The Feasibility Of D-FICCA To Detect Intrusion Detection in WSN

[1] T.Kamalaharidharini, [2] T.keerthana, [3] R.Kalipriyadharshini, [4] K.S.Dhanalakshmi
Department Of ECE ,Kalasalingam University

,

***Abstract*—It is really a challenging task for the detection of malicious behavior using the traditional intrusion detection systems in Wireless Sensor Network (WSN), because of the scattered property of the Denial-of-Service attacks. Hence for the effective detection of such attacks, this paper proposes a hybrid clustering approach namely a Density-based Fuzzy Imperialist Competitive Clustering Algorithm (D-FICCA). The Imperialist clustering algorithm (ICA) is modified with the Density-based spatial clustering of applications with noise (DBSCAN) and fuzzy logic to achieve optimum clustering in WSN. The density-based clustering algorithm improves the ICA for forming clusters of arbitrary shapes and controlling noise. A fuzzy logic controller adjusts the fuzzy rules and adapts to the imperialistic competition, to prevent possible errors in the selection strategy of the worst imperialist action. The hybrid algorithm converges more quickly than ordinary evolution algorithms. The proposed algorithm achieves higher clustering quality and detection accuracy, when compared to the existing approaches, without requiring more resources.**

Index Terms*—Denial-of-Service Attacks, Density-based Fuzzy Imperialist Competitive Clustering Algorithm (D-FICCA), Density-based spatial clustering of applications with noise (DBSCAN), End-to-End Delay, Fuzzy Logic, Packet Delivery Ratio, Packet Overhead, Throughput and Wireless Sensor Network (WSN)

I. INTRODUCTION

Clustering techniques are part of numerous applications. One of the clustering techniques is a partitioning-based clustering algorithm such as K-means and Fuzzy C-mean clustering. For instance, the Fuzzy C-mean forms a cluster originated on the distance metrics to find an abnormal behavior in the wireless sensor network (WSN). However, partitioning clustering algorithms find only spherical clusters, while the clustering result is influenced by noise. The attack detection accuracy of the partitioning-based clustering algorithm is low. The density-based clustering methods overcomes the drawbacks of the partitioning algorithms. In the density-based clustering algorithms, the dense regions of the objects in the data space are considered as clusters, which are separated by low-density regions.

Density-based clustering method performs scanning for the highest density regions that are separated by the lowest density regions. It can find arbitrary shape clusters and handle noise, without requiring the information about the number of clusters. Density-based spatial clustering of applications with noise (DBSCAN) is the most effective density-based clustering method due to its accuracy. The DBSCAN technique performs effective discovery of clusters with different local density and identification of unknown intrusions, by analyzing the content of individual packets for the detection of malicious traffic.

Recently, ICA has developed as a novel and evolutionary algorithm for obtaining optimal solutions in numerous applications. The ICA implements the socio-political process of imperialism of governing many countries and exploiting their sources, by dominating the colonies by the rules. The most powerful countries are determined as imperialists and other countries are decided as the colonies. Next, there arises competition between the imperialists, to obtain more colonies. The best imperialist obtains more chances of possessing more colonies. An imperialist along with its colonies forms an empire.

This paper proposes a hybrid clustering approach namely a Density-based Fuzzy Imperialist Competitive Clustering Algorithm (D-FICCA). The Imperialist clustering algorithm is modified with theDensity-based spatial clustering of applications with noise (DBSCAN) and fuzzy logic to achieve optimum clustering in WSN. The density-based clustering algorithm improves the ICA for forming clusters of arbitrary shapes and controlling noise. A fuzzy logic controller adjusts the fuzzy rules and adapts to the imperialistic competition, to prevent possible errors in the selection strategy of the worst imperialist action. The main aim of the proposed approach is to realize the benefits of DBSCAN and fuzzy based clustering in Imperialist Competitive Algorithm (ICA), to improve the detection accuracy, clustering quality and false alarm rate.In the proposed approach, fuzzy logic controller (FLC) is applied for modifying the assimilation operator in the competition phases of ICA. Fuzzy min–max is utilized in the assimilation operator, for selecting the worst performing action to allot colonies to the imperialists. In addition, the DBSCAN approach is applied in the ICA clustering technique, to enhance the clustering quality by detecting the noise as low-density regions. However, the hybrid-based approach is adapted to the clustering techniques, for improving the system convergence and time complexity.

The rest of the paper is systematized as follows: Section II illustrates the conventional clustering techniques. Section III describes about the hybrid approach with density and fuzzy based clustering algorithm. Section IV illustrates the performance evaluation results of the proposed approach. Section V describes the conclusion of this paper.

II. RELATED WORK

Clustering is an effective approach to organize the network nodes into a hierarchical topology and aggregate the sending data to the base station, for improving the network lifetime. But it leads to the abrupt death of the nodes in the hot spots and there is disruption in the network services, due to heavy traffic load. For balancing the load over the nodes, the cluster head (CH) is rotated among all nodes and the size of the cluster is determined for the uniform distribution of energy consumption in the network. Naghibzadeh et al [1] proposed a clustering algorithm for choosing the nodes having maximum remaining energy in each region as the target CHs, and the best nodes among the chosen nodes are selected as the final CHs. The fuzzy logic is utilized for adjusting the cluster radius of the nodes of CH, based on the local information. Simulation results show that the proposed approach can improve the network lifetime, by reducing the hot spot problem.Liao et al [2] proposed a load-balanced clustering algorithm for the WSN, based on their distance and density distribution, by assuming that the residual energy of the nodes follows the random distribution. The simulated results indicate that the proposed algorithm can create more stable clustering structure and improve the network lifetime, since it is essentially different from the previous clustering algorithms.

Saranya and Padmavathi [3] suggested machine-learning based methods as an efficient technique in terms of detection accuracy, based on the observation results of various intrusion detection methods. A brief study on different intrusions along with the machine learning based anomaly detection methods are reviewed in this work. The study also classifies the machine learning algorithms into supervised, unsupervised and semi-supervised learning–based anomaly detection. The performances of the algorithms are compared and efficient methods are identified.Khan et al [4] described about all existing defensive schemes against the security attacks and the drawbacks of the schemes, to provide a better understanding of the attacks and current solution. The proposed schemes are classified according to their nature classified into Distributed and Centralized nature and defense measures classified into detection and prevention.Kosar et al [5] proposed and analyzed an approach to mitigate the hole problem. By using the proposed approach, the sensing quality is sustained above a given threshold and doubling of the network lifetime is possible. The simulation results clearly show the suitability of the approach for the WSN in the border surveillance tasks.

Jadidoleslamy[6] proposed a novel centralized clustering algorithm for large-scale WSNs, based on the distance between the sensor nodes, average distance between nodes. The proposed algorithm utilizes the deployment location coordinates of the sensor nodes in the WSN. The distance calculation is done by using the mathematical and statistical formula, to verify the purpose and capabilities of the clustering techniques, for the efficient organization and management of the WSN.H. Sedjelmaci and S. M. Senouci[7] proposed a lightweight Security Framework for the WSN, by integrating the benefits of cryptography and intrusion detection techniques to guarantee the communication privacy and detect the most dangerous attacks. To reduce the energy level of the nodes, the cryptography process is executed during detection of malicious node within the cluster. According to the simulation results, the false positive rate, attack detection rate, energy consumption level and average efficiency of the proposed framework are improved, when compared to other security frameworks.Farooqi et al [8] presented a novel intrusion detection framework for securing the WSN from the routing attacks. The online prevention mode of the proposed framework allows protection of the network from the abnormal nodes and offline detection mode finds the nodes that are compromised by the opponent during next time period. The simulation results demonstrate that the proposed scheme achieves high performance rate and intrusion detection rate, while reducing the false positive rate.

M.Kim et al [9] proposed an energy-efficient clustering algorithm that balances the remaining energy on the sensor nodes, for reducing the overall energy consumption level of the network and improving the lifetime of sensor networks. The clusters are updated dynamically and the load on the heavily loaded cluster heads is distributed among different nodes. Kumarage et al [10] proposed a robust and scalable mechanism for the accurate and efficient detection of malicious anomalies using the distributed in-network processing in a hierarchical framework. Unsupervised data partitioning is performed distributively adapting *fuzzy c-means* clustering in an incremental model. Non-parametric and non-probabilistic anomaly detection is performed through fuzzy membership evaluations and thresholds on observed inter-cluster distances. Robust thresholds are determined adaptively using second order statistical knowledge at each evaluation stage. The experiment results demonstrate that the proposed framework achieves high detection accuracy compared to the existing data clustering approaches with more than 96% less communication overheads opposed to a centralized approach.

Khamiss et al [11] proposed a density-aware clustering algorithm based on region density and utilized the fuzzy clustering technique for the cluster formation. The cluster head selection method depends on intra and inter-communication distances in addition to residual energy. The simulation results indicate that the algorithm can balance the energy load between nodes, reduce energy consumption and increase the stability period and life time of network compared to the traditional techniques.GhasemiGol et al [12] presented a new distributed anomaly detection approach and a foresight response strategy based on the support vector data description for WSN. The Linear Programming-based Fuzzy-Constraint support vector data description method is proposed for the accurate detection of outliers within a specific time period. A foresight response strategy is presented to resist various types of anomalies. The overall experiment results reveal the significance of the proposed method to achieve high detection accuracy on the real and artificial WSN datasets.

Kuang et al [13] proposed a novel energy-efficient clustering method based on the convergence degree chain, to decrease the energy consumption of sensor node and increase the stability of the WSN. The cluster head is selected using the convergence degree and residual energy and energy consumption of the member node is reduced using the cluster joining policy, for improving the stability of the network topology. The communication cost is reduced by rotating the cluster head according to the convergence degree chain created at the initial stage. Analysis and simulation results show that the proposed method can improve the cluster header characteristics and network lifetime. E. Darra and S. K. Katsikas[14] reviewed the types of malicious attacks against WSNs and relevant intrusion detection approaches, to identify the attack detection capabilities of the detection approaches.Mansouri et al [15] proposed an energy-conservation solution to detect compromised nodes in the

WSN, based on the hierarchical clustering technique.The control nodes that analyze the traffic inside a cluster is selected and warning is sent to the cluster head, during the detection of abnormal behavior. Better energy balance is achieved, while maintaining good detection rate, based on the distance between the sensor nodes, packet transmission delay and network throughput. To overcome the limitations of the existing techniques, this paper proposes a hybrid approach based on density and fuzzy based clustering algorithm for the efficient detection of intrusions in the WSN.

III. Hybrid Approach Based On Density And Fuzzy Based Clustering Algorithm

The DBSCAN can effectively discover clusters with different local density and identify unknownintrusions, by analyzing the individual packetcontentsfor malicious traffic. In this paper, theDBSCAN algorithm performs data clustering, for identifying and reporting the abnormal information. The DBSCAN approach is able to form clusters of arbitrary shape and effectively deal with the noise. The distribution zone with normal values forms a high-density distribution zone, while the distribution zone with abnormal values forms a low-density distribution zone. Fig.1 shows the workflow diagram of the proposed hybrid approach.

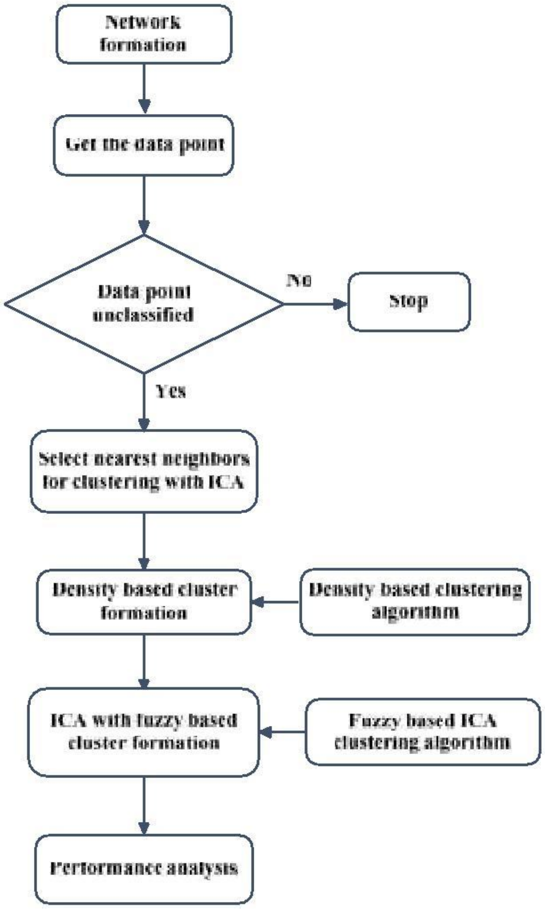
Network formation
Get the data point
Data point unclassified
No
Stop
Yes
Select nearest neighbors for clustering with ICA
Density based cluster formation
Density based clustering algorithm
ICA with fuzzy based cluster formation
Fuzzy based ICA clustering algorithm
Performance analysis

Fig.1 Workflow diagram of proposed hybrid approach

DBSCAN algorithm

```
Input: a data set S
Output: arbitrary shape clusters
for each data point d in S do
  if d is not marked as 'seen' then
    mark p as 'seen'
    Find $H_n(d,S)$ /*find n neighborhood of data point d */
    if $|H_n(d,S)|$ <MinDps then
      mark data point cluster id as noise
    else
      clustered=clustered + 1
    end if
    for all $m \in H_n(d,S)$ do
      mark data point m as 'seen'
      find $H_n(m,S)$
      if $|H_n(m,S)| > MinDps$ then
        give a clusterid to data point m
      end if
    end for
  end if
end for
```

The input parameter S is a data set, MinDps is the minimum number of data points in a predefine radius (n). The output contains high and low-density regions. The high-density regions form clusters with arbitrary shapes, while the low density areas indicate noisepresent in the dataset. Thus, DBSCAN performs the following steps for each data point (d) in the data set:

Step 1: Start with an arbitrary starting point in dataset(S) that has not been visited.

Step 2: Calculate the distance of each data point (m) thatexists in (n) threshold neighborhood of the data point(d). The aim is to find the number of data points present in the neighborhood radius (H_n (d)).

$$H_n(d) = \{m \in S | dist(d, m) \le n\} \tag{1}$$

Step 3: Compare the number of neighborhood radius H_n (d) with MinDps, to clarify the status of the data points. In other words, if H_n (d) isless than MinPts, it is considered as a noise, otherwise,it is assigned to a new cluster.

$$|H_n(d)| \ge Mi\ nDps \tag{2}$$

Step 4: If data point (d) is assigned to be part of thecluster, for all n neighborhoods of (d), repeat the procedure from the Step 2, until all points in the cluster aredetermined.

Step 5: A new unvisited point is retrieved and processed, to discovera new cluster ornoise.

Step 6: This process continues until all points aremarked as having been visited.

The general clustering problems such as sensitivity to initialization, specification of number of clusters, or detection of particular cluster shapes is avoided by using the density-based clustering technique for intrusion detection. The main idea of intrusion detection based on DBSCAN is that most of the data is normal, and normal data are gathered together into a high-density cluster, while the invasion data is vary few, and very different with normal data. Therefore, the invasion data would be a low-density cluster. As a result, the largest cluster of data is normal network data, while the small cluster of data that is considered to be the invasion data.

The fuzzy set adapts to the action selectionstrategy to adjust its rules in order to avoid possible faultsof the worst imperialist selection.The low, medium and high fuzzy sets identified in the current Buffer size discriminate the cases, when Bs is less than 3 k, which has been defined as the length of packet received from source during specified time window. The output linguistic variable represents the Detect Confidence (DC) of the proposed system in the presence of abnormal behavior. To illustrate, if the confidence value is higher than 80, then the system is more than 80% certain that there is an abnormal entity, if the detection confidence is smaller than 40, it is more likely that there is no abnormality. However, input and output variables give us a notion of the change in the traffic connection.

A. Density-Based Fuzzy Imperialist CompetitiveClustering Algorithm (D-FICCA)

The ICA clustering-based intrusion detection strategy is primarily a combination of the density methodand fuzzy logic controller. The modified ICA-based detection system operates to sense DDoS attacks, where the sinknode selects the optimal strategy to detectan immediateattack and reports it to the base station. Irrespective of carrying the attacks on a regular or irregular basis, the sink node in terms of IDS can adjust its optimization density-based clustering parameters throughfuzzy rules to identify future attacks. In our scheme, theproposed D-FICCA steps are described below:

Step 1: Generate an initial population

An initial population of input sensor data is generatedby DBSCAN initialization as follows:

$$I=\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{N_{initial}} \end{bmatrix} \quad (3)$$

$$y_j=colony_j \left[y_j^1, y_j^2, \ldots\ldots, y_j^D \right] 1<j<n \quad (4)$$

$$C_k=Cluster_k\left[c_1, c_2, \ldots., c_p \right] 1<k<p$$

I is the population and$y_j$is one of the colonies. $N_{initial}$is thenumber of the population and D is the number ofdimensions of each colony. p is the number of arbitraryshape clusters (C_p); and $N_{new}$is calculated based on thededuction of $N_{initial}$from the number of noise (N_{noise}).

Step 2: Calculate cost function value

The cost function is evaluated for each colony asfollows: For each data point (d), the following distanceis calculated

cost (d): the average distance between (d) and all otherobjects in its colony

$$N_{new}=N_{initial}-N_{noise}$$

$$cost(d)=\sum_{d'\in C_i, d\neq d'} distance(d,$$

Step 3: Sort the initial population according to objectivefunction values.The initial population ascends based on the value of itsobjective function.

Step 4: Select the imperialist states.

Colonies with the maximum objective function are theselected imperialist states and the remaining onesbecome these imprialists' countries.

Step 5: Divide colonies among imperialists.

For proportionally dividing the colonies among the imperialists, the normalized cost of an imperialist is defined by the cost function value

$$Cost_n = \mathrm{cost}_n - \max_i \{\mathrm{cost}_i\} \quad (8)$$

where $cost_n$is the cost of the nth imperialist and $Cost_n$isits normalized cost. Having the normalized cost of allimperialists, the normalized power of each imperialistis defined as

$$P_{norm} = \left| \frac{Cost_n}{\sum_{i=1}^{N_{imp}} Cost_i} \right| \quad (9)$$

The initial colonies are divided among empires in orderof their power. The initial number of colonies of the nth empire is given as

$$N \cdot Cost_n = round\,\{P_n \cdot N_{col}\} \quad (10)$$

Where $N_{col}$is the total number of initial colonies. $N \cdot Cost_n$ is the initial number of colonies of thenth empire. For dividing the colonies, initial number of the coloniesare randomly chosen and given to thenth imperialist.These coloniesformthe Nth empire, along with the Nth imperialist.

Step 6: Perform the DBSCAN algorithm for each empire.

Step 7: Move colonies toward their imperialist statesbased on fuzzy min–max.

Step 8: Check the cost of all colonies in each empire. Step 9: Run imperialistic competition.

Step 10: Remove the weakest empire.

Step 11: Inspect the number of empires; if it is 1, thengo to Step 7.

$$d')\,/\,|C_i|-1$$

IV. Performance Results

This section describes about the comparison results of the performance metrics of the proposed Density-based Fuzzy Imperialist Competitive Clustering Algorithm(D-FICCA) approach and existing Partitioning-based clustering scheme (PCS). The density-based clustering algorithm improves the ICA for forming clusters of arbitrary shapes and controlling noise. A fuzzy logic controller adjusts the fuzzy rules and adapts to the imperialistic competition, to prevent possible errors in the selection strategy of the worst imperialist action.

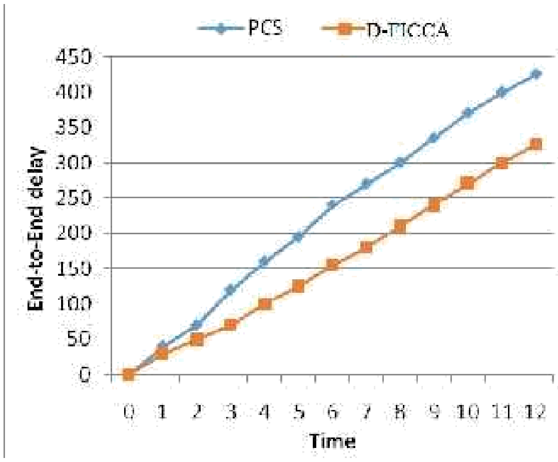

Fig.2 End-to-End Delay

Fig.2 shows the graph illustrating the end-to-end delay of the proposed D-FICCA approach and existing PCS. End-to-End delay is the time taken for a packet to be transmitted from the source to the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. From the comparison graph, the end-to-end delay of the proposed approach is lower than the existing technique.

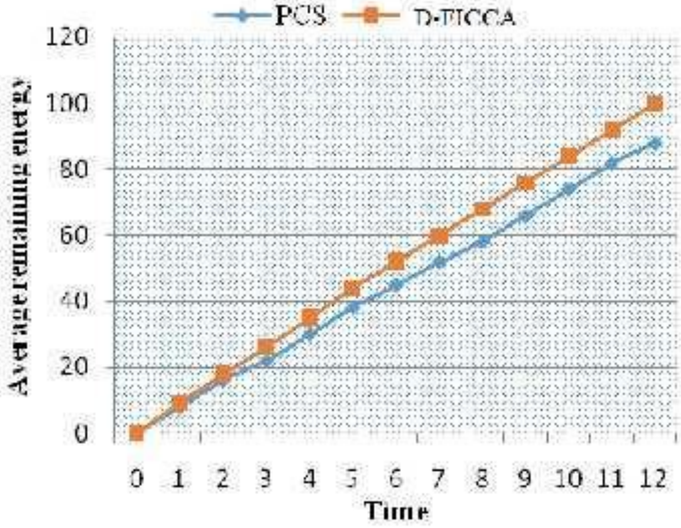

Fig.3 Average Remaining Energy

Fig.3 shows the graph illustrating the average remaining energy of the proposed D-FICCA approach and existing PCS. Average remaining energy is defined as the average amount of residual energy in the sensor nodes. From the comparison graph, the average remaining energy of the proposed approach is greater than the existing technique.

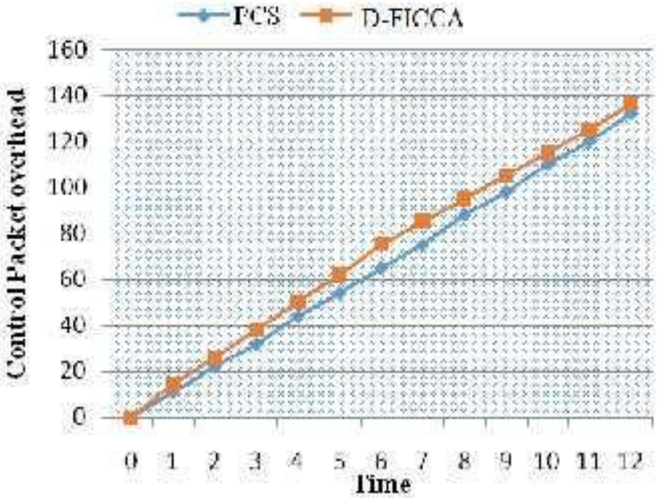

Fig.4 Control packet overhead

Fig.4 shows the graph illustrating the control packet overhead of the proposed D-FICCA approach and existing PCS. The control packet overhead is the time taken to transmit data on the network. From the comparison graph, the control packet overhead of the proposed approach is higher than the existing technique.

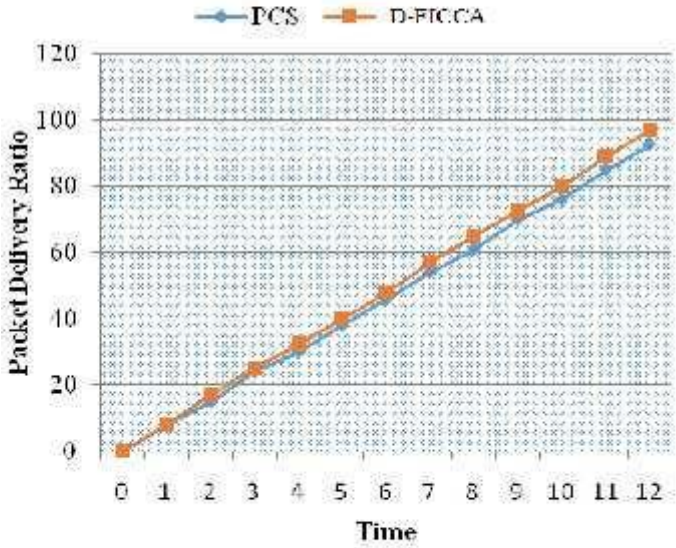

Fig.5 Packet delivery ratio

Fig.5 shows the graph illustrating the packet delivery ratio of the proposed D-FICCA approach and existing PCS. Packet delivery ratio is the ratio of the number of delivered data packet to the destination.From the comparison graph, the packet delivery ratio of the proposed approach is higher than the existing technique.

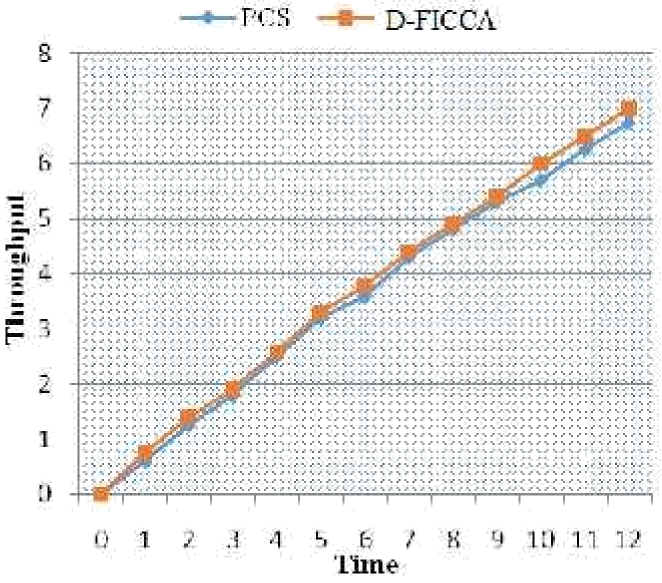

Fig.6 Throughput

Fig.6 shows the graph illustrating the throughput of the proposed D-FICCA approach and existing PCS.The throughput is the average rate of successful data delivery over the channel and it is measured in data packets per time slot.From the comparison graph, the throughput of the proposed approach is higher than the existing technique.

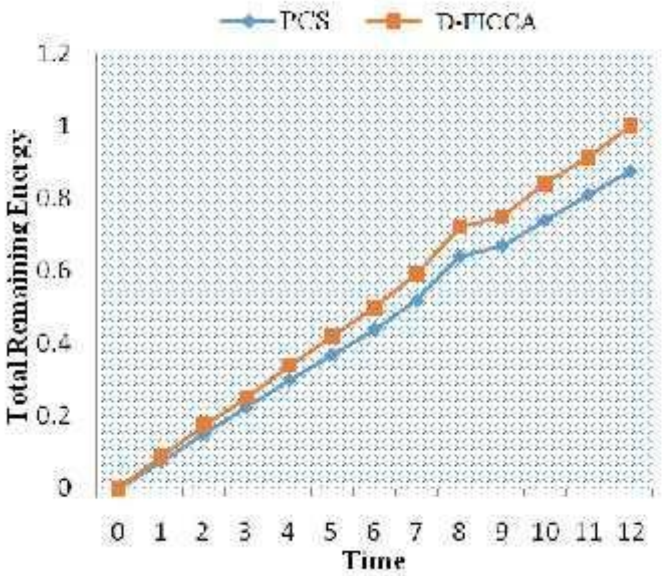

Fig.7 Total Remaining Energy

Fig.7 shows the graph illustrating the total remaining energy of the proposed D-FICCA approach and existing PCS. The total remaining energy is the total amount of residual energy in the network. From the comparison graph, the total remaining energy of the proposed approach is higher than the existing technique. Hence the proposed approach is more efficient than the existing technique.The hybrid algorithm converges more quickly than ordinary evolution algorithms.

V. Conclusion

In this paper, a hybrid clustering approach namely a Density-based Fuzzy Imperialist Competitive Clustering Algorithm (D-FICCA) is proposed. The Imperialist clustering algorithm is modified with theDensity-based spatial clustering of applications with noise (DBSCAN) and fuzzy logic to achieve optimum clustering in WSN. The main aim of the proposed approach is to realize the benefits of DBSCAN and fuzzy based clustering in Imperialist Competitive Algorithm (ICA), to improve the detection accuracy, clustering quality and false alarm rate.The density-based clustering algorithm improves the ICA for forming clusters of arbitrary shapes and controlling noise. A fuzzy logic controller adjusts the fuzzy rules and adapts to the imperialistic competition, to prevent possible errors in the selection strategy of the worst imperialist action.The hybrid algorithm converges more quickly than ordinary evolution algorithms. The experimental results indicate that the proposed hybrid approach is considered as a feasible and an efficient heuristic method for intrusion detection.The proposed algorithm achieves improved detection accuracy and clustering quality, when compared to the existing approaches, without requiring more resources.

VI. ACKNOWLEDGEMENT

we thank the department of Electronics and Communication Engineering of kalasalingam University,(kalasalingam Academy of Research and Education),Tamilnadu,India for permitting to use the computational facilities available in centre for research in Signal Processing and VLSI design which was setup with the support of the Department of Science and Technology(DST),Newdelhi under FIST program in 2013.

REFERENCES

[1] M. Naghibzadeh, H. Taheri, and P. Neamatollahi, "Fuzzy-based clustering solution for hot spot problem in wireless sensor networks," in *7th International Symposium on Telecommunications (IST), 2014*, 2014, pp. 729-734.

[2] Y. Liao, H. Qi, and W. Li, "Load-balanced clustering algorithm with distributed self-organization for wireless sensor networks," *IEEE Sensors Journal,*, vol. 13, pp. 1498-1506, 2013.

[3] J. Saranya and G. Padmavathi, "A Brief Study on Different Intrusions and Machine Learning-based Anomaly Detection Methods in Wireless Sensor Networks," *Int. J. Advanced Networking and Applications,* vol. 6, pp. 2414-2421, 2015.

[4] W. Z. Khan, Y. Xiang, M. Y. Aalsalem, and Q. Arshad, "The selective forwarding attack in sensor networks: Detections and countermeasures," *International Journal of Wireless and Microwave Technologies (IJWMT),* vol. 2, p. 33, 2012.

[5] R. Kosar, I. Bojaxhiu, E. Onur, and C. Ersoy, "Lifetime extension for surveillance wireless sensor networks with intelligent redeployment," *Journal of network and computer applications,* vol. 34, pp. 1784-1793, 2011.

[6] H. Jadidoleslamy, "A Novel Clustering Algorithm for Homogenous and Large-Scale Wireless Sensor Networks: Based on Sensor Nodes Deployment Location Coordinates," *IJCSNS,* vol. 14, p. 97, 2014.

[7] H. Sedjelmaci and S. M. Senouci, "A lightweight hybrid security framework for wireless sensor networks," in *IEEE International Conference on Communications (ICC), 2014*, 2014, pp. 3636-3641.

[8] A. H. Farooqi, F. A. Khan, J. Wang, and S. Lee, "A novel intrusion detection framework for wireless sensor networks," *Personal and ubiquitous computing,* vol. 17, pp. 907-919, 2013.

[9] M. Kim, S. Kim, J. Seo, K. Choi, and S. Han, "CAPNet: An Enhanced Load Balancing Clustering Algorithm for Prolonging Network Lifetime in WSNs," *International Journal of Distributed Sensor Networks,* vol. 2014, 2014.

[10] H. Kumarage, I. Khalil, Z. Tari, and A. Zomaya, "Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling," *Journal of Parallel and Distributed Computing,* vol. 73, pp. 790-806, 2013.

[11] A. Khamiss, S. Chai, B. Zhang, J. Luan, and Q. Li, "An energy-efficient and density-aware clustering for WSNs," in *33rd Chinese Control Conference (CCC), 2014*, 2014, pp. 377-382.

[12] M. GhasemiGol, A. Ghaemi-Bafghi, M. H. Yaghmaee-Moghaddam, and H. Sadoghi-Yazdi, "Anomaly detection and foresight response strategy for wireless sensor networks," *Wireless Networks,* pp. 1-18, 2015.

[13] X. H. Kuang, L. Liu, Q. Liu, and X. Li, "A clustering approach based on convergence degree chain for wireless sensor networks," *Security and Communication Networks,* 2014.

[14] E. Darra and S. K. Katsikas, "Attack detection capabilities of intrusion detection systems for Wireless Sensor Networks," in *Fourth International Conference on Information, Intelligence, Systems and Applications (IISA), 2013* 2013, pp. 1-7.

[15] D. Mansouri, L. Mokdad, J. Ben-Othman, and M. Ioualalen, "Detecting DoS attacks in WSN based on clustering technique," in *IEEE Wireless Communications and Networking Conference (WCNC), 2013*, 2013, pp. 2214-2219.