intrusion Detection and Prevention Systems (IDPS) and Security Issues', IOSR Journal of Computer Engineering (IOSR-JCE), vol. 16, no. 1, pp. 47-52.

Akila I.S, Manisekaran S.V, Venkatesan, S.V 2017, 'Modern Clustering Techniques in Wireless Sensor Networks' Wireless Sensor Networks-Insights and Innovations; Sallis, P.J.; Ed.; InTech Open: London, UK, pp. 141–156.

Akyildiz I.F, Su.W, Sankarasubramaniam.Y, Cayirci.E 2002, 'Wireless Sensor Networks: a survey', Computer Networks, vol. 38, no. 4, pp. 393-422.

Al-Aboody. N. A. & Al-Raweshidy H. S. 2016, 'Grey wolf optimization-based energy-efficient routing protocol for heterogeneous wireless sensor networks', in 4th International Symposium on Computational and Business Intelligence (ISCBI), Olten, pp. 101-107.

Al-Karaki A. Kamal 2004, 'Routing Techniques in Wireless Sensor networks: A Survey', Security and Networks, vol. 11, no. 6, pp. 6-28.

Toor A. S. & Jain, A K 2018, 'A Novel Energy Efficient RoutingProtocol EACBM for Scalable Wireless Sensor Networks', *International Journal of Computer Network and Information Security* vol. 10, no. 5, pp. 9- 17.

Amirhosein Fathinavid, Amir Bagheri Aghababa, Alireza Enami Eraghi and A.Farahani 2013, 'CADLA: an efficient cluster-based anomaly nodesdetection for mobile ad-hoc networks: a learning automata approach', Journal of Information Assurance and Security, vol. 8, pp. 250-259.

Ana Paula R. da Silva, Marcelo H. T. Martins, Bruno P. S. Rocha, Antonio A. F. Loureiro, Linnyer B. Ruiz, and Hao Chi Wong 2005, 'Decentralized intrusion detection in wireless sensor networks', in Proceedings of the 1st ACMinternational workshop on Quality of service & security in wireless and mobilenetworks, pp. 16–23.

Anat Bremler-Barr, David Hay, Yaron Koral 2014, 'CompactDFA: Scalable Pattern Matching Using Longest Prefix Match Solutions', IEEE Trans.Networking, vol. 22, pp. 415-428.

Anderson, J 1995. 'An introduction to neural networks', Cambridge: MIT Press.

Andy Liaw & Matthew Wiener 2002, 'Classification and Regression by Random Forest', R News, vol. 2, no. 3, pp. 18-22.

Ataul Bari, Arunita Jaekel, Subir Bandyopadhyay 2008, 'Clustering strategies for improving the lifetime of two-tiered sensor networks', ComputerCommun., vol. 31, pp. 3451-3459.

Scholkopf B. and Smola A.J. 2001, 'Learning with Kernels:Support Vector Machines, Regularization, Optimization, and Beyond. MIT Press.

Rashid B., Rehmani M.H. 2016, 'Applications of wirelesssensor networks for urban areas: A survey', Journal of Network and ComputerApplications, vol. 60, no. C, pp. 192–219.

Butun, I, Morgera, S, Sankar 2014, 'A survey of intrusion detectionsystems in wireless sensor networks', IEEE Commun Surv Tut; vol. 16, no. 1,pp. 266-282.

Charles Elkan 2000, 'Results of the KDD'99 classifier learning', ACM SIGKDD Explorations Newsletter, vol. 1, no. 2, pp. 63-64.

Chen Yi-Ping & Chen Yu-Zhong 2010, 'A Novel energy efficient routingalgorithm for wireless sensor networks', in Proceedings of ninth international conference on machine learning and cybernetics, pp. 1031-1035.

Chee-Yee Chong & Srikanta P. Kumar 2003, 'Sensor networks: Evolution,opportunities, and challenges', in Proc. IEEE vol. 91, no. 8, pp. 1247-1256.

Chor Ping Low, Can Fang, Jim Mee Ng, Yew Hock Ang 2008, 'Efficient Load-Balanced Clustering Algorithms for Wireless Sensor Networks', Computer Communications, vol. 31, pp. 750-759.

Cortes & Vapnik 1995, 'Support-vector networks', Machine Learning, vol.20, pp. 273-297.

Danish Mahmood, Nadeem Javaid, Shaharyar Mahmood, S. U. Qureshi, S. U. Qureshi, A. M. Memon and T. Zaman 2013, 'MODLEACH: A variant of LEACH for WSNs', in Proceeding of 8th Int. Conf. Broadband Wireless Comput. Commun. Appl. (BWCCA), pp. 158-163.

Deepthy K Denatious & Anita John, 2012, 'Survey on data mining techniques to enhance intrusion detection', in International Conference on Computer Communication and Informatics, pp. 1–5.

Dennis Decoste & Nello Cristianini 2002. 'Training Invariant Support Vector Machines', Machine Learning, vol. 46, pp. 161-190.

Devaraju Sellappan & Ramakrishnan Srinivasan 2014, 'Performance Comparison for Intrusion Detection System Using Neural Network with KDDDataset', ICTACT Journal on Soft Computing, vol. 4, no.3, pp. 743-752.

Divyatmika & Manasa Sreekesh 2016, 'A Two-tier Network based Intrusion Detection System Architecture using Machine Learning Approach', in Electrical Electronics and Optimization Techniques (ICEEOT) InternationalConference, pp. 42-47.

Dua, D. & Graff, C 2019, 'UCI Machine Learning Repository', Irvine, CA:University of California, School of Information and Computer Science. Available from: <<http://archive.ics.uci.edu/ml>>

Elham Hajian, Kamal Jamshidi and Ali Bohlooli 2010, 'Improve Energy Efficiency Routing in WSN by using Automata', International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), vol. 1, no. 2, pp. 1-7.

Elshakankiri, M.N., Moustafa, M.N., and Dakroury, Y. 2008, 'Energy Efficient Routing Protocol for Wireless Sensor Networks', in International Conference on Intelligent Sensors, Sensor Networks and Information Processing, pp. 393-398.

Farzad Kiani 2016, ‘AR-RBFS: Aware-Routing Protocol Based on Recursive Best-First Search Algorithm for Wireless Sensor Networks’, Journalof Sensors, vol. 2016, pp. 1-10.

Fatemeh Barani 2014, ‘A Hybrid Approach for Dynamic Intrusion Detection in Ad Hoc Networks Using Genetic Algorithm and Artificial Immune System’, *In Proc. of the 2014 Iranian Conference on Intelligent Systems(ICIS’14)*, Bam, Iran, pp. 1-6.

Fathinavid, A & Aghababa 2012, ‘A protocol for intrusion detection based on learning automata in forwarding packets for distributed wireless sensor networks’, in Proceedings of the international conference on cyber-enabled distributed computing and knowledge discovery, Sanya, China, pp.373–380.

Amirhossein Fathinavid, Ansari, M 2015, ‘CLAIDS: cellular learningautomata-based approach for anomaly nodes detection in clustered mobile ad hoc networks’, Ad Hoc Sens Wirel Netw, vol. 29, no. 1, pp. 31-51.

Fei Hu & Neeraj K.Sharma 2005, ‘Security considerations in ad hoc sensornetworks’, Ad Hoc Networks, vol. 3, no. 1, pp. 69-89.

Furtado.H & Trobec.R 2011, ‘Applications of Wireless Sensors in Medicine’, in MIPRO, 2011 Proceedings of the 34th International Convention,pp. 257–261.

Gao Yi, Sun Guiling, Li Weixiang and Pan Yong 2009, ‘Recluster- LEACH: A recluster control algorithm based on density for wireless sensor network’, in Proceeding of 2nd International Conference on Power Electronicsand Intelligent Transportation System, vol. 3, pp. 198-202.

Georgios Smaragdakis, Ibrahim Matta, Azer Bestavros 2004, ‘SEP: A Stable Election Protocol for clustered heterogeneous wireless sensor networks’,in Proceedings of SANPA, pp. 1-11.

Gregory J Pottie, William J Kaiser 2000, ‘Wireless integrated network sensors’, Commun. ACM, vol. 43, pp. 51-58.

Gui Jing-Jing, Wang Jin-Shuang, Zhang Yu-Sen, and Zhang Tao 2011, ‘Formal threat analysis for ad-hoc routing protocol: modelling and checking thesybil attack’, Intelligent Automation & Soft Computing, vol. 17, no. 8, pp. 1035–1047.

Hao Ge, Shenghong Li, Jianhua Li and Xudie Ren 2017, ‘A Parameter-Free Learning Automaton Scheme’, Cornell University Library, pp. 1-13.

Hao Sheng., Zhang Huyin, Song Mengkai 2018, ‘A stable and energy- efficient routing algorithm based on learning automata theory for MANET’, Journal of Communications and Information Networks, vol. 3, no. 2, pp. 52-66.

Hichem Sedjelmaci and Sidi Mohammed Senouci 2014, ‘A Lightweight Hybrid Security Framework for Wireless Sensor Networks’, IEEE InternationalConference on Communications (ICC), Sydney, NSW, 2014, pp. 3636-3641.

Hiren Kumar Deva Sarma and Avijit Kar 2006, ‘Security Threats inWireless Sensor Networks’, Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International, pp. 243 -251.

Hui Zhou, Dongliang Qing, Xiaomei Zhang, Honglin Yuan, Chen Xu 2012,‘A Multiple-Dimensional Tree Routing Protocol for Multi sink Wireless SensorNetworks based on Ant Colony Optimization’, International Journal of Distributed Sensor Networks, vol. 2012, pp. 1-10.

Huy Anh Nguyen, Deokjai Choi 2008, ‘Application of Data Mining to Network Intrusion Detection: Classifier Selection Model’, Springer-Verlag, pp.399-408.

Iftikhar Ahmad, Mohammad Basheri, Muhammad Javed Iqbal and Aneel Rahim 2018, ‘Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection’, IEEE Access, vol. 6, pp. 33789-33795.

Esmaily J., R. Moradinezhad and J. Ghasemi 2015, Intrusion detection system based on multi-layer perceptron neural networks and decision tree’, in 7th International Conference on Information and KnowledgeTechnology, pp. 1-5.

Jamal N. Al-Karaki and Ahmed E. Kamal 2006, ‘Applying Intrusion Detection Systems to Wireless Sensor Networks’, in Proceedings of IEEE Consumer Communications and Networking Conference (CCNC), pp. 640– 644.

Cannady J.D., B.C. Rhodes and J.A.Mahaffey 2000, ‘Multiple self-organizing maps for intrusion detection’, in *Proceedings of the 23rd National Information Systems Security Conference*, Baltimore, MD.

Kennedy J. & Eberhart R. 1995, ‘Particle Swarm Optimization’, in proceedings of the 1995 IEEE International Conferenceon Neural Network, pp. 1942-1948.

Branch J.W. 2003, ‘Extended Automata-Based Approaches to IntrusionDetection’, Thesis Report, Rensselaer Polytechnic Institute Troy, New York.

Zhang J. & Zulkernine M. 2006, ‘Anomaly based network intrusion detection with unsupervised outlier detection’, in Symposium on network security and information assurance – *Proceedings of the IEEE International Conference on Communications (ICC)*, Istanbul,Turkey, vol. 5, pp. 2388-2393.

Scarfone K., Mell P. 2007, ‘Guide to intrusion detection and prevention systems (IDPS)’, NIST Special Publication. Available from: <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>

Karlof C. & Wagner D. 2003, ‘Secure routing in wireless sensor networks: Attacks and countermeasures’, in First IEEE International Workshop on SensorNetwork Protocols and Applications, pp. 113–127.

Kayacik H. G., Zincir-Heywood A. N., Heywood M. I. 2005, ‘Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Benchmark’, in proceedings of the PST 2005 – International Conference on Privacy, Security, and Trust, pp. 85-89.

Kemmerer, R. A., & Vigna, G. 2002, ‘Intrusion detection: A brief history and overview’, IEEE Security and Privacy Magazine, vol. 35, no.4, pp. 27-30.

Kumar Neeraj, Tyagi, Sudhanshu, Deng, Der-Jiunn 2014, 'LA-EEHSC: Learning automata-based energy efficient heterogeneous selective clustering for wireless sensor networks', Journal of Network and Computer Applications,vol. 46, pp. 264-279.

Kumar Parasuraman & Anbarasa Kumar 2018, 'Performance Comparisonof Multi class SVM, Support Vector Machine, k-NN and Binary Classification for Intrusion Detection', International Journal of Computer Sciences and Engineering, vol. 6, no. 8, pp.204-211.

Kuo-Qin Yan, Shu-Ching Wang, Shun-Sheng Wang and C. W. Liu 2010, 'Hybrid Intrusion Detection System for Enhancing the Security of a Cluster- based Wireless Sensor Network', in proceedings of the 3rd IEEE InternationalConference on Computer Science and Information Technology (ICCSIT '10), pp. 114–118.

Leonardo B Oliveira, Adrian Ferreira, Marco A Vilaça, Hao Chi Wong, Marshall Bern, Ricardo Dahab, Antonio AF Loureiro 2007, 'SecLEACH – Onthe security of clustered sensor networks', Signal Processing, vol. 87, pp. 2882–2895.

Li Han 2010, 'LEACH-HPR: An energy efficient routing algorithm for Heterogeneous WSN', in proceedings of IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS), vol. 2, pp. 507–511.

Lior Rokach and Oded Maimon 2014, 'Data Mining with Decision Trees: Theory and Applications', 2nd Edition, World Scientific, Series in Machine Perception Artificial Intelligence, vol. 81.

Logambigai.R & Kannan.A 2018, 'Energy conservation routing algorithmfor wireless sensor networks using hybrid optimization approach', InternationalJournal of Communication Networks and Distributed Systems, vol. 20, no. 3.

Low CP, Fang C, Ng JM, Ang YH 2008, 'Efficient load-balanced clustering algorithms for wireless sensor networks', Computer Communications, vol. 31, no. 4, pp. 750-759.

Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu and Ali Akbar Ghorbani 2009, 'A Detailed Analysis of the KDD CUP 99 Data Set', in proceedings of Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), pp.1-6.

Mahbod Tavallaee, Natalia Stakhanova and Ali Akbar Ghorbani 2010, 'Toward credible evaluation of anomaly-based intrusion detection methods,' IEEE Transactions on Systems, Man, and Cybernetics, Part-c: (Applications and Reviews), vol. 40, no. 5, pp. 516-524.

Majid Gholipour & Mohammad Reza Meybodi 2008, 'LA-mobicast: A learning automata based mobicast routing protocol for wireless sensor networks', Sensor Letters, vol. 6, no. 2, pp. 305-311.

Mao Ye, Chengfa Li, Guihai Cehn and J. Wu 2005, 'EECS: An Energy Efficient Clustering Scheme in Wireless Sensor Networks', in Proceedings of IEEE International Performance Computing and Communications Conference(IPCCC), pp. 535-540.

Marin, G.A 2005, 'Network security basics', Security & Privacy, IEEE, vol. 3, no. 6, pp. 68-72.

Matt Bishop 2004, 'Computer Security: Art and Science', Addison Wesley,Pearson Education, Inc., Boston.

Matteo Avalle, Fulvio Risso and Riccardo Sisto 2012, 'Efficient Multistriding of Large Non-deterministic Finite State Automata for Deep Packet Inspection' in proceedings of IEEE International Conference on Communications (ICC), Ottawa, Ontario, pp. 1079-1084.

McHugh J 2000, 'The 1998 Lincoln laboratory IDS evaluation. A critique', in proceedings of the Recent Advances in Intrusion Detection, pp. 145–61.

McHugh J 2000, 'Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory', ACM Transactions on Information and System Security, vol. 3, no. 4, pp. 262–294.

Md. Al Mehedi Hasan, Mohammed Nasser and Biprodip Pal 2013, 'On the KDD'99 Dataset: Support Vector Machine Based Intrusion Detection System (IDS) with Different Kernels', International Journal of Electronics Communication and Computer Engineering, vol. 4, pp. 1164-1170.

Md. Al Mehedi Hasan, Mohammed Nasser, Shamim Ahmad, Khademul Islam Molla 2016, 'Feature Selection for Intrusion Detection Using Random Forest', Journal of Information Security, vol. 7, pp. 129-140.

Md Azharuddin and Prasanta K. Jana 2017, 'PSO-based approach for energy-efficient and energy-balanced routing and clustering in wireless sensornetworks', Soft Computing, vol. 21, no. 22, pp. 6825–6839.

Megha Jain Gowadiya 2016, 'An Optimised Approach for Intrusion Detection in KDD CUP 99 Dataset Using KNN & GA', International Journal of Scientific & Engineering Research, vol. 7, no. 6.

Michael Riecker, Sebastian Biedermann, Rachid El Bansarkhani, MatthiasHollick, 2014, 'Lightweight energy consumption-based intrusion detectionsystem for wireless sensor networks', International Journal of Information Security, vol. 14, no. 2, pp. 155-167.

Michael Okwori, Muhammad Enagi Bima, Ogbole Collins Inalegwu, Munira Saidu, Waheed Audu, U. Abdullahi 2016, 'Energy Efficient Routing inWireless Sensor Network Using Ant Colony Optimization and Firefly Algorithm', International Conference on Information and Communication Technology and Its Applications, pp.236-242.

Misra, S, Abraham, K, Obaidat, M 2009, 'LAID: a learning automata-based approach for intrusion detection in wireless sensor networks', Secure Communication Network, vol. 2, no. 2, pp. 105–115.

MK Jain 2011, 'Wireless Sensor Networks: Security Issues and Challenges', International Journal of Computer and Information Technology, vol. 2, no. 1, pp. 62-67.

Mohammad Ilyas and Imad Mahgoub 2005, ‘Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems’, CRC Press.

Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas 2012, ‘An Implementation of Intrusion Detection System Using Genetic Algorithm’, International Journal of Network Security & Its Applications(IJNSA), vol.4, no.2.

Mostafaei, Habib & Meybodi, Mohammad & Esnaashari, Mehdi 2010, ‘ALearning Automata Based Area Coverage Algorithm for Wireless SensorNetwork’, Journal of Electronic Science and Technology, vol. 8, no.3, pp. 200–205.

Mrutyunjaya Panda & Manas Ranjan Patra 2009, ‘A Hybrid Clustering approach for network intrusion detection using COBWEB and FFT’, Journal ofIntelligent system, vol. 18, no.3, pp. 229-245.

Mrutyunjaya Panda, Ajith Abraham, Swagatam Das and Manas Ranjan Patra 2011, ‘Network Intrusion Detection System: A Machine Learning Approach. Intelligent Decision Technologies’, vol. 5, no. 4, pp. 347-356.

Muhammad Shakil Pervez and Dewan Md. Farid 2014, ‘Feature Selectionand Intrusion classification in NSL-KDD Cup 99 Dataset Employing SVMs’, The 8th International Conference on Software Knowledge Information Management and Applications (SKIMA 2014), pp. 1-6.

Mukhdeep Singh Manshahia 2015, ‘A Firefly Based Energy Efficient Routing in Wireless Sensor Networks’, African Journal of Computing and ICT(IEEE), vol.8, no.4, pp. 27-32.

Mukherjee B, Heberlein LT, Levitt KN 1994, ‘Network intrusion detection’, IEEE Network, vol. 8, no. 3, pp. 6-41.

Nadiammai, G. V and M. Hemalatha 2014, ‘Effective approach toward Intrusion Detection System using data mining techniques’, Egyptian Informatics Journal, vol. 15, no. 1, pp. 37-50, 2014.

Nasser Abouzakhar, Gordon A. Manson 2004, ‘Evaluation of Intelligent Intrusion Detection Models’, The International Journal of Digital Evidence, vol. 3, no. 1.

Ossama Younis and Sonia Fahmy 2004, ‘HEED: A Hybrid Energy- Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks’, IEEETransactions on Mobile Computing, vol. 3, no. 4, pp. 660-669.

Ossama Younis, Marwan Krunz, and Srinivasan Ramasubramanian 2006, ‘Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges’, in IEEE Network, vol. 20, no. 3, pp. 20-25.

Paul Innella & McMillan, O 2001, ‘An Introduction to Intrusion DetectionSystems’, Tetrad Digital Integrity, LLC.

Pedregosa F, Varoquaux, Ga"el, Gramfort A, Michel V, Thirion B, Grisel O, et al 2011, ‘Scikit-learn: Machine learning in Python’, Journal of machine learning research, vol.12, pp. 2825-30.

Peter Schaffer, Karoly Farkas, Adam Horvath, Tamas Holczer, Levente Buttyan 2012, ‘Secure and reliable clustering in wireless sensor networks: A critical survey’, ACM, Computer Networks: The International Journal of Computer and Telecommunications Networking, vol.5, no. 11, pp. 2726-2741.

Pradhan, W. Ward, K. Hacioglu, J. Martin, and D. Jurafsky 2004, ‘Shallow semantic parsing using support vector machines’, Conference of the North American Chapter of the Association for Computational Linguistics & HumanLanguage Technologies (NAACL-HLT), pp. 233-240.

Pratyay Kuila and Prasanta K.Jana 2014, ‘Energy efficient clustering androuting algorithms for wireless sensor networks: Particle swarm optimization approach’, Engineering Applications of Artificial Intelligence, vol. 33, pp. 127– 140.

Puketza N, Zhang K, Chung M, Mukherjee B, Olsson R 1997, ‘A methodology for testing intrusion detection systems’, IEEE Software, vol. 4, no. 5, pp. 43–51.

Qi Dong & Donggang Liu 2009, ‘Resilient cluster leader election for wireless sensor network’, in proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON 2009, Italy. pp. 1-9.

Quinlan 1993, ‘C4.5: Programs for Machine Learning’, Morgan Kaufmann Publishers, San Mateo, CA.

Radim Belohlavek Vilem Vychodil 2010, ‘Discovery of optimal factors in binary data via a novel method of matrix decomposition’, Journal of Computer and System Science, vol. 76, no. 1, pp. 3-20.

Rashid Hussain, JL Sahal, Purvi Mishra, Babita Sharma 2012, ‘Application of WSN in rural development, Agricultural water management’, International Journal of Soft Computing and Engineering, vol .2, pp.68-72.

Roman R., Zhou J., and Lopez J. 2006, ‘Applying Intrusion Detection Systems to Wireless Sensor Networks’, 3rd IEEE Consumer Communicationsand Networking Conference, 2006., Las Vegas, NV, USA, pp. 640–644.

Rebecca Gurley Bace 2000, ‘Intrusion detection’, Indianapolis, USA: Macmillan Technical Publishing.

Ross Quinlan 1986, ‘Induction of Decision Trees’, Machine Learning, vol. 1, no. 1, pp. 81–106

RStudio Team 2015, ‘RStudio: Integrated Development for R’, RStudio, Inc., Boston, MA. Available from: <http://www.rstudio.com>

Sahabul Alam & Debashis De 2014, ‘Analysis of Security Threats inWireless Sensor Network’, International Journal of Wireless & Mobile Networks (IJWMN), vol. 6, no. 2, pp. 35-46.

Sahu S K, S. Sarangi, and S. K. Jena 2014, ‘A detail analysis on intrusiondetection datasets’, In Advance Computing Conference (IACC) IEEEInternational, Gurgaon, India, pp. 1348–1353.

Sandip Hingane & Umesh Kumar Lilhore 2018, ‘A Hybrid Intrusion Detection Technique Based on IRF & AODE for Kdd-Cup 99 Dataset’, International Research Journal of Engineering and Technology (IRJET), vol. 5,no.6, pp.938-942.

Santar Pal Singh and Subhash Chander Sharma 2017, 'A Particle SwarmOptimization Approach for Energy Efficient Clustering in Wireless Sensor Networks', International Journal of Intelligent Systems and Applications, vol. 6, pp. 66-74.

Sasikumar P, Sibaram Khara 2012, 'K-Means Clustering in Wireless Sensor Networks', in Proceedings of IEEE Fourth International Conference ofComputational Intelligence and Communication Networks (CICN), pp. 140- 144.

Schaffera.P, Farkas.K, Horvath.A, Holczer.T and Buttyan.L 2012, 'Secure and reliable clustering in wireless sensor networks: a critical survey. Computer Networks', vol. 56, no. 11, pp. 2726–2741.

Seyedali Mirjalili, Seyed Mohammad Mirjalili, Andrew Lewis 2014, 'Grey Wolf Optimizer', Advances in Engineering Software, vol. 69, pp. 46-61.

Sheng-Shih Wang & Ze-Ping Chen 2013, 'LCM: A link-aware clustering mechanism for energy-efficient routing in wireless sensor networks',IEEE Sensors Journal, vol. 13, no. 2, pp. 728-736.

Shubhangi Singh & Rajendra Singh Kushwah 2016, 'Energy Efficient Approach for Intrusion Detection System for WSN by applying Optimal Clustering and Genetic Algorithm', in Proceedings of the international conference on advances in information communication technology &computing—AICTC '16, New York, NY: ACM Press, pp. 1-6.

Shujuan Jin & Keqiu Li 2009, 'LBCS: A Load Balanced Clustering Scheme in Wireless Sensor Networks', Third International Conference on Multimedia and Ubiquitous Engineering, pp.221-225.

Sohrabi.K, Gao.J, Ailawadhi.V and Pottie G.J. 2000, Protocols for self-organization of a wireless sensor networks, *IEEE Personal Communications*, Vol. 7, no. 5, pp. 16-27.

Sutharshan Rajasegarar, Christopher A Leckie, and Marimuthu Palaniswami 2008, 'Anomaly detection in wireless sensor networks', IEEE Wireless Communications, vol. 15, no. 4, pp. 34-40.

Sven Dietrich, David Dittrich, Jelena Mirkovic, Peter Reiher 2005, 'Internet Denial of Service: Attack and Defense Mechanisms', Prentice Hall.

Svetnik, V., Liaw, A., Tong, C., Culberson, J.C., Sheridan, R.P. and Feuston, B.P. 2003, 'Random Forest: A Classification and Regression Tool forCompound Classification and QSAR Modeling', Journal of ChemicalInformation and Computer Sciences, vol. 43, pp. 1947-1958.

Thein T., S.-D. Chi, and J.S. Park 2008, 'Increasing availability and survivability of cluster head in WSN', in Proceedings of the 3rd International Conference on Grid and Pervasive ComputingSymposia/Workshops, GPC 2008, pp. 281–285.

Vaidyanathan.S & Vaidyanathan.M 2011, 'Wireless Sensor Networks- Issues & Challenges. Information Systems: Behavioral & SocialMethods', eJournal, Available from: <https://ssrn.com/abstract=1972636> [28 November 2011]

Vimalarani C, Subramanian R, Sivanandam S N 2016, 'An enhanced PSO-based clustering energy optimization algorithm for wireless sensor network', Scientific World Journal, vol. 2016, pp. 1-11.

Jing-Xin W., Zhi-Ying W. and Kui D. 2004, 'A network intrusion detection system based on the artificial neural networks', International Conference on Machine Learning and Cybernetics, vol. 3. pp. 1337-1342.

Loh W.-Y. 2008, 'Classification and regression tree methods', Encyclopedia of statistics in quality and reliability, Ruggeri, Kenett and Faltin(eds.), Wiley, pp. 315–323.

Heinzelman W.R., A. Chandrakasan, and H. Balakrishnan 2000, 'Energy-Efficient Communication Protocol for Wireless Microsensor Networks', in Proceedings of the Hawaii Conference on System Sciences, vol.2, pp. 10.

Wenke Lee and Salvatore J. Stolfo 2000, 'A framework for constructingfeatures and models for intrusion detection systems', ACM Transactions on information and system security (TISSEC), vol. 3, no. 4, pp. 227-26.

Xiaoqiang Zhao, Hui Zhu, Slavisa Aleksic, Qiang Gao 2018, 'Energy- Efficient Routing Protocol for Wireless Sensor Networks Based on Improved Grey Wolf Optimizer', KSII Transactions on Internet and Information Systemsvol. 12, no. 6. pp. 2644-257.

Yan Sun and Min Sik Kim 2011, 'DFA-Based Regular Expression Matching on Compressed Traffic. Communications', (ICC) IEEE International Conference on Communications, pp. 1-5.

Yahia, Ibrahim & Gaafar, Adel. 2019, 'Energy Efficient Routing Protocol for Heterogeneous Wireless Sensor Networks', Journal of Engineeringand Computer science, vol.20, no. 1.

Yi-an Huang & Wenke Lee 2003, 'A cooperative intrusion detection system for ad hoc networks', in SASN: Proceedings of the 1st ACM workshopon Security of ad hoc and sensor networks, pp. 135–147.

Yick.J, Mukherjee.B, Ghosal.D 2008, 'Wireless Sensor Network Survey', Computer Networks, vol. 52, no. 12, pp. 2292-2330.

Aung Y.Y. and Min M.M. 2018, 'Hybrid Intrusion Detection System using K-means and Classification and Regression Trees Algorithms', 19th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pp.195-199.

Zhang Y. and Lee W. 2000, 'Intrusion detection in wireless ad-hoc networks', in MobiCom'00: Proceedings of the 6th annual international conference on Mobile computing and networking, ACM Press, pp. 275–283.

Zhang Y., Lee W., Huang Y.-A. 2003, 'IntrusionDetection Techniques for Mobile Wireless Networks', Wireless Networks, vol.9, pp. 545-556.

Zhou, H., Qing, D., Zhang, X., Yuan, H., Xu, C 2012, 'A multiple- dimensional tree routing protocol for multi sink wireless sensor networks based on ant colony optimization', *International Journal of Distributed Sensor Networks*, vol. 2012, pp. 1-12.

KDD Dataset: Available from: <<http://kdd.ics.uci.edu/databases/ kddcup99/kddcup/>>

NSL-KDD dataset, Available from: <<http://nsl.cs.unb.ca/NSL-KDD/>>

MIT Lincoln Labs, 1998 DARPA Intrusion Detection Evaluation. Available from: <http://www.ll.mit.edu/mission/communications/ist/ corpora/ideval/ index.html> [February 2008]

MIT Lincoln Laboratory, DARPA Intrusion Detection Evaluation, MA, USA. July, 2010. Available from: <http://www.ll.mit.edu/CST.html,>

Biographical notes

Dr. S. Prithi is of the Department of Computer Science and Engineering, Sri Rajalakshmi Engineering College Chennai, India while Professor **S. Sumathi** is a Professor at the Department of Electrical and Electronics Engineering, PSG College of Technology, Coimbatore, India