JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Energy Drain Attack Detection In Underwater Sensor Networks

Dr.A.Senthil Kumar[1*] ,K .Chaithanya [2*] ,Gudipati V M S L Vyshnavi[3],Kallam Charitha Reddy [4],Alisetty Triveni [5],Putla Kejiya Deepika [6]

[1]Associate Professor: Vignan's Nirula Institute of Technology and Science for Women.
[2]Assistant Professor: Vignan's Nirula Institute of Technology and Science for Women.
[3,4,5,6] B.Tech Scholar: Vignan's Nirula Institute of Technology and Science for Women.
senthilkumar9012@gmail.com,chaitanyacns3@gmail.com,22nn1a05e0.vyshnavi@gmail.com,22nn1a05e3charithareddy@gmail.com, 22nn1a05c1@gmail.com, 22nn1a05g8.kejiya@gmail.com.

Abstract:
Underwater Wireless Sensor Networks (UWSN) have gained more attention from researchers in recent years due to their advancement in marine monitoring, deployment of various applications, and ocean surveillance. In this field the main work is focused on different attacks which are related to nodes and deployment of the networks. Energy is the much costlier resource for these networks, so in this paper we are focusing on those attacks which are on power resources of the node by the advisory. Our first intension is to explore the knowledge about the energy drain attacks. In Wireless sensor and actor networks (WSANs), sensors gather information about the physical world, while actors take decisions and then perform appropriate actions upon the environment, which allows a user to effectively sense and act from a distance. Here we examine radio interference attacks from both sides of the issue. Here we study the problem of conducting radio interference attacks on wireless networks, and second, we examine the critical issue of diagnosing the presence of jamming attacks. In particular, we observe that signal strength and carriers ensuring time are unable to conclusively detect the presence of a jammer. Further, we observe that although by using packet delivery ratio we may differentiate between congested and jammed scenarios, we are none the less unable to conclude whether poor link utility is due to jamming or the mobility of nodes.

Keywords:
Wireless sensor networks, Sensor nodes, Monitoring, Battery Power, Data gathering ,Energy Consumption, Security, Military and Medical applications ,Denial Of Service Attacks

1.Introduction:
In a human life wireless sensor network is an important factor and a very use full technology. [1-15]Wireless sensor networks are the combination of sensors nodes in which every node is depend on the battery power energy[16-30].In wireless sensor network sensors are the soul of it and play an important role for gathering the data so it is also called as „mote".[31-45]The sensors in a node provide the facility to get the data and the main goal of the applications is achieved by the cooperation of all sensor nodes in the network[46-52]. The main application of the sensor networks are the Medical Application and the military applications of sensor nodes include monitoring, surveillance and battlefield guiding systems of intelligent missiles etc..

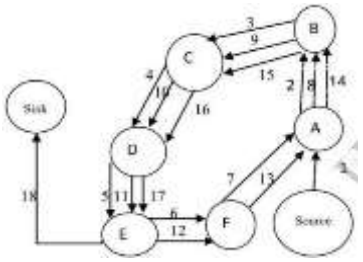
Energy Drain Attacks :
The name "energy drain" show the wasting of energy and making dead the node. Attackers may use malicious nodes to inject forgery or corrupt reports or data into the network or generate large amount of traffic in the network. The main goal of these types of attacks is to degrade the performance of the networks and destroying the networks. There are two types of energy drain attacks.

A.Vampire Attack: "Vampire attack" is based on the routing .In wireless sensor networks data is transmit node to node by a defined routing protocol. This attack is done on these routing protocols of the sensor networks by either continuous repeating the corrupt data.

1.Carousel Attack:

This targets source routing protocols by allowing a corrupt packet to loop through the same nodes repeatedly, consuming energy. For example, a packet sent from node A to sink might loop back to A after several hops, causing excessive energy usage.Asweshowinthefigure1 a.

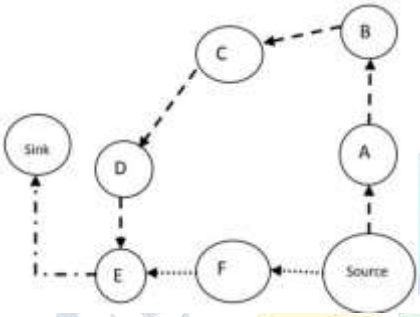
Fig1a:Malicious route construction attacks on source routing: carousel attack



2.Stretch Attack

In this type of attack corrupt data packet choose the longest routing path instead of shortest path. We call it the stretch attack, since it increases data packet path lengths, causing data packets to be processed by a number of nodes that is independent of hop count along the shortest path between the source adversary and packet destination. In this figure we illustrated the working of the stretch attack by the given example. In this example we show the network of eight nodes in this figure we show the honest route by dotted line and malicious route by dashed line, link node E to sink is same for both routing. Here, The node waste its energy that doesn't belong to honest route path.

Fig1b:Malicious route construction attacks on source routing: stretch attack



B.Denial of Sleep Attacks(DS):

This is the second class of energy drain attack in this attack advisory used the legitimate data for wasting the energy by sending it either continuously or sending in a wrong way. The DS attack is that targets a battery powered devices power supply in an effort to wear out this embarrassment resource and degrade the network life time. Denial of sleep attacks divided into six categories.

1)Sleep Deprivation Attack

In the network every node sends a request to send the data to its neighbour node after receiving the request receiver node check from its routing table if requesting node in its table the n it clear to send otherwise discard it and go to in sleep mode. As per the name of this attack malicious node continuously send the data, so that node does not go in the sleep mode and waste its energy .

2)Barrage Attack

In this attack attacker creates bombarding by the genuine requests to the victim node and waste the energy. The main difference between the sleep deprivation attack and barrage attack is in first attack attacker is in idle mode but in second attacker is in active mode.

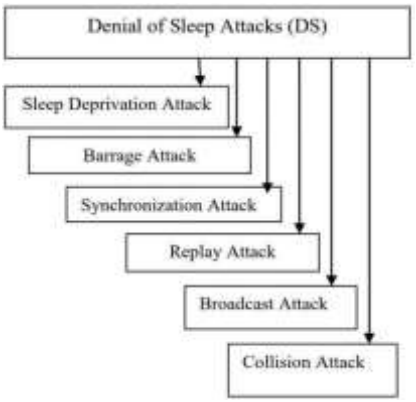


Fig 2:Classification of denial of sleep attack (DS)

3)Synchronization Attack

In this attack attacker creates the disturbance in the synchronization of packet receiving and packet sending due to this the synchronization problems occur at the MAC layer and due to this node drain its battery power.

4)Replay Attack

In this attack all information which is in stored or recorded manner can be transmit again and again without any logical mean and waste the energy of the node.

5)Broadcast Attack

In this attack, malicious node broadcasts unauthenticated traffic into the network and reduce sensor nodes lifetime. In this attack long massage can be transmit in to the network to create the artificial traffic due to more drain of energy.

6)Collision Attack

The malicious node does not follow medium access control protocol due to this collision occur with the neighbour node packet. After collision data packet has been lost and node has to send the data again due to this energy is wasted.

2.Proposed Methodology:

Energy Monitoring Algorithm(EMA):

Description: EMA involves continuously monitoring the energy consumption of each node in the network and setting thresholds for normal energy usage. When a node exceeds these thresholds, it may indicate an energy drain attack.

1..Initialization

For each node **i**:

Set E_max[i], E_current[i] = E_max[i], and threshold[i] = 10% of E_max[i].

Set T_monitor = monitoring interval, and α = abnormal consumption threshold.

2.Periodic Monitoring

At every $T_{monitor}$:

Measure current energy E_current[i] and calculate consumption $\Delta E[i] = E_{previous}[i] - E_{current}[i]$

3.Check for Low Energy

If Ecurrent[i]<threshold[i],alert the base station and mark node i as low energy.

4.Detect Abnormal Energy Consumption

If ΔE[i]>α×ΔEnormal, flag node i as potentially under attack.

5.Neighbor Verification

- Neighbors of node i cross-check their energy.
- **If multiple neighbors** report abnormal energy, confirm the attack and alert the base station.

6.Mitigation

Isolate node iii and recalculate routing paths at the base station to avoid the affected node.

7.Recovery

- **If** energy consumption normalizes, reintegrate node i.
- **If** energy is exhausted, remove node i from the network.

8.Update

Update E_previous[i] = E_current[i] for the next monitoring period.

9.Termination

Continue monitoring until all nodes are drained or no attacks are detected.

3.Literature Survey:

[1]IrfanAhmadet.al[2021]:This research has used Terrestrial wireless sensor networks(TWSN). Underwater Wireless Sensor Networks (UWSNs) are commonly used nowadays to detect and monitor the underwater environment. It contains several sensors and vehicles placed in a selected area to perform specific tasks. These networks are further connected with base stations and satellites to process the detected data for further processing. The technology used in underwater wireless sensor networks can replace conventional methods by remote control of underwater appliances and onshore systems, advanced data recording devices, and real-time monitoring. Attackers can easily take advantage of these characteristics to steal the data between the source and destination.

[2]Akhil Dubey, VaishaliJainet.al[2014]: It has used the holistic security approach for energy drain attacks. Wireless sensor networks are the combination of sensors nodes in which every node is depend on the battery power energy. In wireless sensor network sensors are the soul of it and play an important role for gathering the data so it is also called as „mote". Wireless sensor network plays an important role in natural calamities. It was vastly use in environmental monitoring like through it we can effectively act to prevent the consequences of floods. The sensor nodes have been deployed in the river where nodes monitor the change of water level in real time. At the time of national disaster enemy country can attack on these networks, so it provides wrong information and disaster will become more horrible. So, we have to defend all types of attack on WSN, energy drain attack is one of them.

[3]Akyildiz IF, Pompili D, Melodia Tet.al[2004]:It uses the acoustic sensor networks. In this paper, we examine radio interference attacks from both sides of the issue: first, we study the problem of conducting radio interference attacks on wireless networks, and second we examine the critical issue of diagnosing the presence of jamming attacks. Wireless networks are being deployed in a variety of forms, ranging from ad hoc networks to wireless LANs to sensor networks. The shared nature of the wireless medium will allow adversaries to pose non-cryptographic security threats by conducting radio interference attacks. We showed that by using signal strength, calculates sensing time, or the packet delivery ratio individually, one is not able to definitively conclude the presence of a jammer.

[4]Ian F. Akyildiz et.al[2004]:It had used the collaborative monitoring missions. underwater vehicles (UUVs, AUVs),equipped with sensors, will enable the exploration of natural undersea resources and gathering of scientific data in collaborative monitoring missions. Underwater acoustic networking is the enabling technology for these applications. Underwater networks consist of a variable number of sensors and vehicles that are deployed to perform collaborative monitoring tasks over a given area.

[5] Wenyuan Xu, Wade Trappe, Yanyong ZhangandTimothyWoodet.al[2005]:This research has used Denial of Service, Jamming, Jammer detection attacks. In this paper, we examine radio interference attacks from both sides of the issue: first, we study the problem of conducting radio interference attacks on wireless networks, and second we examine the critical issue of diagnosing the presence of jamming attacks. This paper has been focusing on both sides of the issue by presenting four different jammer attack models that may be employed against a wireless network, as well as exploring techniques for detecting the presence of a jamming attack. We have studied the effectiveness of our four jammer strategies by constructing prototy pes using the MICA2 Mote platform and measuring how each of the jammers fared in terms of their effect on the packet send ratio and packet delivery ratio. We showed that by using signal strength, calculate sensing time, or the packet delivery ratio individually, one is not able to definitively conclude the presence of a jammer.

[6]Misra,S.,Krishna,P.V.,Abraham,K.I.,Sasikumar,N.,Fredunet.al[2010]:It had used the Optimized link state routing protocol. In this paper, we have proposed a protocol to prevent DDoS attacks in a wireless mesh network. Wireless Mesh Networks(WMNs) have potentially unlimited applications in the future. Hence, establishing a viable and secure wireless network routing protocol for these networks is essential. These networks can also support connecting remote areas of the country, instead of having to lay a cable all the way. In the future, we intend to compare DLSR with other protocol developed for WMNs.

[7]Kong,J.,Cui,J.H.,Wu,D.,Gerlaet.al: It has used the Denial of Service, Jamming, Jammer detection attacks. Mobile underwater sensor networks are usually featured with three-dimensional topology ,high node mobility and long propagation delays. In this paper, we proposed avoidance protocol, called Vector-Based Void Avoidance (VBVA), to address the routing void problem in mobile underwater sensor networks. VBVA adopts two mechanisms, vector-shift and back-pressure, to handle voids. The shared nature of the wireless medium will allow adversaries to pose non-cryptographic security threats by conducting radio interference attacks. This paper has sought to focus on both sides of the issue by presenting four different jammer attack models that may be employed against a wireless network, as well as exploring techniques for detecting the presence of a jamming attack. We introduced two enhanced detection algorithms: one employing signal strength as a consistency check, and one employing location information as a consistency check.

[8]XingxingXiao,HainingHuang,WeiWanget.al[2021]:It uses the Data Fusion and Genetic Algorithms. Underwater wireless sensor networks(UWSNs) consist of many underwater wireless sensor nodes distributed within the marine environment, which support a wide variety of applications such as surveillance, navigation, data acquisition, resource exploration, and disaster prevention. The responsibility of the sensor nodes is to monitor the underwater environment such as the temperature, and send the collected data to a sink node(SN)through a single hop or multiple hops. In the underwater environment, the radio signals face the absorption problem and attenuate quickly. Hence, they are not suitable for long-distance underwater communications. This work focuses on the simulation experiment rather than the real implementation. The sea experiment, which is extremely complicated and expensive to perform, is our following work.

[9]R.Mehmed, F.Comeau, W.Phillips,and N.Aslamet.al[2021]:It used Void Avoidance Opportunistic Routing Protocol. In this paper, we propose EEDOR-VA, avoid avoidance protocol. In addition, EEDOR-VA improves the reliability of the network by detecting void/ trapped nodes in advance of data transmission using the hop count discovery process. It also reduces the number of nodes that actually transmit the data packets by using *Rank* to distinguish between node holding times. This approach helps to decrease the energy expenditure in the data transmission process as well as packet collision and its associated cost. The analyses of experimental simulation results show that EEDOR-VA enhances network performance in terms of energy consumption, packet delivery ratio and the number of nodes that actually complete the transmitting process. We further analyzed the impact of single and multiple sinks as well as two different sink deployment techniques on the EEDOR-VA performance in terms of total energy consumption and PDR.

[10]K.M.Awan,P.A.Shah,K.Iqbal,S.Gillani,W.Ahmad,andY.Nam[2019]:It had used the mobile computing. In this paper, we have discussed several techniques of underwater sensor networks. The objective of the reviewed techniques is to overcome the underwater challenges and to give directions to future researchers. Also, we presented

a vibrant view to academic by providing a base for a better solution. In this perspective, we have presented future directions which are still not yet explored in this research area. Therefore, routing and media access control protocols need to design by taking care of maximizing channel utilization. AGPS like localizations achemis still not created for underwater sensor networks and localization of a freely moving node is still an open area for research.

[11]M.Ali,A.Khan, K.Aurangzebetal et.al[2019]:This research states that Persistence operation of UA-WSNs needs scrutiny due to its applications, uniqueness, challenges, and difficulties. Applications like sub-marine detection and navigation, surveillance, marine animal imaging, oil spill detection, pollution monitoring, etc. The proposed SiM-RPO and CoSiM-RPO algorithms are presented for the reliable and persistence operation of the network. The proposed SiM-RPO and CoSiM-RPO algorithms are presented for the reliable and persistence operation of the network. For the MSs' path determination, the network is split into four equal squares. To cover all the network and collect more information, the triangular paths are defined for the MSs.

[12]X.Du,Z.Zhou,Y.Zhang,andT.Rahmanet.al[2020]:Here we can see about the *I*nternet *o*f *T*hings(*IoT*) networks have become the infrastructure to enable the detection and reaction of anomalies in various domains, where an efficient sensory data gathering mechanism is fundamental since *IoT* nodes are typically constrained in their energy and computational capacities. This paper proposes an energy-efficient sensory data gathering mechanism. Specifically, sensory data are encoded into binary category data in *IoT* nodes, and then they are routed to their corresponding edge nodes through a routing tree. This paper proposes an energy-efficient sensory data gathering mechanism. Specifically, sensory data are encoded into binary category data in *IoT* nodes, and then they are routed to their corresponding edge nodes through a routing tree.

[13]S.Rani,S. H.Ahmed,J.Malhotra,andR.Talwaret.al[2017]:This paper proposes about to explore the vast ocean, internet of underwater things has become the most attractive area of research. Underwater Smart things are deployed to facilitate the discovery of unexplored regions of ocean. In recent past, various protocols have been proposed for energy efficient routing (Anon, 2016) in underwater WSNs. UWSNs have many constraints like packet delivery, energy efficiency, timely delivery etc. Due to the seconds traints , E2E routing is assumed as most time consuming.

[14]Pompili,D.,Melodia,T.,Akyildiz,I.Fet.al[2012]:Here we can see about Underwater sensor networks will find applications in oceanographic data collection, pollution monitoring, offshore exploration, disaster prevention, assisted navigation, and tactical surveillance. Underwater acoustic networking is the enabling technology for these applications. The problem of data gathering in a three-dimensional underwater sensor network was investigated, by considering the interactions between the routing functions and the underwater acoustic physical channel. A resilient routing solution tailored for long-term critical monitoring missions was proposed. The problem of data gathering in a three-dimensional underwater sensor network was investigated, by considering the interactions between the routing functions and the underwater acoustic physical channel.

[15]Timothy K Buen nemeyer Randy C .Marchany, JosephG.Trontet.al[2007]:This paper describes a unique Battery-Sensing Intrusion Protection System (B-SIPS)for mobile computers, which alerts on power changes detected on small wireless devices, using an innovative Dynamic Threshold Calculation algorithm. B-SIP Sen abled hosts are employed as sensors in a wireless network and form the basis of the intrusion detection system (IDS). The concept of employing battery constraints as a means of intrusion detection is a relatively new capability that was only recently made possible by developments in smart battery and ACPI technologies. The concept of employing battery constraints as a means of intrusion detection is a relatively new capability that was only recently made possible by developments in smart battery and ACPI technologies.

[16]Monica Curti, Alessio Merlo†, Mauro Migliardi, Simone Schiappacasse et.al[2013]:

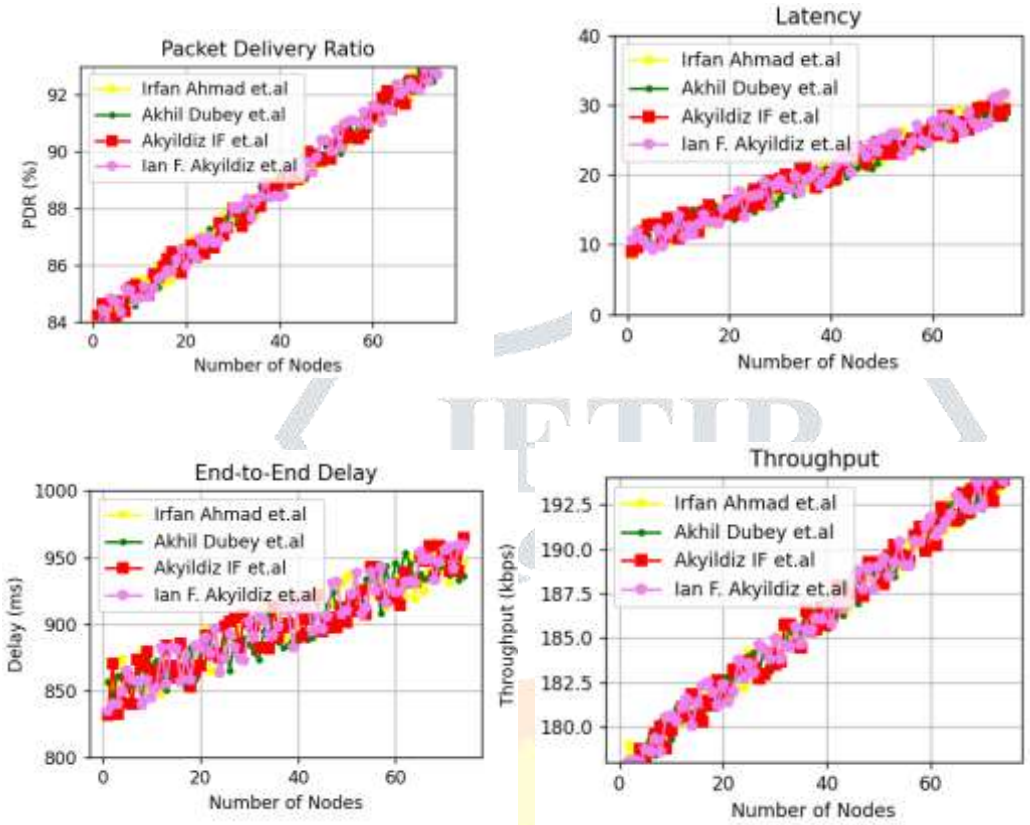
This paper investigates the correlations between the energy consumption of Android devices and the presence of threats (e.g. battery-drain attacks). In particular, this paper proposes a model for the energy consumption of single hardware components of a mobile device during normal usage and under attack. In this paper, we have defined a road-map to energy-aware security and we have developed a specific use case to test our idea of energy-aware detection of attacks on mobile devices. In particular, we have discussed how to model energy consumption in Android devices in order to get the precise consumption of hardware components. At present, most of the research projects dedicated to the study of energy consumption on mobile devices are focused on power saving, while none(to the best of our knowledge).

[17]AlsirhaniandKhanet.al: In this paper we can see about Blockchain-enabled Internet of Things(IoT) envisions a world with rapid development and implementations to change our everyday lives based on smart devices. These devices are attached to the internet that can communicate with each other without human interference. A spam DIS attack is one of the energy depletions attacks in which a malicious node generates multiple fictitious identities and sends a DIS request to increase the transmission process in the network and thus depletes the battery of the nodes. We compare energy consumption in an original RPL, DIS attack, and under the DISAM states. Simulation results show that the attacking state consumes more energy than the normal state, and under DISAM, slightly more energy is consumed.

[18]L. LIU,S.ZHOUANDJ.-H. CUIet.al [2008]: This paper is about, In the last several years, underwater sensor network (UWSN) has found an increasing use in a wide range of applications such as coastal surveillance systems, environmental research, autonomous underwater vehicle (AUV)operation, to name a few [1–4]. By deploying a

distributed and scalable sensor network in a three-dimensional underwater space, each underwater sensor can monitor and detect environmental parameters and events locally. Based on the discussion in previous sections, we have the following summary points .Up to date and extending to the near future, acoustic waves will be staying as the major carrier of wireless communication in UWSNs. Up to date and extending to the near future, acoustic waves will be staying as the major carrier of wireless communication in UWSNs.

4.Results:



5.Conclusion:

In the finalization of this study on the detection of energy drain attacks in underwater sensor networks, obviously, security perspectives for the senet works are of importance. This is because they have very important applications in environmental monitoring, underwater surveillance, and resource exploration. Due to their specific features, such as limited bandwidth, high latency, and the harsh underwater environment, UWSNs present many challenges for implementing the traditional mechanisms that provide security. Energy drain attacks have huge impacts on the stability and lifetime of a sensor network. Effective detection mechanisms need to address these constraints through monitoring energy consumption patterns, anomaly detection, and lightweight cryptographic methods. In such lines, the present study proposes a hybrid approach that combines anomaly detection and trust management to detect and mitigate energy drain attacks. The results of the simulation for this approach were given, showing the effectiveness of the method in detecting attacks with very few false positive responses, hence improving the network resilience and operational lifetime of the sensor nodes. In the near future, there is a need for research work aimed at improving the scalability and robustness of the detection mechanisms; this could be done by integrating possibly machine learning techniques and coming up with adaptive algorithms necessary to implement a successful intrusion detection system.

References:

1. 1.Ahmad,I.,Rahman,T.,Zeb,A.,Khan,I.,Ullah,I.,Hamam,H.,&Cheikhrouhou,
2. O. (2021). Analysis of security attacks and taxonomy in underwater wireless sensor networks. *Wireless CommunicationsandMobileComputing*,*2021*(1), 1444024.
3. Dubey,A.,Jain,V.,&Kumar,A.(2014).Asurvey in energy drain attacks and their counter measures in wireless sensor networks. *Int. J. Eng. Res. Technol*, *3*(2), 1206-1210.
4. 3Akyildiz,I.F.,Pompili,D.,&Melodia,T.(2004).Challenges for efficient communication networks. *ACM Sigbed Review*, *1*(2),3-8.
5. Patibandla, R. S. M. L., Rao, B. T., Narayana, V. L., & Srinivas, V. S. (2021). An overview of ontology-based artificial intelligence services in health care systems. In Proceedings of the International Conference on Health Care Systems (pp. 47–63).
6. Maddumala, V. R., Maha Lakshmi, K., Anusha, P., & Lakshman Narayana, V. (2020). Enhanced morphological operations for improving the pixel intensity level. Journal of Computational and Theoretical Nanoscience, 29(3), 9191–9201.

7. Narayana, V. L., Malleswari, K. S. N., Divyanjali, M., Nandini, S., & Purnima, G. (2023). Video frame based prompt compression model with steganography for secure data transmission. In Proceedings of the International Conference on Advanced Intelligent Systems (pp. 373–377). https: // doi .org /10.1109/ ICAIS56108. 2023.10 073883
8. Naresh, A., Pavani, V., Meghana Chowdary, M., & Lakshman Narayana, V. (2020). Energy consumption reduction in cloud environment by balancing cloud user load. Journal of Critical Reviews, 7(7), 1003–1010. https://doi.org/10.31838/jcr.07.07.184
9. Patibandla, R. S. M. L., & Vejendla, L. N. (2022). Significance of blockchain technologies in industry. In Advances in Blockchain Technologies (pp. 19–31). https://doi.org/10.1007/978-3-030-70501-5_2
10. Pasala, S., Pavani, V., Lakshmi, G. V., & Narayana, V. L. (2020). Identification of attackers using blockchain transactions using cryptography methods. Journal of Critical Reviews, 7(6), 368–375. https://doi.org/10.31838/jcr.07.06.65
11. Mounika, B., Anusha, P., Narayana, V. L., & Lakshmi, G. V. (2020). Use of blockchain technology in providing security during data sharing. Journal of Critical Reviews, 7(6), 338–343. https://doi.org/10.31838/jcr.07.06.59
12. Narayana, V. L., Vinayaki, K. V., Swetha, P. A., Sri, K. D., & Chaithanya, G. (2024). Superior attribute weighted set for object skeleton detection using ResNet50 with edge-based segmentation model. In Proceedings of the International Conference on Smart Computing and Systems (pp. 1132–1139). IEEE. https:/ /doi.org /10.1 109/ICSC SS6 0660.2024.10624879
13. Gopi, A. P., & Naik, K. J. (2022). An IoT model for fish breeding analysis with water quality data of pond using modified multilayer perceptron model. 2022 International Conference on Data Analytics for Business and Industry (ICDABI), 448-453. https://doi.org/10.1109/ICDABI56818.2022.10041617
14. Arepalli, P. G., & Naik, K. J. (2024). A deep learning-enabled IoT framework for early hypoxia detection in aqua water using lightweight spatially shared attention-LSTM network. Journal of Supercomputing, 80(2), 2718-2747. https://do i.org/10.100 7/s 112 27-023-05580-x
15. Arepalli, P. G., & Naik, K. J. (2023). An IoT-based water contamination analysis for aquaculture using lightweight multi-headed GRU model. Environmental Monitoring and Assessment, 195(12), Article 1516. https://doi.org/10.1007/s10661-023-12126-4
16. Gopi, A. P., Gowthami, M., Srujana, T., Gnana Padmini, S., & Durga Malleswari, M. (2023). Classification of denial-of-service attacks in IoT networks using AlexNet. In Smart Innovation, Systems and Technologies (Vol. 316, pp. 349-357). https://doi.org/10.1007/978-981-19-5403-0_30
17. Bikku, T., Gopi, A. P., & Prasanna, R. L. (2019). Swarming the high-dimensional datasets using ensemble classification algorithm. In Advances in Intelligent Systems and Computing (Vol. 815, pp. 583-591). https://doi.org/10.1007/978-981-13-1580-0_56
18. Arepalli, P. G., & Khetavath, J. N. (2024). Water quality classification using multi-cell RNN in aquaculture ponds for Catla fish. In Lecture Notes in Networks and Systems (Vol. 897, pp. 363-370). https://doi.org/10.1007/978-981-99-9704-6_34
19. Arepalli, P. G., & Naik, K. J. (2024). Water contamination analysis in IoT-enabled aquaculture using deep learning-based AODEGRU. Ecological Informatics, 79, Article 102405. https://doi.org/10.1016/j.ecoinf.2023.102405
20. Arepalli, P. G., & Naik, K. J. (2024). An IoT-based smart water quality assement framework for aqua-ponds management using Dilated Spatial-temporal Convolution Neural Network (DSTCNN). Aquacultural Engineering, 104, Article 102373. https://doi.org/10.1016/j.aquaeng.2023.102373
21. Gopi, A. P., Narayana, V. L., & Kumar, N. A. (2018). Dynamic load balancing for client-server assignment in distributed systems using genetic algorithm. Ingenierie des Systemes d'Information, 23(6), 87-98. https://doi.org/10.3166/ISI.23.6.87-98
22. Sarada, K., Narayana, V. L., Gopi, A. P., & Pavani, V. (2020). An iterative group based anomaly detection method for secure data communication in networks. Journal of Critical Reviews, 7(6), 208-212. https://doi.org/10.31838/jcr.07.06.39
23. Narayana, V. L., Gopi, A. P., & Chaitanya, K. (2019). Avoiding interoperability and delay in healthcare monitoring system using blockchain technology. Revue d'Intelligence Artificielle, 33(1), 45-48. https://doi.org/10.18280/ria.330108
24. Gopi, A. P., Jyothi, R. N. S., Narayana, V. L., & Sandeep, K. S. (2023). Classification of tweets data based on polarity using improved RBF kernel of SVM. International Journal of Information Technology, 15(2), 965-980. https://doi.org/10.1007/s41870-019-00409-4
25. Narayana, V. L., Gopi, A. P., Khadherbhi, S. R., & Pavani, V. (2020). Accurate identification and detection of outliers in networks using group random forest methodology. Journal of Critical Reviews, 7(6), 381-384. https: //doi.org/ 10.31838/ jcr.07.06.67
26. Rao, B. T., Patibandla, R. S. M. L., Narayana, V. L., & Gopi, A. P. (2021). Medical data supervised learning ontologies for accurate data analysis. In Semantic Web for Effective Healthcare Systems (pp. 249-267). http s://doi. org/10.10 02/9 7811 19764 175.ch11
27. Patibandla, R. S. M. L., Gopi, A. P., Narayana, V. L., & Rao, B. T. (2023). Decentralized smart healthcare systems using blockchain and AI. In Blockchain applications in healthcare: Innovations and practices (Vol. 1,

pp. 139-154). DOI: 10.1002/9781394229512.ch8
28. Rani, B. M. S., Majety, V. D., Pittala, C. S., Vijay, V., Sandeep, K. S., & Kiran, S. (2021). Road Identification Through Efficient Edge Segmentation Based on Morphological Operations. Traitement du Signal, 38(5).
29. Kanumalli, S. S., Ch, A., & Murty, P. S. R. C. (2020). Secure V2V Communication in IOV using IBE and PKI based Hybrid Approach. International Journal of Advanced Computer Science and Applications, 11(1).
30. Chaitanya, Kosaraju, and Sankara Narayanan. "Security and Privacy in Wireless Sensor Networks Using Intrusion Detection Models to Detect DDOS and Drdos Attacks: A Survey." 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2023.
31. Krishna, Komanduri Venkata Sesha Sai Rama, et al. "Classification of Glaucoma Optical Coherence Tomography (OCT) Images Based on Blood Vessel Identification Using .CNN and Firefly Optimization." Traitement du Signal 38.1 (2021).
32. Chaitanya, Kosaraju, et al. "Predicting the Spread of Covid Disease Based on Chest X-Ray Images Using Convolutional Neural Network with Improved Accuracy." 2023 6th International Conference on Advances in Science and Technology (ICAST). IEEE, 2023.
33. Ekkurthi, A., Sujatha, V., Kumar, K.V.,"Effective Moving Object Tracking Using Adaptive Background Subtraction with Advanced Probability Evolutionary Algorithm",International Journal on Recent and Innovation Trends in Computing and Communication, 2023, 11, pp. 1–3
34. Sujatha, V., Yaddala, M., Kollipara, V., Shaik, K., Burri, R.K(23),"Movie reviews data classification using convolution neural networks",AIP Conference Proceedings. 2023, 2724, 030009
35. Godavarthi, B., Majety, V. D., Mrudula, Y., & Nalajala, P. (2019). Fault identification in power lines using GSM and IoT technology. Advances in Intelligent Systems and Computing, 815, 647–655. https://doi.org/10.1007/978-3-319-91117-2_70
36. Majety, V. D., & Murali, G. (2018). A remote epileptic patient supervising system. Advances in Modelling and Analysis B, 61(4), 207–210. https://doi.org/10.18280/ama_b.610402
37. Naresh, A., TSLP, H., Ch, G., & Kumari, G. R. P. (2023, July). Early Prophecy of Low-Birth-Weight Babies Using BM Error Rate Classifier. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
38. Kumari, G. R. P., Reddy, A. H., Lakshmi, K., Abhinaya, B., Sanjana, S., & Naresh, A. (2024, March). Time-Frame-Based Drowsiness Detection System Using CNN. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 711-716). IEEE.
39. V. Pavani, K. Divya, V. V. Likhitha, G. S. Mounika and K. S. Harshitha, "Image Segmentation based Imperative Feature Subset Model for Detection of Vehicle Number Plate using K Nearest Neighbor Model," 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2023, pp. 704-709, doi: 10.1109/ICAIS56108.2023.10073848.
40. V. Pavani, M. N. Swetha, Y. Prasanthi, K. Kavya and M. Pavithra, "Drowsy Driver Monitoring Using Machine Learning and Visible Actions," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 1269-1279, doi: 10.1109/ICEARS53579.2022.9751890.
41. Sri, Kurra Santhi, et al. "Advanced system control with traffic handling for secure communication in IoT routing protocol." Journal Européen des Systèmes Automatisés 54.2 (2021): 229-233.
42. Arumugham, Vinothini, et al. "An explainable deep learning model for prediction of early‐stage chronic kidney disease." Computational Intelligence 39.6 (2023): 1022-1038.
43. Majety, Vasumathi Devi, et al. "Enhanced secure communication AODV routing protocol using SVM in MANETS." AIP Conference Proceedings. Vol. 2724. No. 1. AIP Publishing, 2023.
44. Krisha, P.S., Peram, S.R. (2023). CT image precise denoising model with edge based segmentation with labeled pixel extraction using CNN based feature extraction for oral cancer detection. Traitement du Signal, Vol. 40, No. 3, pp. 1297-1304. https://doi.org/10.18280/ts.400349
45. P. S. Krishna, V. R. Aparna, V. Priyanka, P. T. Niharika and T. Shivangi, "Convolution Neural Network Model with Feature Linked Vector for Oral Cancer Detection," 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 2023, pp. 304-308, doi: 10.1109/CSNT57126.2023.10134660.
46. Eswaraiah, Rayachoti, Tirumalasetty Sudhir, and Prathipati Silpa Chaitanya. "Curvelet transform based watermarking for telemedicine." Wireless Personal Communications 122.1 (2022): 309-329.
47. Varshini, Y., Mounika, T., Kumari, G. R. P., Sirisha, G., & Deepthi, Y. (2023, March). Crop Yield Forecast Using Machine Learning. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2310-2315). IEEE.
48. B. Aruna Kumari "Time Series Data Classification for Precise Stock Market Price Prediction using ML" ICICACS International Conference on Integrated Circuits and Communication Systems, Scopus indexed, ISBN:979-8-3503-1755-8/ https://ieeexplore.ieee.org/document/10498248,18 April 2024
49. B.Aruna Kumari "HumanvAction Recognition From Video Frames Using Recurrent Neural Networks" ICDT 2nd International Conference on Disruptive Technologies (ICDT),Scopis indexed , ISBN:979-8-3503-7105-5/ https://ieeexplore.ieee.org/document/10489658, 11 April 2024

50. Akyildiz, I. F., & Kasimoglu, I. H. (2004). Wireless sensor and actor networks :research challenges. *Ad hocnetworks*, *2*(4),351-367.
51. Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005, May). The feasibility oflaunching and detecting jamming attacks in wireless networks. In *Proceedings of the6th ACM international symposium on Mobile ad hoc networking and computing* (pp.46-57).
52. Misra, S., Krishna, P. V., Abraham, K. I., Sasikumar, N., & Fredun, S. (2010).An adaptive learning routing protocol for the prevention of distributed denial ofservice attacks in wireless mesh networks. *Computers & Mathematics with Applications*, *60*(2),294-306.