Bio-Inspired Based Distributed Monitoring Technique for Clustering and Optimization in Wireless Sensor Networks

M.S.Vinmathi, M.S.Josephine, V.Jeyabalaraja

Abstract: ***Security threats are vulnerable in recent times. Kaspersky intelligence report confirms that clustering and attacks makes crucial impact on the network as compared with other security attacks in wireless based environment .The current work focus on clustering of nodes in WSNs. Cat swarm optimization (CSO) algorithm is one of the bio-inspired algorithm and implemented for optimization of nodes to find a better route to transmit data packets in WSN. Also the work focuses on the presence of Distributed Monitoring Approach to evaluate the seek or hunt mode and tracing mode nodes for better improvement in clustering the network. The network recital parameters such as ratio of delivery of data packets, and transmission capacity usage are analyzed to detect network flow in WSN. Reviews have been performed with the analysis of network performance with some of the existing techniques.***

Keywords: Bio-inspired algorithm, Clustering,Distributed Monitoring Approach, network parameters, Cat swarm optimization, wireless sensor network

I. INTRODUCTION

WSN comprises of main components namely, nodes or users, gateways, and internet as shown in Figure 1. The spatially dispersed estimation nodes interface with sensors to monitor the nodes present inside the network. It does some of the functions like detecting, information handling, and communicating capabilities. The base station controls the operation of the network and takes care of analyzing and storing the gathered information[2].

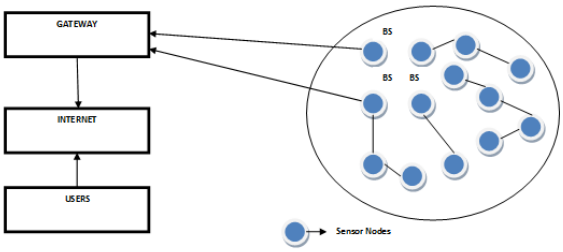

Figure 1 Architecture of Wireless Sensor Network

The topology of WSN has to be known for network building environment where nodes are normally categorized in one of three kinds of network topologies. In a Star Topology, each node links through a gateway. In a Cluster Tree Network, each one of the nodes connects to a higher level node in the network and then, communicates to the interface which is named as gateway[1]. In order to attain reliability in increasable manner, mesh network attribute nodes connect to various other nodes in network and transmit information or data by choosing efficient and consistent route available. Resourceful services provided by Wireless Sensor Networks are higher as compared with the stationary sensor networks. The advantage of MWSN includes improved coverage, enhanced energy efficiency, greater channel competence etc.In addition, numerous authors have just centered on the investigation of execution parameters on portable WSNs where these frameworks include a get-together of sensor centers that can be continued forward their own and can likewise be cooperated with its inclusion zones. In this scenario, the mobile nodes have the capacity to compute sense and interact with network. (Zhang et al. 2003, Shiqun Li et al.2007, Khara 2017).Apparently , the most energy exploitation attack in Wireless Sensor Networks is denial of service attacks[18][19] in which an invader depletes the energy of sensor nodes by means of influencing the unaffected nodes to get up, even though there is no movement to hold or to control the environment. Along with this effect, energy of sensor nodes is reduced phenomenally and sensor nodes also move towards untargeted locations. Hence, the lifetime of a WSN gets reduced by impacting the signals of the receiving end by depleting the rundown battery in small period of time. Here, energy is inefficiently used due to conflict, over-listening, overhead occurrence in control packet and over-emittion by the attacker (Shital Patil et al.2016).

Another energy utilization issue is overhead in control packet, where the prescribed number of request-to-send and clear-to-send packets is sent for information transmission and remaining nodes are alerted for controlling the packets to consume the battery life. This energy utilization attacks are performed by means of DL (Data Link) layer.

WSNs guarantee energizing new applications in the near future. For example, consistent network, ubiquitous on-demand, analysing energy and deployable message are needed for initial responders and military purposes. Presently, these systems perform production line execution and ecological conditions to give some example applications. Because of their associations, these systems are especially vulnerable against Denial of Service (DoS) attacks[18][19] .Huge investigations have been done to improve security, and there are three essential commitments

Revised Manuscript Received on January 2020

***** Correspondence Author

M.S.Vinmathi , Research Scholar ,Dr. M.G.R. Educational and Research Institute, Department of CSE, Periyar E.V.R. High Road, Viswasa Nagar, Maduravoyal, Chennai, Tamil Nadu 600095,

Dr.M.SJosephine , Addl. HOD &Prof, Department of Computer Applications ,Dr. M.G.R. Educational and Research Institute , Periyar E.V.R. High Road, Viswasa Nagar, Maduravoyal, Chennai, Tamil Nadu 600095,

Dr.V.Jeyabalaraja, Professor, CSE department ,Vellammal Engineering College, Velammal Nagar, Ambattur-Red Hills Road,Chennai - 600 066

(Rodrigo Roman et al. 2006, Pooja Sharma et al. 2010, Md. Safiqul Islam et al. 2010). In the first place, the liabilities of existing protocols are completely assessed to analyze the routing layer battery depletion attacks. Secondly, it is observed that safety efforts to keep these exhaustion attacks are orthogonal to ensure the existing secure directing conventions, and its infrastructure.

II. LITERATURE REVIEW

Table 1 Survey

Name of the Algorithm		Author	Control Parameters	Based on	Areas of Application	Advantages	Disadvantages	Operator
Genetic Algorithm	**GA**	John Holland (1960s & 1970s)	Population size(chromosomes), Crossover, Mutation, Selection	Evolutionary ideas of natural selection & genetics	Data mining, classification problem.	Inherently parallel, at all times an answer; at all times gets better with period, Likelihoods of getting optimal solutions are more.	Population measured for moderate Evolution (normally 20-30,50-100), hybrid rate ought to be 80% - 95%, pace of transformation ought to be low 0.5% - 1% (very much considered best), The technique off choice ought to be reasonable, engraving of wellness capacity ought to be exact rate.	Crossover, Mutation & Selection
Particle swarm Optimization	**PSO**	Kennedy and Eberhart (1995)	Population size (particles), Velocity, Location	Is a population based technique. Witnessing social behaviour among animal herding, fishes, birds & even humans.	Telecommunication, Datamining, Combinatorial problems, Signal processing, power systems.	PSO depends on the insight it tends to be applied to both Research for Scientific results and uses in engineering stream, Calculation in PSO is straightforward.	The strategy easily experiences the incomplete Optimism, The strategy can't exercise the issues of dissipating and streamlining.	Mutation & Selection

Ant Colony Optimization	**ACO**	Dorgio& Di Caro (1999)	Population size (ants), Pheromone evaporation rate, pheromone reward factor	Incisive for ideal way in diagram dependent on conduct of ants looking for a way between their state and wellspring of nourishment.	Combinatorial optimization problems	Inherent parallelism, Positive Feedback represents quick revelation of good arrangements, Skilled for Traveling Salesman Problem and practically identical issues, can be used in incredible applications (adjusts to changes, for example, new separations, and so forth)	Hypothetical examination is hard, Classifications of irregular choices, Probability dispersal deviations by repetition, Time to conjunction indeterminate	Mutation & Selection
Artificial Bee Colony Algorithm	**ABC**	DervisKaraboga (2005)	Population size(swarm), limit dimension	Advancement calculation grounded on shrewd scrounging conduct of bee with honey and swarm.	Benchmarking Optimization, Scheduling, Bioinformatics, Clustering & mining, Image Processing and in Engineering design & Applications.	Simplicity, flexibility, robustness, Capability to reconnoiter local solutions, Capability to knob objective cost.	Slow down when used in sequential dealing out, High number of objective function estimations, the population of solution rises computational costs.	Mutation & Selection
Cuckoo Search	**CS**	Xin-She Yang (2009)	Population size(host nest), cuckoo, fitness	Necessitate brood parasitism of cuckoo.	Applied in various areas of optimization and computational intelligence, Engineering design problems, very effective for solving non- linear problems. wireless sensor network	Global search customs Levy flights. Combined with both local and search abilities guarantee global convergence, pacts with multi criteria optimization problem, easy to implement, simplicity.	Only single parameter is used equated to Harmony search and Particle swarm optimization.	Mutation & Selection

Firefly Algorithm	**FA**	Xin-She Yang (2008)	Population size(flies), Light intensity, Light absorption coefficient	Flashing behavior of firefly.	Engineering Design problems, efficiently solve NP-hard Scheduling problems, Classification and clustering problems.	Automatic subdivision, and ability to agreement with multimodality.	High probability of existence trapped in local optima as they are local search algorithms.	Mutation
Bat Algorithm	**BA**	Xin-She Yang (2010)	Position, velocity, frequency, loudness, pulse rate	Echolocation behavior of micro bat	Optimization, Fuzzy logic, Classification, Image processing, Scheduling and Data mining.	It is easy to implement, accurate, efficient, simplicity and flexibility.	Converge very quickly at the initial stage and the converge rate slow down, no mathematical analysis to link parameters with convergence rate, Accuracy may be inadequate if the function evaluations are not high	Mutation & Selection

III. CAT SWARM OPTIMIZATION (CSO)

CSO optimization is an enduring approach of enhancement that can emulate the cat's conduct [21]. In the most recent years, CSO have been applied to locate the ideal answer for certain applications [22][23]. The biological name of cat used in this section is felis catus.The mode looking for is applied during the resting time frame for cats, however they are observant; while the drawing attention mode is relating to the neighborhood search strategy to acquire the ideal arrangement elucidation of the present issue.

3.3.1. Search for Hunt method

The quest for hunt conduct is predominantly contained four fundamental components; scan for chase pool of memory (SHMP), which characterizes the log size of looking for memory; scan for chase scope of the selected length (SRl), which characterizes the minimal and maximal estimations of the quest for chase run; counts of measurement to change (CDC), which speaks to the measurements number in the looking for method which is not changed; self-position thought (SPC), which is a Boolean-esteemed variable. At that point, we can utilize a term called blend proportion (MR) as a small amount of the populace that has a little worth to guarantee that felines as a rule invest the greater part of their energy on account of watching and resting). The way toward seeking for is quickly portrayed as pursued below.

1. The MR can be chosen haphazardly as a small amount of populace np for looking for cats.
2. SHMP duplicates are identified upon nth cat.
3. The situation of all duplicates as give or take must be updated for SRD division of the current position esteem haphazardly .Then supplant their values afterward.
4. Estimations of wellness of all duplicates can be assessed.
5. The determined duplicates of likelihood of all the competitors are analyzed and afterward pick the apt one to put it at the situation of nth looking for feline.
6. Rehash procedure number 2 to include all the other seeking nature for felis catus.

3.3.2. The Tracing method

The tracing method is focused as strategy of investigation in the advancement procedure. Here, the Felis catus can follow the expected objective with elevated vitality. The speedy pursue assigned to feline will be displayed and a scientific structure is shown by rearranging the location. In this manner, characterization of the location and speed assigned to nth cat in the d-measure mental area by Equation 1 where limits used as $1 \le a \le d$

$$T_{i=}T_{i1}, T_{i2}, T_{i3} \dots, T_{id} \quad (1)$$

The accurate position for route optimization is depicted by the following Equation (2)

$$C_{gpb} = C_{gpb1}, C_{gpb2}, \dots, C_{gpbd} \quad (2)$$

In this way, the proposed advances that are associated with the following mode are displayed beneath

(i) Use the accompanying scientific structure as appeared in Equation (3) to figure the new speed of the nth cat:

$$V_e = inw.V_e + ac.m(C_{gpbd} - X_e) \quad (3)$$

where inw depicts to the dormancy load, ac stands for speeding up steady increase of velocity constant, and m is a numerical value to facilitate haphazardly to chose upon interim [0, 1]. At that point, the global best C_{gpb} can be haphazardly chosen from the outer chronicle.

(ii) Evaluate the refreshed situation of a nth cat by utilizing the accompanying Equation (4):

$$X_{id} = X_{id} + V_e \quad (4)$$

(iii) The comparing limit esteem is chosen to be another measurement.
(iv) Weigh up the wellness of each Felis catus. T_e
(v) In conclusion, refresh their substance of document by means of the situation of felis catus.
Table 2 show about the algorithm used in CDA approach which is endorsed from CSO algorithm

3.3.3 Distributed Monitoring Approach for Clustering of Nodes

Table 2 Algorithm of Distributed Monitoring Approach

// Network connection **N** has many 100 nodes(n) which in turn has route requests and route replies.
//Malicious behavior is extracted from cumulative requests and replies.
//INPUT: Data packets from, Source **S**, Destination **D**, Set Cluster nodes N
//OUTPUT: Finding routes **I** by computing PDR over t time rounds
//METHOD: shared monitoring
PROCEDURE:
For network scenario $\mathbf{N}_i$
n=100;
Initialize data communication for S&D ε N
Assign S, D.
1. **Begin** (**at t = 0**)
2. **If** packets forwarded $\mathbf{S_p}$=Acknowledged packets $\mathbf{R_p}$
3. Normal flow of data
Else
4. **If** packets forwarded $\mathbf{S_p}$> Acknowledged packets **Rp then**
5. **CDA** monitors seeking mode nodes and tracing mode nodes ∀ N
6. Compute **PDR** and Traffic flow **F** for t rounds in profiling and detection phase
End if
End if
If seeking mode $\mathbf{S_e}$ with in threshold limit T_e
7. Check for malicious or abnormal activity or Intruders
8. Repeat the process for t rounds for clustering
9. **End if**
End

3.3.4 Implemantation Scenario

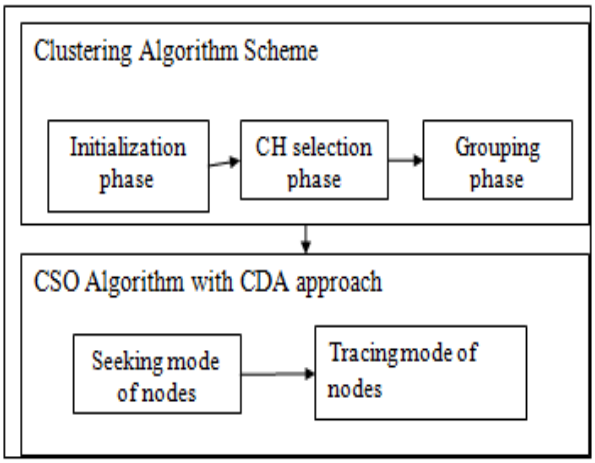

Figure 3 CDA Based Model

Figure 3 incorporates development of group and choice of Cluster head (CH). CH is chosen on rotational or grouping premise. There are two plans in group development the first is seeking mode of nodes evaluation conspire. This conspire figures the heaviness of the nodes with the goal that the rotational bunch adjusts the heap in the system. The tracing mode of nodes subsequent plan is defensive component plot. This plan ascertains the most extreme separation between the nodes and the base station. Vitality or energy executives are planned dependent on the remaining vitality and averting superfluous transmissions.

IV. SIMULATION RESULTS

NS-2 reproduction test framework is used for the utilization of the proposed arrangement. The AODV show participated in NS-2 was used as the base show. TCP was used as the substitute show. Movement sources used are Constant-Bit-Rate (CBR) and the network area course of action is 800 x 800m with 100 nodes.

4.1 Metrics [24]:

1. Typical number of packet of data received (nrp): Entirety of quantities of all the moderate (nodes among source and goal nodes) abiding log of data forwarded by all the starting place hubs (rps) divided by number of got bundles at all the aspiration nodes (rpd) as shown in equation 1.

$$\Sigma nrp=\Sigma rps/\Sigma rpd \quad (1)$$

2. Typical number of packet of data forwarded (nfp): Whole of quantities of all the moderate (nodes among source and goal hubs) sending log of data packets forwarded via every starting place nodes (frps) with number of acknowledged bundle of log of data packets by the side of every aspiration nodes (rpd) as shown in equation 2.

$$\Sigma nfp=\Sigma frps/\Sigma rpd \quad (2)$$

3. Number of packet of data plunged (dpd): The quantity of information dropped at some random sensor node. Moreover, the significant factor within these scenario, the capacity of plunged bundle of data expands, the throughput (tr) would reduce as shown in equation 3.

$$\Sigma dpd=(\Sigma \pm tr) \quad (3)$$

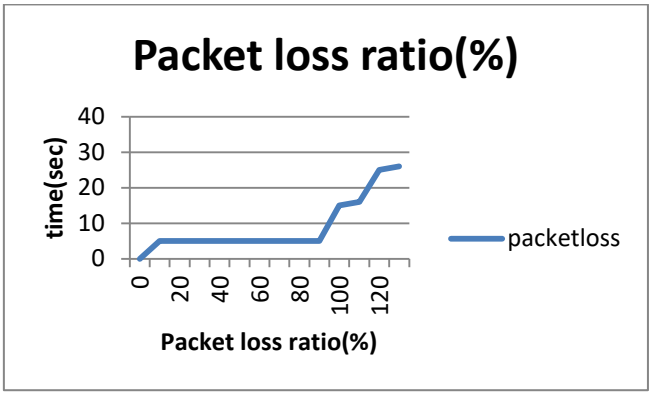

Figure 4 Loss Ratio of Data Packets

In Figure 4, experiments of parcel of packets misfortune proportion show greater misfortune proportion from starting intensity to one hundred percentages upon the known time interims. This is because of the unfriendly impact of malicious behavior pretend to be as the starting place of aggressive attack.

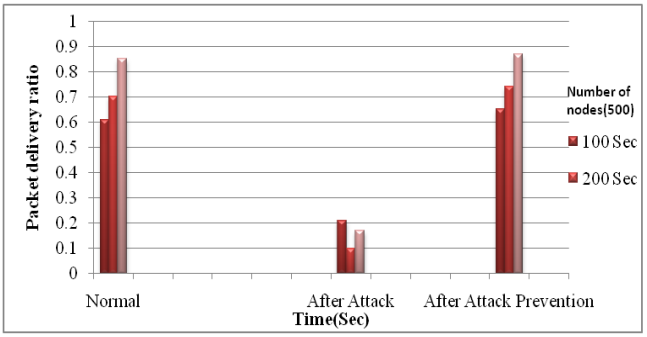

Figure 5 Packet Delivery Ratio of 100 nodes

Figure 5 describes the three-simulation scenario for analyzing the delivery ratio of received data packets. The result showed with the intention of the ratio is accomplished with minimal packet loss before attack prevention, compared with after attack.

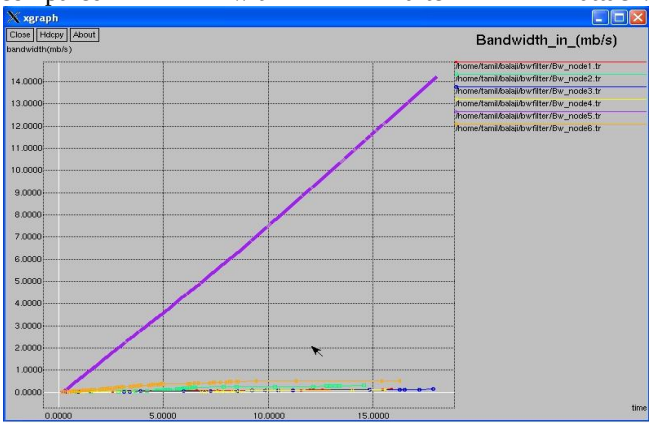

Figure 6 Transmission capacity for sample 6 nodes.

The test cases of transmission capacity with respect to traffic flow *t* rounds is compared with each six nodes (as sample) as shown in Figure 6. In a modularity approach, tests are performed for rest of the nodes.

V. CONCLUSION

In this work, clustering of nodes in wireless sensor network is proposed which is deployed by Coordinated Derelict Approach by assortment of pertinent data. The optimization is deployed by CSO algorithm. Here transmission limit usage have been learned for all nodes and as a final point the system or node dissipate extra transfer speed depicted for the cause of network traffic. We led the assessment in a recreation situation for basic systems which has 100 nodes. In future, this work can also be implemented for cognitive WSN.

REFERENCES

1. Zhang, Y, Lee, W & Huang, YA 2003, 'Intrusion detection techniques for mobile wireless networks', Wireless Networks, vol. 9, no. 5, pp. 545-556.
2. Shiqun Li, Tieyan Li, Xinkai Wang, Jianying Zhou &Kefei Chen 2007, 'Efficient Link Layer Security Scheme for Wireless Sensor Networks', Journal of Information And Computational Science, vol. 4, no. 2, pp. 553-567.
3. Khara, S 2017, 'A Review on Security Issues in Wireless Sensor Network', International Journal of Sensor Networks and Data Communications, vol. 1, pp. 1-3.
4. ShitalPatil & SangitaChaudhari 2016, 'DoS attack prevention technique in Wireless Sensor Networks', Procedia Computer Science, vol. 79, pp. 715-721.
5. Pooja Sharma &PawanBhadana 2010, 'An Effective Approach for Providing Anonymity in Wireless sensor Network: Detecting Attacks and Security Measures', International Journal on Computer Science and Engineering, vol. 02, no. 05, pp. 1830-1835.
6. Mohammad Saiful Islam Mamun 2010, 'Hierarchical design based intrusion detection system for wireless ad hoc sensor network.' International Journal of Network Security & Its Applications, vol. 2, no. 3, pp. 102-117.
7. Rodrigo Roman, Jianying Zhou & Javier Lopez 2006, 'Applying Intrusion Detection Systems to Wireless Sensor Networks', 3rd IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA. pp. 640-644.
8. Hong-Chi Shih, Jiun-Huei Ho, Bin-Yih Liao &Jeng-Shyang Pan 2013, 'Fault Node Recovery Algorithm for a Wireless Sensor Network', IEEE Sensors Journal, vol. 13, no. 7, pp. 2683-2689.
9. Tapalina Bhattasali, Rituparna Chaki& Sugata Sanyal 2012, 'Sleep Deprivation Attack Detection in Wireless Sensor Network', International Journal of Computer Applications, vol. 40, no. 15, pp. 19-25.
10. Bhorkar, AA, Naghshvar, M &Javidi, T 2012, 'An Adaptive Opportunistic Routing Scheme for Wireless Ad-hoc Networks', IEEE / ACM Transactions on Networking, vol. 20, no. 1, pp. 243-256.
11. Glenn Robertson &SrihariNelakuditi 2012, 'Handling Multiple Failures in IP Networks through Localized On-Demand Link State Routing', IEEE Transactions on Network and Service Management, vol. 9, no. 3, pp. 293-305.
12. Shui Yu, Wanlei Zhou, Robin Doss &WeijiaJia 2011, 'Traceback of DDoS Attacks Using Entropy Variations', IEEE Transactions On Parallel And Distributed Systems, vol. 22, no. 3, pp. 412-425.
13. Rung-Ching Chen, Chia-Fen Hsieh & Yung-Fa Huang 2010 , 'An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Networks', Journal Of Networks, vol. 5, no. 3, pp. 335-342.
14. Rizwan Khan &Vatsa, AK 2011, 'Detection and Control of DDOS Attacks over Reputation and Score Based MANET', Journal of Emerging Trends in Computing and Information Sciences, vol. 2, no. 11, pp. 646-655.
15. Chi-Yin Chow, Mohamed F Mokbel&Tian He 2011, 'A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks', IEEE Transactions on Mobile Computing, vol. 10, no. 1, pp. 94-107.
16. David R Raymond, Randy C Marchany, Michael I Brownfield & Scott F Midkiff 2009, 'Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols' ,IEEE transactions on vehicular technology, vol. 58, no. 1, pp. 367-380.
17. Hosque, MS, Mukit, M, Bikas, M &Naser, A 2012. 'An implementation of intrusion detection system using genetic algorithm'. arXiv preprint arXiv:1204.1336.

18. S. Suresh, N. Sankar Ram , " Feasible DDoS attack source traceback scheme by deterministic multiple packet marking mechanism" JOURNAL OF SUPERCOMPUTING(Springer) , ISSN: 0920-8542, E-ISSN 1573-0484, DOI: https://doi.org/10.1007/s11227-018-2323-8,March 2018.
19. S. Suresh, N. Sankar Ram," Reroute the Packets After Finding Zombie using DPM Techniques" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1,pp 1121-1124, Retrieval Number A2122058119/19 ,May 2019.
20. Pradhan PM, Panda G,"Solving multi-objective problems using cat swarm optimization", Expert Syst Appl 2012;39: 2956-2964.
21. Saha Suman Kumar, Ghoshal Sakti Prasad, Kar Rajib, Mandal Durbadal, "Cat Swarm Optimization algorithm for optimal linear phase FIR filter design", ISA Trans 2013 ;52:781-794.
22. Ashraf Darwish 2018, "Bio-inspired computing: Algorithms review, deep analysis, and the scope of applications", Future Computing and Informatics Journal Vol.3 pp.231-246.
23. Balaji.S, Sasilatha.T 2019, 'Detection of Denial of Service Attacks by Domination Graph Application in Wireless Sensor Networks' in Cluster Computing- The Journal of Networks, Software Tools and Applications, Volume 22 Supplement 6, pp.15121 15126(https://doi.org/10.1007/s10586-018- 2504-5).

AUTHORS PROFILE

M.S.Vinmathi , Research Scholar ,Dr. M.G.R. Educational and Research Institute, Department of CSE, Periyar E.V.R. High Road, Viswasa Nagar, Maduravoyal, Chennai, Tamil Nadu 600095, vinmathis@gmail.com
Dr.M.SJosephine , Addl. HOD &Prof, Department of Computer Applications ,Dr. M.G.R. Educational and Research Institute , Periyar E.V.R. High Road, Viswasa Nagar, Maduravoyal, Chennai, Tamil Nadu 600095, josejbr@yahoo.com
Dr.V.Jeyabalaraja, Professor, CSE department ,Vellammal Engineering College, Velammal Nagar, Ambattur-Red Hills Road,Chennai - 600 066 , Jeyabalaraja@velammal.edu.in