RESEARCH ARTICLE OPEN ACCESS

Deployment with Location Knowledge by Multi Area Approach

Shashidhar Kasthala
Assistant Professor Indian Naval Academy

ABSTRACT

Wireless Sensor Network (WSN) is profoundly imperative for securing network protection. Profoundly basic attacks of different types have been reported in wireless sensor network till now by numerous researchers. Various replica node detection techniques have been proposed to detect these replica nodes. These methods incur control overheads and the detection accuracy is low when the replica is selected as a witness node. To stop the node replica attack, e propose a location cluster detection scheme using deployment knowledge. From the implementation results the proposed model compared with Area based cluster Approach (ABCD) and Fingerprint based detection techniques.

Keywords: Networking, Wireless Sensor Networks (WSN), clustering, replica Detection, and Knowledge discovery technique.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a wireless network comprising of spatially conveyed self-ruling devices utilizing sensors to screen physical or ecological conditions [1-6]. LEACH protocol is the primary convention of various leveled routing which proposed data combination; it is of point of reference hugeness in clustering routing protocol. Routing procedures and security issues are awesome research challenge [7-16]. Replica node attacks are very dangerous to the operation of sensor networks. With a single captured sensor node, the adversary can create as many replica nodes as he wants; there could easily be as many replica nodes as uncompromised nodes [17-28]. The time and effort needed to inject so many replica nodes into the network is much less than the effort to compromise the equivalent number of original nodes [29-35]. A witness node that receives two conflicting location claims for a node concludes that the node has been replicated and initiates a process to revoke the node. In the line-selected multicast scheme, both intermediate nodes, which relay the claims, and witness nodes participate in detecting and revoking replicas [36-46]. The objective of this attack is to make a sufficiently huge nearness of false activity with the end goal that authentic web movement expected for real web clients is backed off and postponed [47]. Different works manage methods for anticipating unapproved access to data or with the essential safety measures to ensure data genuineness and uprightness inside the network. DoS attacks are keep the source node to convey its data to the goal [48-53]. The attacks which work at the network layer are alluded to as routing attacks. Monitoring tools can distinguish an attack and recognize essential properties, for example, traffic rates and packet types. Despite that, on the grounds that attackers can produce most packet data, describing attacks as single-or multi-source and recognizing the quantity of attackers is troublesome [54-60]. RN will be deployed back into the networks to eavesdrop communications or launch attacks.

II. RELATED WORKS

Wireless Sensor Networks (WSN) has wide applications in data gathering and data transmission by means of wireless networks by [61]. Because of the shortcomings in the WSN, the sensor nodes were powerless against the vast majority of the security dangers. Denial of-Service (DoS) attack is most mainstream attack on these sensor nodes. Some attack aversion procedures must be utilized against DoS attacks. There are distinctive methods to avert DoS attack in wireless sensor network. An invulnerable framework was proposed for the DoS attack on WSN which will enhance the precision rate of attack anticipation; decrease the false alarm rate and ready to perceive distinctive Dos attack.

To solve these issues by enhancing the Single Hop Detection (SHD) method using the Clonal Selection algorithm to detect the clones by selecting the appropriate witness nodes [62]. The advantages of the proposed method include (i) increase in the detection ratio, (ii) decrease in the control overhead, and (iii) increase in throughput. One among them is the node replication attack. In this, the physically insecure nodes are acquired by the adversary to clone them by having the same identity of the captured node, and the adversary deploys an unpredictable number of replicas throughout the network. Hence replica node detection is an important challenge in Mobile Wireless Sensor Networks.Considering the limitations of centralized detection schemes for static wireless sensor networks, a few distributed solutions have been recently proposed [63]To facilitate the discovery of contradictory conflicts, we propose a hybrid local and global detection method. The local detection is performed in a local area smaller than the whole deployed area to improve the meeting probability of contradictory nodes, while the distant replicated nodes in larger area can also be efficiently detected by the global detection.

III. REPLICA NODE DETECTION IN WSN

- The replica nodes are controlled by the adversary. The problem is the replica nodes also contain the key that is required for secured communication in the network. In addition to these problems, mobility of nodes, the collusion of replica, and sideway attacks are the main difficulty while detecting and controlling these replica nodes.
- When the replicas are not detected, then the network will be open to attackers and the network becomes more vulnerable.
- Security in wireless sensor networks is challenging due to characteristics of sensor networks and the lack of hardware support for incursion protection.
- In the node replication attack, an attacker intentionally puts replicas of a compromised node in many places in the network to make inconsistency. In the wormhole attack, an attacker can tunnel packets through a secret broadband channel between two distant places and replay them to distort the network topology by making two distant nodes believe they are neighbours.
- However, these solutions are not satisfactory. First, they are energy and memory demanding: A serious drawback for any protocol that is to be used in resource constrained environment such as a sensor network.

IV. LEACH PROTOCOL

LEACH protocol is the principal protocol of progressive routing which proposed data fusion; it is of point of reference criticalness in clustering routing protocol. Routing methodologies and security issues are incredible research challenge. These days in WSN, quantities of routing protocols have been proposed however most surely understood protocols are hierarchical protocols like LEACH. The principle point of this protocol is to enhance the life expectancy of wireless sensor networks by bringing down the energy.

- Nodes choose probabilistically regardless of whether to end up noticeably a CH for the current round in view of its outstanding energy and globally known wanted level of CHs. Those will communicate a message promoting this reality, at a level that can be heard by everybody in the network.
- Each node knows when it is its turn to transmit, as per the availability plan and the CHs gather messages from all their cluster individuals, total this information, and send the outcome to the BS.

4.1 Cluster formation for Replication Detection

In a centralized approach for detecting node replication, the location claim of nodes will be forwarded to a central trusted party. The simplest solution is to send all location claims to a base station. However, if the base station stays in a hostile environment, some location claims may not reach to the base station. The cluster head assumes the part of facilitator inside its substructure, which goes about as a medium for data exchange between the nodes. Each CH goes about as an impermanent base station inside its cluster and speaks with different CHs by utilizing gateway nodes shows in figure 1. The Gateway node has at least two cluster heads as its neighbor's. At the point when the clusters are disjoint, in any event there one cluster head and another gateway node should begin. Cluster development helps to advance data transmission reason K means clustering procedure steps appeared in underneath segment.

4.2 Deployment with Location Knowledge (DLK)

To improve the security as well as the performance of this approach with additional knowledge. The basic approach assumes that sensor nodes are deployed group by group, and that each group is expected to be deployed towards a deployment point that can be pre-determined. Prior to deployment, the network operator loads the pre-determined deployment coordinates of every group onto every sensor node. The sensor nodes in the same group are very likely to be close to each other after deployment. Our schemes use this knowledge to stop node replication. To evaluate the security of Scheme , we would like to point out that it is infeasible to completely eliminate replicas from the network.

Detection Steps

Initialize the network topology (Size from 1 to 500). The Base station is settled and situated a long way from the sensors with correct threshold esteem.

V. RESULTS AND ANALYSIS

Replica node detection process results are discussed in Network Simulator (NS2) with simulation parameters and IEEE 802.11b is connected to the MAC layer protocol.

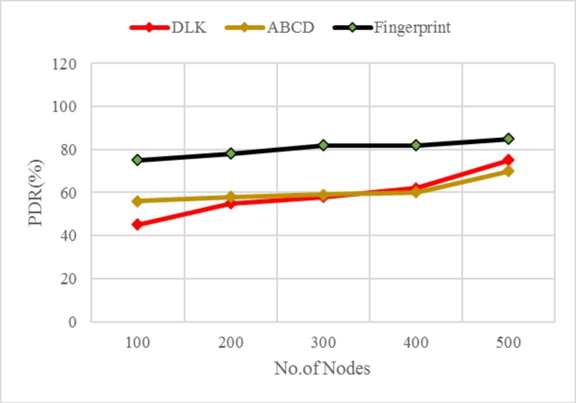

Figure 1: PDR Analysis

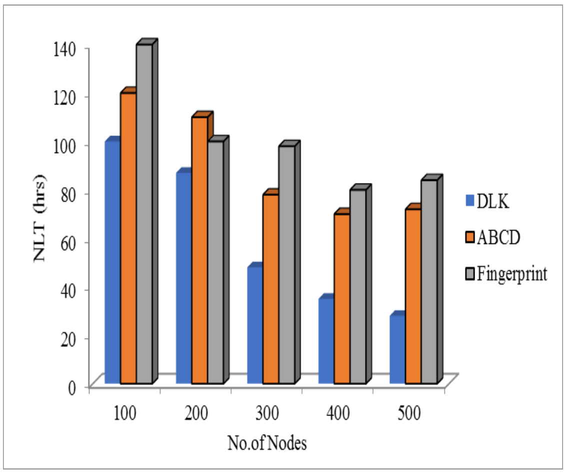

Figure 2: NLT analysis

Figure 1 and 2 shows the results for PDR and NLT, Compared to all the techniques, the proposed model gets maximum that means the routing protocol chooses the trust node and carry out the data forwarding while constructing the WSN process. Our proposed clustering achieves 35% for all the parameters and reaches 40% in PDR so; it has the route recovery mechanism. In the route recovery procedures, the consumption begins to increase when the speed increase.

VI. CONCLUSION

The privacy and security of data are the real issues worried about the wireless sensor networks. Extraordinary avoidance methods are required to manage the clone node attacks in WSNs. Moreover, the principle goal of this procedure was to maximize replica detection level on the number of nodes, clusters, and privacy of the transmission. Our proposed detection model This is because replicated nodes would not trigger a revocation procedure, and a claim message may be lost in the route path to the corresponding witness node. Both of the results demonstrate that our approach provides better security resilience against the presented types of attack strategies in terms of a higher detection rate with a reasonable increase of communication overhead, and minimized the Delay.

REFERENCE

[1] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, Dac Nhuong Le, Smart Surveillance Robot for the Real Time Monitoring and Control System in Environment and Industrial Applications, Advances in Intelligent System and Computing, pp 229-243, Springer

[2] Ezhilarasu, P., & Krishnaraj, N. (2015). Applications of Finite Automata in Lexical Analysis and as a Ticket Vending Machine– A Review. Int. J. Comput. Sci. Eng. Technol, 6(05), 267-270.

[3] Agrawal, U., Arora, J., Singh, R., Gupta, D., Khanna, A., & Khamparia, A. (2020). Hybrid Wolf-Bat Algorithm for Optimization of Connection Weights in Multi-layer Perceptron. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 16(1s), 1-20.

[4] Prasanna, S., & Ezhilmaran, D. (2016). Association rule mining using enhanced apriori with modified GA for stock prediction. International Journal of Data Mining, Modelling and Management, 8(2), 195-207.

[5] Pustokhina, I. V., Pustokhin, D. A., Gupta, D., Khanna, A., Shankar, K., & Nguyen, G. N. (2020). An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. IEEE Access, 8, 107112-107123.

[6] Shankar, K., Zhang, Y., Liu, Y., Wu, L., & Chen, C. H. (2020). Hyperparameter tuning deep learning for diabetic retinopathy fundus image classification. IEEE Access, 8, 118164-118173.

[7] Joshi, G. P., Perumal, E., Shankar, K., Tariq, U., Ahmad, T., & Ibrahim, A. (2020). Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks. Electronics, 9(9), 1358.

[8] Saračević, M. H., Adamović, S. Z., Miškovic, V. A., Elhoseny, M., Maček, N. D., Selim, M. M., & Shankar, K. (2020). Data Encryption for Internet of Things

Applications Based on Catalan Objects and Two Combinatorial Structures. IEEE Transactions on Reliability.

[9] Namasudra, S., & Roy, P. (2017). Time saving protocol for data accessing in cloud computing. IET Communications, 11(10), 1558-1565.

[10] Elsir, A., Elsier, O., Abdurrahman, A., & Mubarakali, A. (2019). Privacy Preservation in Big Data with Data Scalability and Efficiency Using Efficient and Secure Data Balanced Scheduling Algorithm.

[11] Ezhilarasu, P., Krishnaraj, N., & Babu, S. V. (2015). Applications of finite automata in text search-a review. International Journal of Science, Engineering and Computer Technology, 5(5), 116.

[12] Huyen, D.T.T., Binh, N.T., Tuan, T.M., Nguyen, G.N, Dey, N., Son, L.H, Analyzing trends in hospital-cost payments of patients using ARIMA and GIS: Case study at the Hanoi Medical University Hospital, Vietnam, Journal of Medical Imaging and Health Informatics, 7(2), pp. 421-429.

[13] Prasanna, S., & Maran, E. (2015). Stock Market Prediction Using Clustering with Meta-Heuristic Approaches. Gazi University Journal of Science, 28(3).

[14] Pustokhina, I. V., Pustokhin, D. A., Rodrigues, J. J., Gupta, D., Khanna, A., Shankar, K., ... & Joshi, G. P. (2020). Automatic Vehicle License Plate Recognition using Optimal K-Means with Convolutional Neural Network for Intelligent Transportation Systems. IEEE Access.

[15] Namasudra, S. (2018). Cloud computing: A new era. Journal of Fundamental and Applied Sciences, 10(2).

[16] Uthayakumar, J., Elhoseny, M., & Shankar, K. (2020). Highly Reliable and Low-Complexity Image Compression Scheme Using Neighborhood Correlation Sequence Algorithm in WSN. IEEE Transactions on Reliability.

[17] Deepalakshmi, P., & Shankar, K. (2020). Role and Impacts of Ant Colony Optimization in Job Shop Scheduling Problems: A Detailed Analysis. Evolutionary Computation in Scheduling, 11-35.

[18] Ashwin, M., Kamalraj, S., & Azath, M. (2019). Multi objective trust optimization for efficient communication in wireless M learning applications. Cluster Computing, 22(5), 10687-10695.

[19] Ezhilarasu, P., & Krishnaraj, N. (2015). Double Substring based Classification for Nondeterministic Finite Automata. Indian Journal Of Science And Technology, 8, 26.

[20] Amira S. Ashour, Samsad Beagum, Nilanjan Dey, Ahmed S. Ashour, Dimitra Sifaki Pistolla, Gia Nhu Nguyen, Dac-Nhuong Le, Fuqian Shi (2018), Light Microscopy Image De-noising using Optimized LPA-ICI Filter, Neural Computing and Applications, Vol.29(12), pp 1517–1533, Springer, ISSN: 0941-0643.

[21] Prasanna, S., Govinda, K., & Kumaran, U. S. (2012). An Evaluation study of Oral Cancer Detection using Data Mining Classification Techniques. International Journal of Advanced Research in Computer Science, 3(1).

[22] Sankhwar, S., Gupta, D., Ramya, K. C., Rani, S. S., Shankar, K., & Lakshmanaprabu, S. K. (2020). Improved grey wolf optimization-based feature subset selection with fuzzy neural classifier for financial crisis prediction. Soft Computing, 24(1), 101-110.

[23] Namasudra, S., & Deka, G. C. (2018). Introduction of DNA computing in cryptography. In Advances of DNA computing in cryptography (pp. 1-18). Chapman and Hall/CRC.

[24] Mubarakali, A., Srinivasan, K., Mukhalid, R., Jaganathan, S. C., & Marina, N. (2020). Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems. Computational Intelligence.

[25] Le Nguyen Bao, Dac-Nhuong Le, Gia Nhu Nguyen, Vikrant Bhateja, Suresh Chandra Satapathy (2017), Optimizing Feature Selection in Video-based Recognition using Max-Min Ant System for the Online Video Contextual Advertisement User-Oriented System, Journal of Computational Science, Elsevier ISSN: 1877-7503. Vol.21, pp.361-370.

[26] Ezhilarasu, P., Thirunavukkarasu, E., Karuppusami, G., & Krishnaraj, N. (2015). Single substring based classification for nondeterministic finite automata. International Journal on Applications in Information and Communication Engineering, 1(10), 29-31.

[27] Bhateja, V., Gautam, A., Tiwari, A., Nhu, N.G., Le, D.-N, Haralick features-based classification of mammograms using SVM, Advances in Intelligent Systems and Computing, Volume 672, 2018, Pages 787-795.

[28] Latha, A., Prasanna, S., Hemalatha, S., & Sivakumar, B. (2019). A harmonized trust

assisted energy efficient data aggregation scheme for distributed sensor networks. Cognitive Systems Research, 56, 14-22.

[29] Krishnaraj, N., Elhoseny, M., Lydia, E. L., Shankar, K., & ALDabbas, O. (2020). An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment. Software: Practice and Experience.

[30] Namasudra, S., Roy, P., Vijayakumar, P., Audithan, S., & Balusamy, B. (2017). Time efficient secure DNA based access control model for cloud computing environment. Future Generation Computer Systems, 73, 90-105.

[31] Lakshmanaprabu, S. K., Shankar, K., Rani, S. S., Abdulhay, E., Arunkumar, N., Ramirez, G., & Uthayakumar, J. (2019). An effect of big data technology with ant colony optimization based routing in vehicular ad hoc networks: Towards smart cities. Journal of cleaner production, 217, 584-593.

[32] Namasudra, S., & Deka, G. C. (Eds.). (2018). Advances of DNA computing in cryptography. CRC Press.

[33] Mubarakali, A., Ashwin, M., Mavaluru, D., & Kumar, A. D. (2020). Design an attribute based health record protection algorithm for healthcare services in cloud environment. Multimedia Tools and Applications, 79(5), 3943-3956.

[34] Dey, N., Ashour, A.S., Chakraborty, S., Le, D.-N., Nguyen, G.N, Healthy and unhealthy rat hippocampus cells classification: A neural based automated system for Alzheimer disease classification, Journal of Advanced Microscopy Research, 11(1), pp. 1-10

[35] 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).

[36] Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., & Gandomi, A. H. (2020). The revolution of blockchain: State-of-the-art and research challenges. Archives of Computational Methods in Engineering.

[37] Goel, N., Grover, B., Gupta, D., Khanna, A., & Sharma, M. (2020). Modified Grasshopper Optimization Algorithm for detection of Autism Spectrum Disorder. Physical Communication, 101115.

[38] Prasanna, S., Narayan, S., NallaKaruppan, M. K., Anilkumar, C., & Ramasubbareddy, S. (2019). Iterative Approach for Frequent Set Mining Using Hadoop Over Cloud Environment. In Smart Intelligent Computing and Applications (pp. 399-405). Springer, Singapore.

[39] Le, D.-N.a, Kumar, R.b, Nguyen, G.N., Chatterjee, J.M.d, Cloud Computing and Virtualization,
DOI: 10.1002/9781119488149, Wiley.

[40] Raj, R. J. S., Shobana, S. J., Pustokhina, I. V., Pustokhin, D. A., Gupta, D., & Shankar, K. (2020). Optimal Feature Selection-Based Medical Image Classification Using Deep Learning Model in Internet of Medical Things. IEEE Access, 8, 58006-58017.

[41] Namasudra, S., & Deka, G. C. (2018). Taxonomy of DNA-based security models. In Advances of DNA Computing in Cryptography (pp. 37-52). Chapman and Hall/CRC.

[42] Mubarakali, A., Ramakrishnan, J., Mavaluru, D., Elsir, A., Elsier, O., & Wakil, K. (2019). A new efficient design for random access memory based on quantum dot cellular automata nanotechnology. Nano Communication Networks, 21, 100252.

[43] Ramakrishnan, J., Mavaluru, D., Sakthivel, R. S., Alqahtani, A. S., Mubarakali, A., & Retnadhas, M. (2020). Brain–computer interface for amyotrophic lateral sclerosis patients using deep learning network. NEURAL COMPUTING & APPLICATIONS.

[44] Van, V.N., Chi, L.M., Long, N.Q., Nguyen, G.N., Le, D.-N, A performance analysis of openstack open-source solution for IaaS cloud computing, Advances in Intelligent Systems and Computing, 380, pp. 141-150.

[45] Sinha, A., Shrivastava, G., Kumar, P., & Gupta, D. (2020). A community-based hierarchical user authentication scheme for Industry 4.0. Software: Practice and Experience.

[46] Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). Towards DNA based data security in the cloud computing environment. Computer Communications, 151, 539-547.

[47] Mubarakali, A., Durai, A. D., Alshehri, M., AlFarraj, O., Ramakrishnan, J., & Mavaluru, D. (2020). Fog-Based Delay-Sensitive Data Transmission Algorithm for Data Forwarding and Storage in Cloud Environment for Multimedia Applications. Big Data.

[48] Reshmi, T. R., & Azath, M. (2020). Improved self-healing technique for 5G networks using predictive analysis. Peer-to-Peer Networking and Applications, 1-17.

[49] Namasudra, S., Chakraborty, R., Majumder, A., & Moparthi, N. R. (2020). Securing multimedia by using DNA based encryption in the cloud computing environment. ACM Transactions on Multimedia Computing Communications and Applications.

[50] Patro, K. K., Reddi, S. P. R., Khalelulla, S. E., Kumar, P. R., & Shankar, K. (2020). ECG data optimization for biometric human recognition using statistical distributed machine learning algorithm. The Journal of Supercomputing, 76(2), 858-875.

[51] Rajagopal, A., Joshi, G. P., Ramachandran, A., Subhalakshmi, R. T., Khari, M., Jha, S., ... & You, J. (2020). A Deep Learning Model Based on Multi-Objective Particle Swarm Optimization for Scene Classification in Unmanned Aerial Vehicles. IEEE Access, 8, 135383-135393.

[52] Chakchai So-In, Tri Gia Nguyen, Gia Nhu Nguyen: Barrier Coverage Deployment Algorithms for Mobile Sensor Networks. Journal of Internet Technology 12/2017; 18(7):1689-1699.

[53] Mubarakali, A., Bose, S. C., Srinivasan, K., Elsir, A., & Elsier, O. (2019). Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. Journal of Ambient Intelligence and Humanized Computing, 1-9.

[54] Devaraj, A. F. S., Murugaboopathi, G., Elhoseny, M., Shankar, K., Min, K., Moon, H., & Joshi, G. P. (2020). An Efficient Framework for Secure Image Archival and Retrieval System Using Multiple Secret Share Creation Scheme. IEEE Access, 8, 144310-144320.

[55] Mubarakali, A. (2020). Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN (SRHB) Approach. MOBILE NETWORKS & APPLICATIONS.

[56] Namasudra, S. (2019). An improved attribute-based encryption technique towards the data security in cloud computing. Concurrency and Computation: Practice and Experience, 31(3), e4364.

[57] Kathiresan, S., Sait, A. R. W., Gupta, D., Lakshmanaprabu, S. K., Khanna, A., & Pandey, H. M. (2020). Automated detection and classification of fundus diabetic retinopathy images using synergic deep learning model. Pattern Recognition Letters.

[58] Govinda, K., & Prasanna, S. (2015, February). Medical dialysis prediction using fuzzy rules. In 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (pp. 1-5). IEEE.

[59] Sujatha, R., Navaneethan, C., Kaluri, R., & Prasanna, S. (2020). Optimized Digital Transformation in Government Services with Blockchain. In Blockchain Technology and Applications (pp. 79-100). Auerbach Publications.

[60] Govinda, K., & Prasanna, S. (2015, February). A generic image cryptography based on Rubik's cube. In 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (pp. 1-4). IEEE.

[61] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, BioSenHealth 1.0: A Novel Internet of Medical Things (IoMT) Based Patient Health Monitoring System, Lecture Notes in Networks and Systems. Springer, 2019

[62] Prasanna, S., & Narayanan, V. (2017). A Novel Approach for Generation of All-Optical OFDM Using Discrete Cosine Transform Based on Optical Couplers in a Radio-Over-Fiber Link. International Journal of Advanced Research in Engineering and Technology, 8(3).

[63] Sanjeevi, P., Prasanna, S., Siva Kumar, B., Gunasekaran, G., Alagiri, I., & Vijay Anand, R. (2020). Precision agriculture and farming using Internet of Things based on wireless sensor network. Transactions on Emerging Telecommunications Technologies, e3978.

[64] Rathi, V. K., Chaudhary, V., Rajput, N. K., Ahuja, B., Jaiswal, A. K., Gupta, D., ... & Hammoudeh, M. (2020). A Blockchain-Enabled Multi Domain Edge Computing Orchestrator. IEEE Internet of Things Magazine, 3(2), 30-36.

[65] Khanna, A., Rodrigues, J. J., Gupta, N., Swaroop, A., & Gupta, D. (2020). Local mutual exclusion algorithm using fuzzy logic for Flying Ad hoc Networks. Computer Communications.