International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.033 ISSN: 2581-4621

A Novel Security Framework: Trust based routing for Wireless Sensor Network

M.Raju[1], Dr.K.P.Lochanambal[2]
[1]Research Scholar, Government Arts College Udumalpet, Assistant Professor Sri Krishna Arts and Science College
[2] Assistant Professor, Government Arts College, Udumalpet
Orchid ID: 0009-0009-0909-3403

ABSTRACT
Nowadays technology is growing very rapidly. The devices are becoming wireless. The telephones are gradually replaced by the mobile and wires are replaced by wireless devices. Even though there is advancement in technology, threats to security are also increasing. Since the medium is wireless, chances of eavesdropping is more and there is security issue of information being transmitted over wireless medium. The nodes can be compromised. The limitations of the nodes are low capacity of storage and lesser battery life. Hence, the security of the data being transmitted on the wireless medium is a serious concern. Because the information that is being transmitted over wireless medium is more vulnerable for attacks. Here, the problem of security and privacy related to the information, that will be passed through the mediatory nodes is considered. Hence a model is proposed to address the problem and solution based on certain considered parameters. Here, we have proposed a model to categorize the nodes into safe and unsafe.

Keywords: Safe Node, Cluster Head, Moderate Node, EDISP

1. Introduction

A cyber threat associates with identifying fraud, intended extortion, loss of critical information such as family photographs. It seeks to influence and demolish sensitive data, extort user cash and disrupts their regular business operations. In today's interconnected culture, everybody profits from innovative data security strategies. Cyber threat relates to the body of techniques, procedures and strategies designed to avoid malicious access to the systems, computers and software's [1]. Incorporating efficient security protocols is exceptionally difficult today as there are numerous computer systems than humans and hackers have become more inventive.

A substantial chunk of the information could be confidential detail, be it personal capital, financial records, private details or other data forms for which security breach or disclosure may have negative repercussions [3]. In the course of business operations, companies transfer classified information through networks and to various machines and cyber safety encompasses the practice devoted to securing that data and the devices used to analyze and manage that content. When the frequency and complexity of cyber-threats increase, businesses and organizations, particularly those dealing with data protection associated with nationwide protection, healthcare, or banking data, need to intervene to safeguard their classified company and personal records.

Internet of things has brought an evolution in the technology. It guarantees that every device can be made to be connected to the network. Such a network may be connection oriented or connection less. Any device that is smart in nature and has a capability to sense the data, can be made as a part of the network. A device is said to be smart if it has a capability to sense the signal, process the input and produce the output after processing [1]. Whenever such smart devices are connected through the wireless medium, then there arises a problem of security. Securing the nodes and the data which is transmitted over the wireless medium is a challenging field of research. So, here we are proposing a technique which is based on the cuckoo search algorithm. Cuckoo technique searches [2] a best possible nest for laying its eggs. It classifies the nest as safe and unsafe based on criteria or attributes. It discards the unsafe nests and lays eggs in the safe nests. Similarly our proposed method classifies the nodes as safe and unsafe based on the attributes. There are a total of 18 attributes which can be considered. Only the top 3 are put to use in this paper because these can suffice to ensure safety. Those attributes which are considered for categorizing the nodes are Trust/Security level of a node, Storage Capacity of the node (Based of buffer level) and Battery level of a node.

The basic understanding of the arrangements of the nodes in the WSN is very much essential in order to understand the proposed model [3]. Following figure 1 shows details of the node and figure 2 shows the architecture of Wireless Sensor Network (WSN).

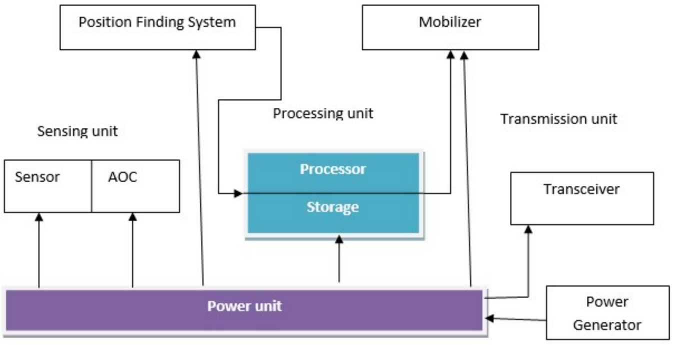


Fig. 1. A typical WSN Node and its components

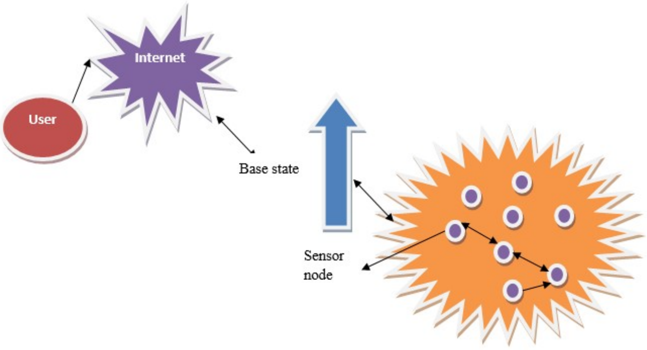


Fig. 2. Architecture of Wireless Sensor Network (WSN)

2. Related work

Each node in the WSN Network has independent decision-making capacities to decide the next transmission node, transmission time, receiving moment etc. However, owing to a heterogeneous form of data packet occurrence on the node at any stage, these are restricted by ongoing decision-making processes from the various devices in the IoT. Node security is a challenge as it is marked by restricted physical security in relation to transferring data in wireless media that are susceptible to and viewed by several hackers. These hackers attempt to infect the other nodes that cause traffic congestion, stop or deny the customer the sort of service. The network ultimately sticks and collapses. Significant research has been carried out in this problem, several of which have been researched and results submitted in this chapter. The papers provided a study of the various kinds of intruding, the nature of assaults and the obvious answers from the nodes. Special emphasis was given in this job on the sort of assault that configures the routing characteristics. The literature has provided a technique to improve the impact of assaults by enhancing general web output [4][5]. This occurs however at the expense of losing packages that are not quite appropriate for certain apps. The literature reveals important quantities of watch dogs who constantly monitor the network for any change in the behaviour of nodes from the optimal design [6]. Various works linked to intrusion detection, both monitored and uncontrolled teaching techniques, have been suggested in the literature. Bayesian models have been used efficiently in hybrid solutions for modeling IDS schemes and other optimization techniques [7]. The standard techniques include tree-based decision-making [8], which is discovered to be very easy in building but improves complexity as the volume of the information being processed and the volume of the network goes beyond some threshold [9]. Conventional classifiers, such as SVM [10], were carefully discussed and used in combined with principal component analysis (PCA) [11 – 13], in order to decrease the vector set dimension. Clustering techniques have been commonly used in literature, either with stand-alone methods or together with optimisation algorithms for the Optimisation of Cluster Heads (CHs) which perform an important part in transmitting data from one node to another [14] [15]. Neural networks were also used to train the network against sample information on standard assaults. They provide a good answer to attaining the required objective, but they are not very stable in the face of freshly established intrusions.

3. Issues and challenges

Wireless Sensor Network (WSN) is a dynamic in nature. Any device can join and leave the network. Authentication is major concern. Self - management, hardware and software issues, operating systems, providing QoS, data collection and transmission are some of the challenges in the WSN[16]. Energy conservation in one of the most important aspect as far as hardware and software related designs are concerned. Secure data collection and transmission with the minimum communication and computation cost is another software related challenge17]. Security calculation has to be as simple as possible to reduce the power usage and for optimal bandwidth utilization [18][19]. So, we have proposed a model to address such issues.

4. Proposed model

Similar to the cuckoo search based algorithmic techniques have been incorporated in to the proposed model. As cuckoo searches for the best nest to lay its eggs, similarly our job in proposed model is to search the secure nodes in the cluster which can be used for routing purpose. The nodes can be divided as safe, unsafe and moderate nodes. Safe nodes will always be part of the routing path. Moderate nodes will be used only in case of emergency. Proposed model has following steps.

4.1. Choosing Cluster Head

The cluster head is elected on the basis of ratio of number of requests successfully completed to the number of requests received.

$$\text{Node}_{\text{val}} = \frac{\text{No. of requests successfully completed}}{\text{No. of requests received.}}$$

$$\text{Node}_{\text{val}} = \frac{\text{Request}_{\text{Complete}}}{\text{Request}_{\text{Received}}}$$

A node with highest Nodeval value will be chosen as the cluster head in each cluster i.e., Node_{CH}. Following figure 3 shows the details.

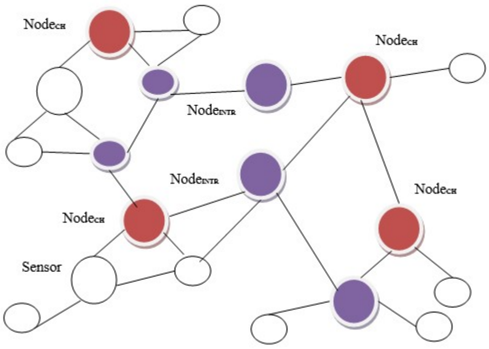
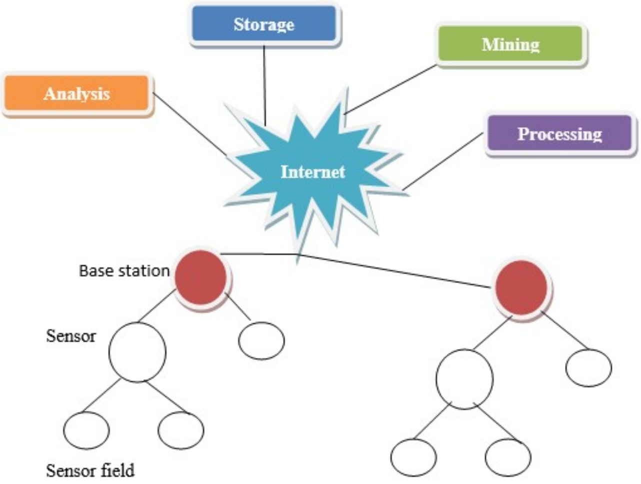


Fig. 3. Choosing the Cluster Head



The routing tables and attribute (security, battery and storage) level values of each node are stored in the $Node_{CH}$ that is cluster head. Our proposed model proposes for cloning of the cluster head in another node whose $Node_{val}$ is more than defined threshold value and is an intermediate node between two clusters that is $Node_{INTR}$. In case of failure of the$Node_{CH}$, the $Node_{INTR}$ will continue to work as the cluster head. This provides the robust system. The figure 4 shows the details of the cluster head and cloned node (Intermediate Node., $Node_{INTR}$)

The figure 4 shows the proposed model. The figure depicts the steps involved in the proposed model. As soon as the cluster head id chosen, attributes are calculated and checked against the respective threshold values. Later the process of marking the nodes as safe, unsafe and moderate nodes takes place. The details will stored in the Cluster Head, so that routing process can be made easier and secure.

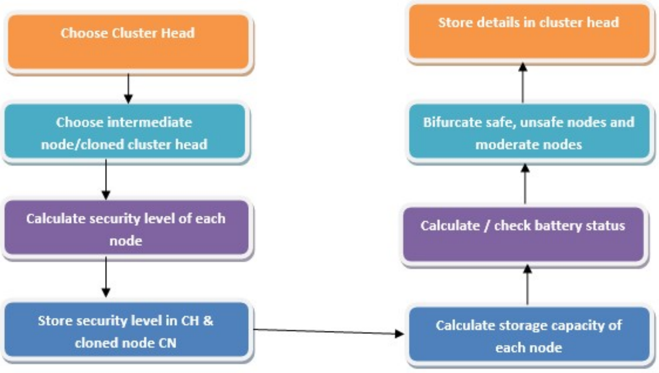

Choose Cluster Head
Choose intermediate node/cloned cluster head
Calculate security level of each node
Store security level in CH & cloned node CN
Calculate storage capacity of each node
Calculate / check battery status
Bifurcate safe, unsafe nodes and moderate nodes
Store details in cluster head

Fig 4. Proposed model

4.2. Calculating security levels of each node

The security level is required to decide whether the node is trustable or not. The trustable nodes will be used for routing. The algorithm for calculating the security level is given below.

Algorithm:

```
Step 1: Calculate treatment ratio a below
    $r = 1-\sqrt{12L(N-L)} \div (NH)N2$
    L→ Number of packets correctly transmitted by the sensor node.
    N→ Total Number of packets transmitted.
Step 2: Calculate trust
    $t = L \div N$
Step 3: if t> 0.9, mark node as trustworthy and store score in Cluster Head (CH).
Step 4: Repeat steps 1 to 3 until all nodes are over.
```

4.3. Calculating storage capacity of the Node

This will help in avoiding dropping of packets. If storage is not there in buffer then packets will be dropped and this leads to retransmission and wastage of bandwidth. Hence, we have to check the Storage status of the node under observation.

```
Algorithm:
   Step1: Free space = Buffer space – Occupied space.
          Fspace=Bspace-Ospace.
          If Fspace>Tspace       Tspace--- Threshold space value
                Mark node as accepted.
                Store values in Cluster Head, $Node_{CH}$.
          Else
                Mark node as rejected.
   Step2:  Repeat step 1 until all nodes are over.
   Step3:       Stop
```

4.4. Calculate battery status of the node.

This is one the important attribute to be considered. If the node with lower battery switches off then this will break the routing path and which will lead to the creation of new path, rerouting and retransmission of the packets. There will be huge wastage of bandwidth. This will drastically affect the performance of the WSN. Following algorithm helps to calculate the battery level.

```
Algorithm:
   Step 1: Calculate
          $E_{TR}= (C_{CKT} * N_B) + E_{DISP} + Dist^2$
          $R_E= (C_{CKT} * N_B)n$
          $C_{AGGR}= (C_{CKT} * N_B* n)$
Where, ETR→Transmitter cost, EDISP→ Energy Dissipation for the transmission amplifier
$C_{CKT}$→ Energy consumption to run the transmitter circuit.
$N_B$→ Number of bits transmitted, $C_{AGGR}$→ Cost of data aggregation
Dist→Distance to be travelled
Step 2: Check If $E_{TR}+ C_{CKT}> T_{TR}+ T_{CKT}$then
Mark the node, update values in CH and store its values in node.
Else then
Unmark the node
(Here$T_{TR}$and$T_{CKT}$are standard experimental values here taken as threshold valuesElse)
   Step 3: Repeat step 1 to 2 until all node in cluster are over.
```

Once the Cluster Head, Node$_{CH}$ has the attributes values for security level (which indicates the trust of a node), storage capacity and battery status of each node stored in the Node$_{CH}$. If there is any change in the values of chosen attributes, the same has to be updated to Node$_{CH}$ periodically. This is help in knowing the exact status of the nodes. This will lead to the better and error free, secure routing.

Figure 5 shows the details of how to mark the nodes and the criteria that has to be followed. A new marking strategy is proposed as moderate which takes values just below the permissible range of the threshold values.

The following table shows the details.

S. No	Safe	Unsafe	Moderate
1	1	0	0/1

Table 1. Non-binary values

The marking of the non-binary pattern of the nodes lead to the creation of the new level called 'moderate'. This is modified version of the binary algorithm where there were only two values as safe ('1') and unsafe ('0'). These moderate nodes play sometimes the crucial role during emergency.

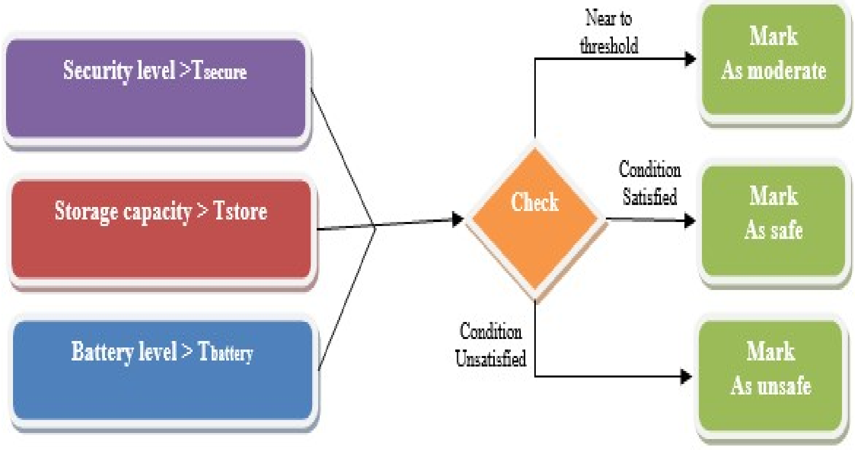


Fig. 5. Marking of nodes according to attribute levels

Marking of a node will be done on the Cuckoo algorithm criteria, we use binary variant of algorithms. Based on the values of security level or trust of node, storage capacity and battery status, we apply the following criteria.

Algorithm:

```
    Step 1: Calculate $T_{sum}= T_{Secure}+T_{Battery}+T_{space}$
If $T_{sum} \geq$ Threshold then
Mark the node as $N_{safe}$.
Step 2: If $T_{sum} \geq T_{Threshold}$ + Adjust factor
    And $T_{sum}$+ Adjust factor ≥ Threshold Then
    Mark the node as $N_{moderate}$.
Step 3: if $T_{sum}<$ Threshold then mark the node as $T_{unsafe}$.
Step 4: Stop.
```

Now the nodes in each cluster are marked. For routing N_{safe}nodes are considered. In case of emergency $N_{moderate}$can also be considered.

The following table shows the details of choosing nodes based on attribute values.

Sl. No	Security level (T_{secure})	Buffer Status (T_{space})	Battery Level ($T_{battery}$)	Marking
1	Yes	Yes	Yes	Safe
2	No	Yes	Yes	Unsafe
3	No	No	Yes	Unsafe

Table 2. Marking nodes

5. Experimentation

Most of the sensor networks face the power related problems. A detailed simulation based experimentation is carried out to produce following results and charts. Figure 6 shows the WSN at work. It shows the nodes that are marked based on the attributes we have considered to mark the number nodes.

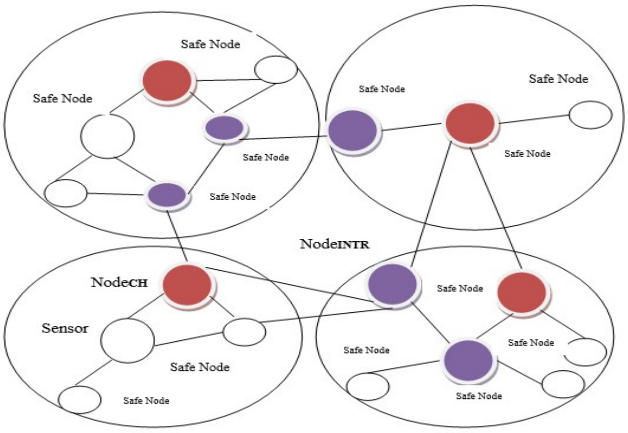


Fig. 6. Marking of Nodes as safe and unsafe nodes

After running the model, it is observed that the performance of the system is enhanced due to the proposed model. The following chart shows the comparison of the details.

Sl No.	No. of Nodes	Performance of Existing system in percentage	Performance of proposed system in percentage
1	10	100.00	100.00
2	50	98.33	100.00
3	100	95.23	100.00
4	500	90.83	99.12
5	1000	86.6	98.87
6	>1000	84.44	97.78

Table 3. Performance analysis

The following figure shows the chart for the above results. It is clearly observed that the proposed system performs better even when the numbers of nodes are increased.

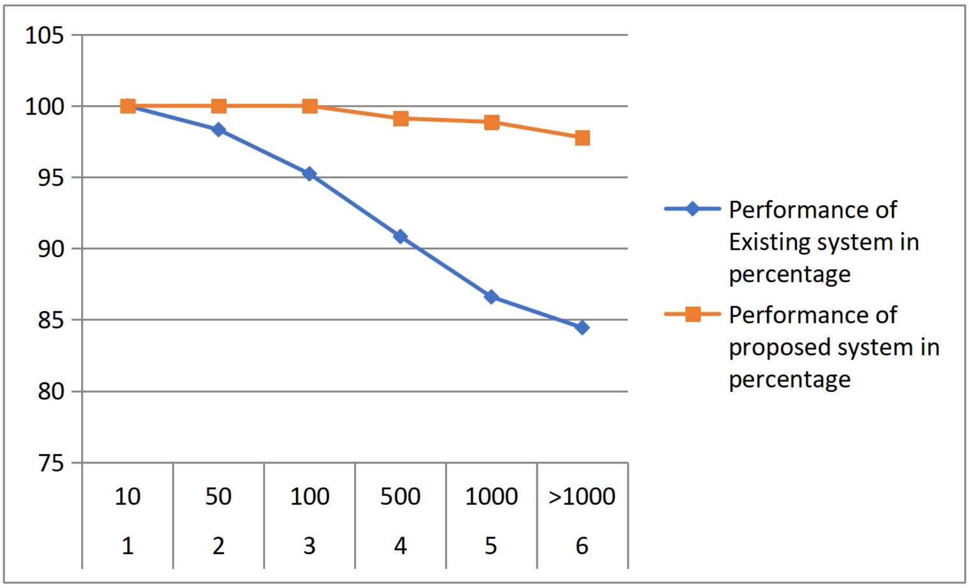


Fig. 7. Chart showing the Performance Analysis.

It is clearly visible from the chart that the performance of the existing system deteriorates as the number of nodes in the network increases. But the performance of the proposed system is considerably better than the existing system.

6. Conclusion and future work

The performance of the proposed system is better even when the number of nodes is considerably high as compared to the existing systems. Here, in the proposed model only top three attributes, out of 18 identified attributes are considered. Further, our intention was to reduce the calculation as much as possible in order to reduce the burden on the nodes, so we chose top 3 attributes only.

As an enhancement to the proposed system, we can try to add some more attributes to the proposed system. Further, clustering algorithms for event monitoring can be also added to the proposed system to enhance the worthiness of the system.

References

1. Sastry N., and Wagner D., 2004. Security considerations for IEEE 802.15.4 networks. In Proceedings of ACM workshop on Wireless security.

2. Bisdikian, C. 2001. An overview of the Bluetooth Wireless technology. IEEE Communication Magazine, vol. 39.

3. Ezhilarasi, M., et al. "A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks." Soft Computing 27.7 (2023): 4157-4168.

4. Saravana Kumar, N. M., S. Deepa, C. N. Marimuthu, T. Eswari, and S. Lavanya. "Signature based vulnerability detection over wireless sensor network for reliable data transmission." Wireless Personal Communications 87 (2016): 431-442.

5. Ngai ECH, Liu J, Lyu MR. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Computer Communications 2007; **30** (11-12): 2353–2364.

6. Ezhilarasi, M., Krishnaveni, V. (2020). A Novel Paradigm Towards Exploration of Rechargeable WSN Through Deep Learning Architecture for Prolonging Network Lifetime. In: Kumar, L., Jayashree, L., Manimegalai, R. (eds) Proceedings of International Conference on Artificial Intelligence, Smart Grid and Smart City Applications. AISGSC 2019 2019. Springer, Cham. https://doi.org/10.1007/978-3-030-24051-6_87

7. Pawar, S. N. "Intrusion detection in computer network using genetic algorithm approach: a survey." International Journal of Advances in Engineering & Technology 6.2 (2013): 730-736.

8. Tahir, S., Bakhsh, S. T., & Alsemmeari, R. A. (2019). An intrusion detection system for the prevention of an active sinkhole routing attack in Internet of things. International Journal of Distributed Sensor Networks, 15(11), 1550147719889901.

9. Li, Xuanang, et al. "PSAP-WSN: a provably secure authentication protocol for 5g-based wireless sensor networks." CMES-Computer Modeling in Engineering & Sciences 135.1 (2023): 711.

10. Munusamy, Nagarajan, Sneha Vijayan, and M. Ezhilarasi. "Role of Clustering, Routing Protocols, MAC protocols and Load Balancing in Wireless Sensor Networks: An Energy-Efficiency Perspective." Cybernetics and Information Technologies 21.2 (2021): 136-165.

11. Singh, Charanjeet, et al. "A Secure IoT Based Wireless Sensor Network Data Aggregation and Dissemination System." Cybernetics and Systems (2023): 1-13.

12. Papadimitriou A, Fessant FL, Viana AC, Sengul C. Cryptographic protocols to fight sinkhole attacks on tree-based routing in Wireless Sensor Networks. 5th Workshop on Secure Network Protocols (NPSec 2009), USA, Princeton, 2009; 43–48.

13. Ezhilarasi, M., Krishnaveni, V. An evolutionary multipath energy-efficient routing protocol (EMEER) for network lifetime enhancement in wireless sensor networks. Soft Comput **23**, 8367–8377 (2019). https://doi.org/10.1007/s00500-019-03928-1

14. Shafiei H, Khonsari A, Derakhshi H, Mousavi P. Detection and mitigation of sinkhole attacks in wireless sensor networks. Journal of Computer and System Sciences 2014; **80**(3): 644–653.

15. Sneha, V., and M. Nagarajan. "Localization in wireless sensor networks: A review." Cybernetics and Information Technologies 20.4 (2020): 3-26.

16. M. Ezhilarasi, A. Kumar, M. Shanmugapriya, A. Ghanshala and A. Gupta, "Integrated Healthcare Monitoring System using Wireless Body Area Networks and Internet of Things," 2023

4th International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 2023, pp. 1-5, doi: 10.1109/ICITIIT57246.2023.10068616.

17. Yilmazel, Rüstem, and Nihat Inanç. "A novel approach for channel allocation in OFDM based cognitive radio technology." Wireless Personal Communications 120.1 (2021): 307-321.

18. Hashim, H. A. (2020). Enhanced Method to Stream Real Time Data in IoT using Dynamic Voltage and Frequency Scaling with Memory. International Journal of Advanced Computer Science and Applications, 11(11).

19. El Attar, Hussein M., and Mohamed Ibrahim El-Emary. "Energy, delay and hop count multi-constraints QoS routing algorithm for wireless ad-hoc networks." 2017 IEEE 17th International Conference on Communication Technology (ICCT). IEEE, 2017.