RESEARCH ARTICLE OPEN ACCESS

Distributed Denial of Service (DDOS) Attack Detection DDOS-WSN-NS in Wireless Sensor Networks using Network Simulator (NS)

Neeraj Gupta

Assistant Professor, Department of ECE, Amity University - Haryana

ABSTRACT

Wireless sensor network (WSN) is highly indispensable for securing network protection. Highly critical attacks of various kinds have been documented in wireless sensor network till now by many researchers. The Distributed denial of service (DDOS) attack is a typical kind of attack in WSN, consisting two types, namely passive attacks and active attacks, of which the latter can cause greater threat. Initially network is divided into number of clusters, every cluster has one header and the header is directly communicated to destination. From that the nodes which frequently misbehaves and based upon their miss ratio they will be eliminated from the network. The effectiveness of our proposed detection system is evaluated using some performance measures and it's implemented in network simulator.

Keywords: Distributed Denial of Service, DDOS, Attack, Detection, WSN, DDOS-WSN-NS.

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions [1]. LEACH protocol is the first protocol of hierarchical routing which proposed data fusion; it is of milestone significance in clustering routing protocol. Routing strategies and security issues are great research challenge [2-34]. A network that tunnel information to another network, that is it get the data from one network replicate it into another network through tunnel that particular network may confused due to this action. At that time hacker may easily enter and do misuse inside the network [35-47] A DDOS attack (better known as a Distributed Denial of Service attack) is a type of web attack that seeks to disrupt the normal function of the targeted computer network. although several solutions were projected to unravel the DDoS downside and a few sorts of the attacks area unit so [5] countered, DDoS attacks still be a main threat within the net. The goal of this attack is to create a large enough presence of false traffic such that legitimate web traffic intended for actual web users is slowed down and delayed [6]. Various works deal with ways of preventing unauthorized access to data or with the necessary precautions to guarantee data authenticity and integrity inside the network. DoS attacks are prevent the source node to deliver its data to the destination [7]. The application of wireless sensor network, resembling a military force, monitors absence of restriction on the infrastructure as well as in the intermediate hop nodes [10]. WSN has several issues like energy, computation, communication capabilities, deployment, storage, power consumption, longevity etc. that makes it prone to various attacks[11].

II. LITERATURE REVIEW

In 2012 Usman Tariq rt al. [12] have proposed the studied attacks and mitigation scenarios to analyze network wide DDoS security anomalies. T This will identify the potential threat of different DDoS attacks for such platform and traffic scanning activity to avoid detection of attacks such as Ping to Death DDoS attack. This longitudinal analysis was necessary for understanding the progression of the threats and vulnerabilities. In conclusion, while analyzing our early results concerning large-scale DDoS attack. We used a hybrid approach to diminish and prevent the attack. Network Simulator 2 (NS-2) is used to imitate the real environment and to create attack traffic with different attack strength. The simulation results are encouraging as we were able to establish, and approximate strength of DDoS attack efficiently.

k-Means Clustering In Wireless Sensor Networks by Sasi kumar and Sibaram Khara in 2012.[13] recently clustering through distributed methods is being

developed for dealing with the issues like network lifetime and energy. In our work, we implemented both centralized and distributed k-means clustering algorithm in network simulator. k-means is a prototype based algorithm that alternates between two major steps, assigning observations to clusters and computing cluster centers until a stopping criterion is satised. Simulation results are obtained and compared which show that distributed clustering is efficient than centralized clustering.

Wireless Sensor Networks (WSN) has wide applications in data gathering and data transmission via wireless networks by Shital Patil, Sangita Chaudhari [14]. Due to the weaknesses in the WSN, the sensor nodes are vulnerable to most of the security threats. Denial-of-Service (DoS) attack is most popular attack on these sensor nodes. Some attack prevention techniques must be used against DoS attacks. There are different techniques to prevent DoS attack in wireless sensor network. An immune system is proposed for the DoS attack on WSN which will improve the accuracy rate of attack prevention, reduce the false alarm rate and able to recognize different Dos attack.

In 2017 Nejla Rouissi et al.[15] have suggested the a novel energy-efficient and data integrity version of LEACH based routing protocol on Watermarking for wireless sensor networks because LEACH routing protocol does not take the security aspect into consideration and the secure improved LEACH works are based only on cryptographic techniques. Our hybrid proposed approach based on the Watermarking-LEACH achieves not only data integrity but also Energy-Efficient. It is the first schema that attempts to add security based on watermarking to LEACH routing protocol.

In 2014 Sonali Swetapadma Sahu rt al.[16] the author surveyed the DDoS (Distributed Denial of Service) is an attack where a number of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users. Not much research work has been done in DDoS in WSN. We are conducting a review on DDoS attack to show its impact on networks and to present various defensive, detection and preventive measures adopted by researchers till now.

III. IMPLEMENTATION METHODOLOGY

WSN are susceptible to both passive and active Distributed Denial of Service Attacks (DoS) attackers. A passive attacker listens to the channel and may access the packet containing secret information transferring from source to destinations. The virtual topology network is industrialized that encompasses a set of various sensor nodes, one base station and server considered, this nodes are grouped based on different mobile network using K means clustering to cluster the nodes, Moreover all clusters group are choose one cluster with help of trust measure and anticipated scheme marks a sensor as a cluster head, if it has minimum energy consumption. Based on the clustered node detect the attacked node of network topology, for this identifications process consider Low-energy adaptive clustering hierarchy (LEACH) protocol to node moving process. All the paths are stored in the routing table at source node. The main idea in LEACH is during route discovery procedure to compute multiple paths for contending link failure. With help of Cluster Head Detect the abnormal behavior nodes, this attacker enters sensor network topology and attacks the network as external attacker, internal attacker or a compromised internal attacker and causes malicious activities like provides illusion as the shortest path neighbor's performs Denial of Service, performs disruption in routing.

IV. NETWORK STRUCTURE

Designing a network topology is the first step in the logical design phase of the top-down network design methodology. To meet a customer's goals for scalability and adaptability, it is important to architect logical topology before selecting physical products or technologies and its this structure shown in figure 1. This proposed designing process follows the LEACH protocol, this protocol operates reactively to reduce overhead finding routes only on demand.

4.1 Cluster Formation for Node Detection

A Cluster helps to increase the performance of MANET at some extent. If algorithm is strong enough, it will increases data transferring rate, decreases delay rate. In a cluster, Cluster head and boundary node form a virtual backbone for routing among all clusters which are very close to CH. The cluster head plays the role of coordinator within its

substructure, which acts as a medium for data transfer between the nodes. Each CH acts as a temporary base station within its cluster and communicates with other CHs by using gateway nodes. The Gateway node has two or more cluster heads as its neighbor's. When the clusters are disjoint, at least there one cluster head and another gateway node should present.

4.2 Distributed denial-of-service (DDoS) Detection Algorithm

The DDoS attacks are among the hardest security problems today to detect, defend and trace because of the limitation of current network components, multiplicity of attack methods and invisibility of the operators to host sites. To identify the DDoS attacks, endow an alarming agent with a tapestry of reactive rules. All attacks seek to make influence on victim. But DDoS attack differs from the point where victim demonstrated its weakness. By doing some improvement on the LEACH protocol, the probability of selecting a route with a DDoS node will be greater reduced.

Detection Steps

Initialize the network topology (Size from 1 to 100). The BS is fixed and located far from the sensors with correct threshold value.

A Cluster contains nodes which are in the communication range of each other. A node among sensor nodes acts as an attacker. Attacker node has capability that it sense data from environment but does not send it to the cluster head or base station.

If the node i which is trying to access data is the one of the nodes to whom frames are multicast then hit is count else miss will be count.

This attacker node may become a cluster head any time. A CH is elected by the sensor nodes.

Then clusters are formed, cluster heads are elected and it becomes the responsibility of the Base Station to detect if any cluster head becomes an attacker. All the cluster heads are in the control of base station.

Every 8 Intervals check attacked node and of the node as MALIOUS means the miss ratio as high compared to our fixed threshold value.
Until check all nodes (up to 100) in network.

V. CONCLUSION

DDos attack reduces the performance of the system. The privacy and security of data are the major issues concerning about the wireless sensor networks. Special prevention techniques are required to deal with the DDoS attacks in WSNs. Above section deeply discussed the DDoS detection process discussed and the performance also evaluated based on performance measures with LEACH protocol. Furthermore, the main objective of this technique was to maximize PDR on the number of nodes, clusters and confidentiality of the transmission. The main problem is that there are still many insecure machines over the Internet that can be compromised to launch a large-scale coordinated DDoS attack. . Besides, the comparison result has proven that our detection system outperforms in terms of detection accuracy.

REFERENCE

[1] Feng, Y., Yi, J. H., & Wang, G. G. (2019). Enhanced Moth Search Algorithm for the Set-Union Knapsack Problems. IEEE Access, 7, 173774-173785.

[2] Sivaram, M., Batri, K., Amin Salih, M., &Porkodi, V. (2019). Exploiting the Local Optima in Genetic Algorithm using Tabu Search. Indian Journal of Science and Technology, 12(1), 1-13.

[3] Venkatraman, S., &Surendiran, B. (2020). Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems. Multimedia Tools and Applications, 79(5), 3993-4010.

[4] Sujitha, B., Parvathy, V. S., Lydia, E. L., Rani, P., Polkowski, Z., & Shankar, K. (2020). Optimal deep learning based image compression technique for data transmission on industrial Internet of things applications. Transactions on Emerging Telecommunications Technologies, e3976.

[5] Ezhilarasu, P., Krishnaraj, N., &Dhiyanesh, B. (2015). Arithmetic Coding for Lossless Data Compression–A Review. International Journal of Computer Science Trends and Technology, 3(3).

[6] Porkodi, V., Singh, A. R., Sait, A. R. W., Shankar, K., Yang, E., Seo, C., & Joshi, G. P. (2020). Resource Provisioning for Cyber–Physical–Social System in Cloud-Fog-Edge Computing Using Optimal Flower Pollination Algorithm. IEEE Access, 8, 105311-105319.

[7] Gao, D., Wang, G. G., &Pedrycz, W. (2020). Solving fuzzy job-shop scheduling problem using DE algorithm improved by a selection mechanism. IEEE Transactions on Fuzzy Systems.

[8] Sivaram, M., Mohammed, A. S., Yuvaraj, D., Porkodi, V., Manikandan, V., &Yuvaraj, N. (2019, February). Advanced expert system using particle swarm optimization based adaptive network based fuzzy inference system to diagnose the physical constitution of human body. In International Conference on Emerging Technologies in Computer Engineering (pp. 349-362). Springer, Singapore.

[9] Jiménez, A. C., García-Díaz, V., González-Crespo, R., &Bolaños, S. (2018). Decentralized Online Simultaneous Localization and Mapping for Multi-Agent Systems. Sensors, 18(8), 2612.

[10] Venkatraman, S., Surendiran, B., & Kumar, P. A. R. (2020). Spam e-mail classification for the Internet of Things environment using semantic similarity approach. The Journal of Supercomputing, 76(2), 756-776.

[11] Lydia, E. L., Raj, J. S., PandiSelvam, R., Elhoseny, M., & Shankar, K. (2019). Application of discrete transforms with selective coefficients for blind image watermarking. Transactions on Emerging Telecommunications Technologies, e3771.

[12] Ezhilarasu, P., Prakash, J., Krishnaraj, N., Kumar, D. S., Babu, K. S., &Parthasarathy, C. (2015). A Novel Approach to Design the Finite Automata to Accept the Palindrome with the Three Input Characters. Indian Journal of Science and Technology, 8(28).

[13] Devaraj, A. F. S., Elhoseny, M., Dhanasekaran, S., Lydia, E. L., & Shankar, K. (2020). Hybridization of firefly and Improved Multi-Objective Particle Swarm Optimization algorithm for energy efficient load balancing in Cloud Computing environments. Journal of Parallel and Distributed Computing.

[14] Zou, D., Wang, G. G., Sangaiah, A. K., & Kong, X. (2017). A memory-based simulated annealing algorithm and a new auxiliary function for the fixed-outline floorplanning with soft blocks. Journal of Ambient Intelligence a+nd Humanized Computing, 1-12.

[15] Kumar, A., Ahuja, H., Singh, N. K., Gupta, D., Khanna, A., & Rodrigues, J. J. (2018). Supported matrix factorization using distributed representations for personalised recommendations on twitter. Computers & Electrical Engineering, 71, 569-577.

[16] Sivaram, M., Porkodi, V., Mohammed, A. S., Manikandan, V., &Yuvaraj, N. (2019). Retransmission DBTMA protocol with fast retransmission strategy to improve the performance of MANETs. IEEE Access, 7, 85098-85109.

[17] Venkatraman, S., & Kumar, P. A. R. (2019). Improving Adhoc wireless sensor networks security using distributed automaton. Cluster Computing, 22(6), 14551-14557.

[18] Lydia, E. L., Govindaswamy, P., Lakshmanaprabu, S., &Ramya, D. (2018). Document clustering based on text mining K-means algorithm using euclidean distance similarity. J. Adv. Res. Dyn. Control Syst.(JARDCS), 10(2), 208-214.

[19] Dhenakaran, S. S., & Naganathan, E. R. (2007). A new approach to multiple symmetric keys. IJCSNS, 7(6), 254-259.

[20] Ortin, F., Mendez, S., García-Díaz, V., & Garcia, M. (2014). On the suitability of dynamic languages for hot-reprogramming a robotics framework: a Python case study. Software: Practice and Experience, 44(1), 77-104.

[21] Krishnaraj, N., Ezhilarasu, P., & Gao, X. Z. Hybrid Soft Computing Approach for Prediction of Cancer in Colon Using Microarray Gene Data. Current Signal Transduction Therapy, 11(2).

[22] Le Nguyen, B., Lydia, E. L., Elhoseny, M., Pustokhina, I., Pustokhin, D. A., Selim, M. M., ... & Shankar, K. (2020). Privacy Preserving Blockchain Technique to Achieve Secure and Reliable Sharing of IoT Data. CMC-COMPUTERS MATERIALS & CONTINUA, 65(1), 87-107.

[23] Chavhan, S., Gupta, D., Chandana, B. N., Khanna, A., & Rodrigues, J. J. (2019). IoT-based Context-Aware Intelligent Public Transport System in a metropolitan area. IEEE Internet of Things Journal.

[24] Gu, Z. M., & Wang, G. G. (2020). Improving NSGA-III algorithms with information feedback models for large-scale many-objective optimization. Future Generation Computer Systems, 107, 49-69.

[25] Porkodi, V., Khan, J., Mohammed, A. S., Bhuvana, J., & Sivaram, M. OPTIMIZED COOPERATIVE QOS ENHANCED DISTRIBUTED MULTIPATH ROUTING PROTOCOL.

[26] Geerthik, S., Venkatraman, S., & Gandhi, R. (2016). AnswerRank: Identifying Right Answers in QA system. International Journal of Electrical and Computer Engineering, 6(4), 1889.

[27] Samad, A., Salima, R., Lydia, E. L., & Shankar, K. (2020). Definition and Features of Rural Marketing Strategies for Encourage Development in Rural Areas. TEST Engineering & Management, 82, 4983-4988.

[28] Palani, E., Nagappan, K., &Alhadidi, B. (2016). Segmentation and Texture Analysis for Efficient Classification of Breast Tumors from Sonograms. Current Signal Transduction Therapy, 11(2), 84-90.

[29] Rajalakshmi, K., & Dhenakaran, S. S. (2015). Analysis of Datamining Prediction Techniques in Healthcare Management System. International Journal of Advanced Research in Computer Science and Software Engineering, 5(4), 1343-1347.

[30] Yasodha, S., & Dhenakaran, S. S. (2014, January). An ontology-based framework for semantic web content mining. In 2014 International Conference on Computer Communication and Informatics (pp. 1-6). IEEE.

[31] Rajagopal, A., Ramachandran, A., Shankar, K., Khari, M., Jha, S., Lee, Y., & Joshi, G. P. (2020). Fine-tuned residual network-based features with latent variable support vector machine-based optimal scene classification model for unmanned aerial vehicles. IEEE Access, 8, 118396-118404.

[32] Mondragon, V. M., García-Díaz, V., Porcel, C., & Crespo, R. G. (2018). Adaptive contents for interactive TV guided by machine learning based on predictive sentiment analysis of data. Soft Computing, 22(8), 2731-2752.

[33] Feng, Y., Yu, X., & Wang, G. G. (2019). A Novel Monarch Butterfly Optimization with Global Position Updating Operator for Large-Scale 0-1 Knapsack Problems. Mathematics, 7(11), 1056.

[34] Mohammed, A. S., & Sivaram, P. (2018). Securing the Sensor Networks Along With Secured Routing Protocols for Data Transfer in Wireless Sensor Networks.

[35] Geerthik, S., Venkatraman, S., & Gandhi, K. R. (2016, February). Reward rank: A novel approach for positioning user answers in community question answering system. In 2016 International Conference on Information Communication and Embedded Systems (ICICES) (pp. 1-6). IEEE.

[36] Sivaram, M., Lydia, E. L., Pustokhina, I. V., Pustokhin, D. A., Elhoseny, M., Joshi, G. P., & Shankar, K. (2020). An optimal least square support vector machine based earnings prediction of blockchain financial products. IEEE Access, 8, 120321-120330.

[37] Ghantasala, G. P., &KrishnaRaj, N. Support Vector Machine Based Automatic Mammogram Classification Using Hybrid Optimization Algorithm.

[38] Sikkandar, M. Y., Alrasheadi, B. A., Prakash, N. B., Hemalakshmi, G. R., Mohanarathinam, A., & Shankar, K. (2020). Deep learning based an automated skin lesion segmentation and intelligent classification model. Journal of Ambient Intelligence and Humanized Computing, 1-11.

[39] Kumar, P. R., & Dhenakaran, S. S. (2012, December). Pixel based feature extraction for ear biometrics. In 2012 International Conference on Machine Vision and Image Processing (MVIP) (pp. 40-43). IEEE.

[40] Zhang, Z., Wang, G. G., Zou, K., & Zhang, J. (2014). A solution quality assessment method for swarm intelligence optimization algorithms. The Scientific World Journal, 2014.

[41] Sivaram, Murugan et al. 'Data Fusion Using Tabu Crossover Genetic Algorithm in Information Retrieval'. 1 Jan. 2020 : 1 – 10.

[42] Khamparia, A., Pandey, B., Tiwari, S., Gupta, D., Khanna, A., & Rodrigues, J. J. (2020). An integrated hybrid CNN–RNN model for visual description and generation of captions. Circuits, Systems, and Signal Processing, 39(2), 776-788.

[43] Geerthik, S., Gandhi, K. R., &Venkatraman, S. (2016, December). Domain expert ranking for finding domain authoritative users on community question answering sites. In 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-5). IEEE.

[44] Muruganantham, A., Nguyen, P. T., Lydia, E. L., Shankar, K., Hashim, W., &Maseleno, A. (2019). Big data analytics and intelligence: A perspective for health care.

[45] Ramkumar, V., &Krishnaraj, N. Weight Based LSA to Retrieve Information from Web Pages Based On Document Score.

[46] Balakiruthiga, B., Deepalakshmi, P., Mohanty, S. N., Gupta, D., Kumar, P. P., & Shankar, K. (2020). Segment routing based energy aware routing for software defined data center. Cognitive Systems Research.

[47] Chu, H. C., Wang, G. G., & Deng, D. J. (2016). The social networking investigation of metadata of forensic artifacts of a typical WeChat session under Windows. Security and Communication Networks, 9(18), 5698-5709.

[48] Sivaram, M., Yuvaraj, D., Mohammed, A. S., Manikandan, V., Porkodi, V., &Yuvaraj, N. (2019). Improved Enhanced Dbtma with Contention-Aware Admission Control to Improve the Network Performance in Manets. CMC-COMPUTERS MATERIALS & CONTINUA, 60(2), 435-454.

[49] Gochhayat, S. P., Lal, C., Sharma, L., Sharma, D. P., Gupta, D., Saucedo, J. A. M., &Kose, U. (2019). Reliable and secure data transfer in IoT networks. Wireless Networks, 1-14.

[50] Subbarayalu, V., Surendiran, B., &Arun Raj Kumar, P. (2019). Hybrid Network Intrusion Detection System for Smart Environments Based on Internet of Things. The Computer Journal, 62(12), 1822-1839.

[51] Rosa, A. T. R., Pustokhina, I. V., Lydia, E. L., Shankar, K., & Huda, M. (2019). Concept of electronic document management system (EDMS) as an efficient tool for storing document. Journal of Critical Reviews, 6(5), 85-90.

[52] Espada, J. P., Diaz, V. G., Crespo, R. G., Bustelo, B. C. P. G., &Lovelle, J. M. C. (2015). An intelligent Mobile Web Browser to adapt the mobile web as a function of the physical environment. IEEE Latin America Transactions, 13(2), 503-509.

[53] Kumar, R. S., Krishnaraj, N., &Keerthana, G. (2017). Assessment of Quality of Service in Communication Network and Evaluating Connectivity Among IP Networks. Asian Journal of Applied Science and Technology (AJAST), 1(3), 319-322.

[54] Elhoseny, M., Rajan, R. S., Hammoudeh, M., Shankar, K., &Aldabbas, O. (2020). Swarm intelligence–based energy efficient clustering with multihop routing protocol for sustainable wireless sensor networks. International Journal of Distributed Sensor Networks, 16(9), 1550147720949133.

[55] Chu, H. C., Wang, G. G., & Park, J. H. (2015). The digital fingerprinting analysis concerning google calendar under ubiquitous mobile computing era. Symmetry, 7(2), 383-394.

[56] Manikandan, V., Sivaram, M., Mohammed, A. S., &Porkodi, V. (2020). Nature Inspired Improved Firefly Algorithm for Node Clustering in WSNs. CMC-COMPUTERS MATERIALS & CONTINUA, 64(2), 753-776.

[57] Kuppusamy, P., Venkatraman, S., Rishikeshan, C. A., & Reddy, Y. P. (2020). Deep learning based energy efficient optimal timetable rescheduling model for intelligent metro transportation systems. Physical Communication, 101131.

[58] Asih, E. S., Nguyen, P. T., Lydia, E. L., Shankar, K., Hashim, W., &Maseleno, A. (2019). Mobile E-commerce website for technology-based buying selling services. International Journal of Engineering and Advanced Technology, 8(6), 884-888.

[59] Lydia, E. L., &Swarup, M. B. (2015). Big data analysis using hadoop components like flume, mapreduce, pig and hive. International Journal of Science, Engineering and Computer Technology, 5(11), 390.

[60] Sengar, S. S., Hariharan, U., &Rajkumar, K. (2020, March). Multimodal Biometric Authentication System using Deep Learning Method. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 309-312). IEEE.

[61] Kumar, P. R., Sailaja, K. L., Dhenakaran, S. S., & SaiKishore, P. (2012). Chakra: A new approach for symmetric key encryption. In 2012 World Congress on Information and Communication Technologies (pp. 727-732). IEEE.

[62] Maseleno, A., Hashim, W., Perumal, E., Ilayaraja, M., & Shankar, K. (2020). Access control and classifier-based blockchain technology in e-healthcare applications. In Intelligent Data Security Solutions for e-Health Applications (pp. 151-167). Academic Press.

[63] Li, J., Lei, H., Alavi, A. H., & Wang, G. G. (2020). Elephant Herding Optimization: Variants, Hybrids, and Applications. Mathematics, 8(9), 1415.

[64] Mohammed, A. S., Kareem, S. W., Al Azzawi, A. K., & Sivaram, M. (2018). Time series prediction using SRE-NAR and SRE-ADALINE. Journal of Advanced Research in Dynamical and Control Systems, Pages, 1716-1726.

[65] Shankar, K., Elhoseny, M., Chelvi, E. D., Lakshmanaprabu, S. K., & Wu, W. (2018). An efficient optimal key based chaos function for medical image security. IEEE Access, 6, 77145-77154.

[66] Geerthik, S., Gandhi, R., &Venkatraman, S. (2006). CATEGORY BASED EXPERT

RANKING: A NOVEL APPROACH FOR EXPERT IDENTIFICATION IN COMMUNITY QUESTION ANSWERING.

[67] Laxmi, C. V., &Somasundaram, K. (2014). Application Level Scheduling (AppLeS) in Grid with Quality of Service (QoS). International Journal of Grid Computing & Applications, 5(2), 1.

[68] Kumar, R. S., Krishnaraj, N., &Keerthana, G. Highly Energy Efficient and Scalable Distributed Clustering Procedure for Dense Wireless Sensor Networks.

[69] Krishnaraj, N., Kumar, K. A., & Kumar, P. K. (2018). DESIGN OF ADAPTIVE SCHEDULER TO IMPROVE PERFORMANCE OF COMPUTATIONAL GRIDS. International Journal of Pure and Applied Mathematics, 119(18), 1741-1751.

[70] Shankar, K., & Eswaran, P. (2016, January). A new k out of n secret image sharing scheme in visual cryptography. In 2016 10th International Conference on Intelligent Systems and Control (ISCO) (pp. 1-6). IEEE.

[71] Wei, C. L., & Wang, G. G. (2020). Hybrid Annealing Krill Herd and Quantum-Behaved Particle Swarm Optimization. Mathematics, 8(9), 1403.

[72] Sivaram, M., Yuvaraj, D., Mohammed, A. S., &Porkodi, V. Estimating the Secret Message in the Digital Image. International Journal of Computer Applications, 975, 8887.

[73] Nieto, Y., Gacía-Díaz, V., Montenegro, C., González, C. C., & Crespo, R. G. (2019). Usage of machine learning for strategic decision making at higher educational institutions. IEEE Access, 7, 75007-75017.