Heliyon 10 (2024) e30675

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Intrusion detection in machine learning based E-shaped structure with algorithms, strategies and applications in wireless sensor networks

Suriyan Kannadhasan [a,*], Ramalingam Nagarajan [b]

[a] *Department of Electronics and Communication Engineering, Study World College of Engineering, Tamilnadu, India*
[b] *Professor, Department of Electrical and Electronics Engineering, Gnanamani College of Technology, Tamilnadu, India*

ARTICLE INFO

Keywords:
E-Shape patch antenna
Machine learning
WSN
VSWR
Intrusion
Reflection coefficient
Accuracy and radiation pattern

ABSTRACT

In the everyday world of computer applications, from the cloud to the Internet of Things, distributed sensor networks are essential (IoT). These computer application devices are often connected to Arduino network connection and microcontrollers such sensors and actuators. Thus, a defensive network with an IDS serves as the need for contemporary networks. The intrusion detection system has unavoidably evolved throughout the years, but despite this, it remains a difficult study topic since the current intrusion detection system uses signature-based approaches rather than anomaly detection. Therefore, improving the current intrusion detection system is challenging since it is difficult to find zero-day attacks in IoT networks when dealing with varied data sources. Filtered Deep Learning Model for Intrusion Detection with a Data Communication Approach is presented in this study. The five steps that make up the suggested model are Initialization of Sensor Networks, Cluster Formation and Head Selection, Connectivity, Attack Detection, and Data Broker. It was discovered that the suggested model for intrusion detection outperformed both the current Deep Learning Neural Net and Artificial Neural Network. In comparison to the most popular algorithms, experimental findings revealed a superior result of 96.12 % accuracy. The E-shaped patch antenna is a brand-new single-patch wide-band microstrip antenna that is presented in this research. A microstrip antenna's patch has two parallel slots built into it to increase its bandwidth. Investigating the behaviour of the currents on the patch allows for the exploration of the wide-band mechanism. A broad bandwidth is achieved by optimising the slot's length, breadth, and location. Finally, a 40.3 % E-shaped patch antenna is developed, made, and tested to resonate at 7.5 and 8.5 GHz for wireless communications. Additionally displayed are the reflection coefficient, VSWR, radiation pattern and directivity.

1. Introduction

Cloud computing (CC) is becoming more and more popular in commercial and educational settings these days, and it is also widely used for data storage and retrieval in the cloud environment. The cloud storage companies, such as Google Drive, Dropbox, and Amazon Simple Cloud Storages Service (S3) agree to store data in several inaccessible places as a way of expanding the amount of data on the cloud servers (CS). This implies that the data is distributed and accumulated over time. Even if there have been many appealing

[*] Corresponding author.
E-mail addresses: kannadhasan.ece@gmail.com (S. Kannadhasan), krrajan71@gmail.com (R. Nagarajan).

https://doi.org/10.1016/j.heliyon.2024.e30675
Received 7 July 2023; Received in revised form 30 March 2024; Accepted 1 May 2024
Available online 4 May 2024

developments in data collection over the last ten years, there are still several major obstacles that remain. Undoubtedly, the variety of sensors available on the market, the constant decline in sensor size and cost, and the tremendous advancements in Sensor Node communication technologies have increased the potential impact of IoT. IoT includes SN that can compute, sense, and communicate the data via a certain kind of communication. The SN are used for sensing, multiple algorithms are used for calculation, and several communication protocols, such as Distributed Network Protocols version (DNPv3) for BACnet's Building Automations and Control Network (BACnet), are used for communication (DNP3).

Extensible Messaging and Presences Protocol (XMPP), Message Queue Telemetry Transports (MQTT), Constrained Application Protocol (CoAP), AQMP, and other protocols are included. These protocols are used to collect the data. The detection of evil deeds is an important process since the obtained data may include harmful actions. Intrusion Detections (ID) are a sign of malicious activity. An intrusion is a collection of actions that violate security policies, including those governing the integrity, confidentiality, and accessibility of data as well as the accessibility of services, by taking advantage of flaws in the security process and the scheme's execution as seen by IDS. With the growing deployment of IoT systems and the fact that their security affects both the IoT systems themselves as well as various structures related to the internet of things, as well as the fact that their safety affects both, the term "intrusionIoT intrusion detection systems (IDs) look for attack signatures, which are certain behaviours that often point to malicious or suspicious origin. This identifies the typical network use as noise characterisation. An intrusion hobby is thought to be anything noticeable in the noise. Amazing techniques for categorising IDs is based on anomaly detection, signature-based abuse, host-based misuse, network-based misuse, and stack-based completely [1–5].

WSN are made up of a group of sensor nodes with a finite lifespan that are placed in various locations to detect nearby physical phenomena. WSN is characterised by a broad range of applications, such as monitoring the environment, surveillance, home security, military applications, medical monitoring, and industrial machine monitoring. A WSN is expected to deliver service for an extended period of time at any given moment while utilising the network's constrained resources. Small, low-cost, resource-constrained sensor devices make up WSN. Researchers are becoming more interested in the topic of addressing security in WSN as a result of the dynamic changes that occur in WSN. Another difficult task is finding security solutions that make the best use of energy. In this paper, we attempt to offer a solution for probabilistically detecting malicious nodes while effectively utilising energy. Our strategy is based on learning automata (LA) concepts [6–10].

The protocols in designed for Wireless Sensor Networks (WSN) have a unique requirement for being of low complexity and energy-efficient. Security, which includes intrusion detection and intrusion prevention, is crucial because to its potential deployment in distant regions for civic, educational, scientific, and military objectives. In this research, we provide an energy-conscious, low-complexity, and straightforward approach for WSN intrusion detection. The protocol is distributed and self-learning in nature. Due to the distributed architecture, when one node is compromised, no other nodes are not sacrificed. The protocol combines the idea of stochastic learning automata with a packet sampling method to create an intrusion detection system that is energy conscious. We have thoroughly assessed the effectiveness of our suggested solution using a number of experiments, and we have discovered that our solution approach is promising. In the trials, a maximum packet sapling effectiveness of 97 % was attained [11–15].

Two approaches for IoT data dissemination to the cloud using IANFIS and safe transmission of the disseminated data using MECC were presented. The IoT device is first authenticated by carrying out registration, login, and verification in order to prevent the device from being used without authorization. Smart sensors are then used to access the device and sense information about related items. The MQTT protocol is also used to execute communication between various IoT sensors. This sensed data from various IoT devices is transferred to the particular cloud server by way of the IANFIS (CS). The data is then securely delivered to the user via the MECC algorithm. The local computation (LC) is then completed using HFPGA. The experiment is carried out to evaluate the effectiveness of the suggested work. The findings indicated that the suggested strategies function better when evaluated against other current algorithms. Farhan Siddiqui et al.'s implementation of open-source execution of the Restricted Packages Protocol (CoAP) and Datagram Transport Layers Protection led to a secure information transfer between IoT devices (DTLS). The investigation tested that the utilisation of a CoAP-DTLS exe-cution with a symmetric key cyphers suite brought about considerable overall performance losses. An unsecured connection used around 10 % more energy than a secure connection using DTLS over CoAP [16–20]. Additionally, the latency examination revealed a more than 100 % increase in the average latency time for secure communications compared to before encryption was used. The method raised an actual IoT testbed for secure experimentation while emphasising many of the execution issues. An information-focused, context-aware approach for dealing with intrusions caused by malicious nodes was advanced [21–25].

2. Intrusion detection based WSN

The networks were divided into clusters using the technology-focused intrusion detection system (KB-IDS), and each cluster was then rendered a CH. The CH tracked each of its associated nodes' performance inside the cluster.Here, the initialised SN is clustered, and the CH is then selected using the Modified K-Means (MKM) technique. The premise behind the well-known partitioning method known as K-means clustering is that the given SN must be divided into K clusters, the value of which must be specified by the user and fixed. This approach is more beneficial for creating the clusters targeted at the many real-world applications of WSN [26–30]. The technique also executes re-clustering at failure stages and has simple, highly reliable, and quick iteration convergence as a feature. Every cluster is picked for clustering in this first centroid, and then data points that pass through a certain cluster with a minimum distance are allocated to that particularcluster according to the chosen centroid. Euclidean distance is often used to calculate the separation between data points and a given centroid. However, the fundamental Euclidean is not appropriate for a large amount of data because the SN sense a large volume of data naturally. As a result, Mahalanobis distance is considered to render better cluster outcomes than the Euclidean distance computation and achieve better clustering accuracy in this case [31–35].

The TON IoT datasets are the latest iterations of Industry 4.0/Internet of Things (IoT) and Industrial IoT (IIoT) datasets used to assess the effectiveness and efficiency of various cybersecurity solutions based on AI and deep learning algorithms. The datasets are known as "ToNIoT" because they include a variety of data sources that were gathered from IoT and IIoT sensor telemetry datasets. The proposed protocol uses the ToN-IoT dataset, which includes both normal and attacked data, to test the performance of the IDS. The sorts of data that are being targeted include data injection, ransomware, distributed denial of service (DDoS), and denial of service (DoS). The ToN-IoT datasets were compiled from a variety of data sources, including Telemetry data from IoT services, Operating System logs, and IoT Network traffic. These sources were used to create a realistic representation of a medium-scale network in the IoT [36–40].

It might be difficult to combine DC with efficient cloud storage. The FDLNN method was used in this article to provide a DC and efficient distributed cloud storage system based on the IDS. The proposed system employs the FDLNN algorithm for IDS, the LFEHO algorithm for the data broker, and MQTT and AQMP communication for the DC. The AQMP is appropriate for heavy devices, whereas MQTT is better for lightweight ones. The TON IoT datasets are used for the IDS analysis, and the FDLNN's performance is compared with that of the exisiting DLNN and ANN algorithms based on precision, recall, F- Measure, and accuracy [37,39]. The performance of the data broker is then examined. Based on average turnaround time, throughput, process time, reaction time, and AWT, the proposed LFEHO is contrasted with the pre-existing IANFIS and ANFIS algorithm. The data broker is evaluated based on the volume of data, and the IDS performance is evaluated based on the number of SNs. The FDLNN has 96.12 % accuracy for 500 nodes. The suggested LFEHO achieved superior performance in data broker analysis for every data count. Therefore, when compared to the current methods, the new system is determined to have good performance. The suggested system may eventually benefit from the use of cutting-edge algorithms and the sophisticated connection protocol, which supports all devices [29].

The unique design of Software Defined Networking (SDN), which offers a possible answer to the administration of quickly expanding networks, has attracted a lot of interest. The administrator side's flexibility and adaptability are maximised by the decoupling of the control and data planes, the centralised controller, and the programmability. As the top layer of a three-layer paradigm, the application layer prepares all the rules and policies set by the administrator. An SDN controller may dynamically change these rules [33]. The behaviour of the whole network could vary if the application layer is modified. The open-source platform has made it possible to no longer just rely on suppliers for application layer development. SDN eliminates the need for licence restrictions and enables network managers to create their own apps to tailor network management on general-purpose hardware. The control layer, on the other hand, serves as the brain of the model. It takes input from the data layer and forwards it to the application layer while converting rules from the application layer into understandable messages. The data layer realises the implementation once the control layer makes a decision.

The SDN's data layer has no intelligence; it only obeys commands from the control plane. Network administrators can automatically handle security measures for massive networks thanks to centralised management. Building, deploying, and maintaining a network are made easier by SDN. Without disclosing the specifics of the underlying layer, access to the network is allowed. By upgrading SDN apps, network functionalities may be easily improved. Therefore, in the network, basic hardware devices are adequate. In addition to being affordable, SDN-based devices have essentially no compatibility problems. Fig. 1 shows Intrusion Detection based WSN structure.

Here, present straightforward learning method procedures to identify malicious information, ensuring that the sensor network's energy is used effectively. The fundamental idea behind our strategy is to teach each node about the relevant network processes so thatA node can quickly identify nodes that are acting improperly. Numerous recent publications discuss and suggest various security

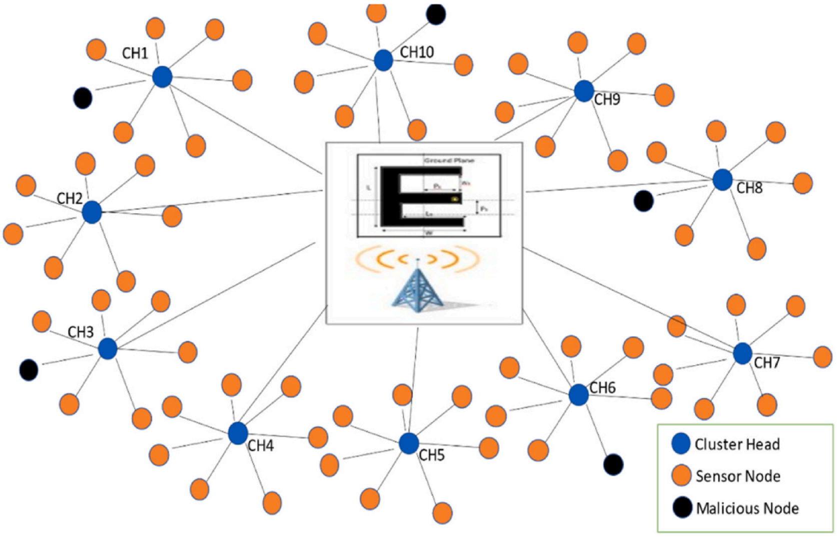

Fig. 1. Intrusion detection-based WSN.

protocols and solutions for use in WSN. The SNEP and SPINS, whichA few examples include the -TESLA protocols, INSENS, ARRIVE, and TinySec. Finding potential network intrusions is one of the most important security issues. Numerous plans exist for creating intrusion detection systems. The problem of intrusion detection and various intrusion detection solutions have recently been addressed in the literature. Since there are no centralized servers to maintain, unlike in infrastructure-based wireless networks, security is one of the difficult problems in WSN.A game between the invader and the system may be used to represent the intrusion detection issue. The system attempts to identify and delete as many harmful packets from the intruder while the intruder tries to inject as many malicious packets into the system as possible. One cannot predict the intruder's conduct in a realistic design approach. The system should be able to identify the attacker's essential traits on its own. Additionally, in any system that uses packet sampling, all malicious packets will be found if the sampling rate is greater than the total number of packets that pass through the node. In theory, each packet that enters an interface should be examined. However, this strategy only works for nodes with substantial processing power and no energy restrictions.

In this study, the security of the data gathering process. Wireless sensors (or nodes) are in fact susceptible to a variety of malicious attacks, such as jamming, physical attacks, and Sybil attacks, because they typically have low computational, storage, and energy requirements. Sensors are also simple to tamper with in order to retrieve the data they collect. A black hole attack, for instance, may be used by an attacker to intercept sensor communications and retrieve the data. As a result, it's essential to include a security system that not only controls invasions but also ensures safe data transfer. Symmetric cryptography is often used to protect data transfer. It really is among the most effective security measures for WSN. With such a system, the data transmitted by a sensor cannot be recovered if the transmission is intercepted. Such a system requires the usage of a secret key to encrypt all communications. Both the data sender and recipient share this key. In reality, this tactic's capacity to intercept is its weak point.

For the purpose of detecting cyberattacks on intrusion detection systems (IDS) in cyber-physical security systems, the deep learning technique is very useful. A crucial component of network security defence is the ability of cyberattacks to alter and breach the security of the network system. An intrusion detection system's (IDS) job is to identify suspicious activity and take necessary action to shield the network from potential assaults. For today's intrusion detection systems, machine learning and deep learning approaches are crucial. However, traditional intrusion detection systems have low accuracy and detection rates and are unable to quickly and accurately identify complex and diverse network attacks. As a result, these methods frequently perform poorly when managing large amounts of data in a large network infrastructure and making extensive use of numerous features. In order to solve these problems and enhance the scalability and accuracy, we have developed a deep learning technique based on a novel multilayer long short-term memory (LSTM) model for network attack detection in this research. The novel aspect of the suggested scheme is that the ideal multilayer architecture is constructed to attain maximum accuracy in the network architecture to improve performance through more efficient stacking of multiple LSTM cell layers, as well as improved stability to consistently perform in binary and multiclass classification on NSL-KDD datasets. The suggested multilayer LSTM model offers exceptional results with 95 % and 96 % accuracy, respectively, in binary and multiclass classification, according to experimental testing using the KDDTest + datasets. To run real-time applications, our ideal multilayer architecture has to be implemented in order to interact with real datasets and achieve acceptable performance in the network design. As a consequence, compared to current state-of-the-art procedures, the outcomes are better and more reliable [41,42].

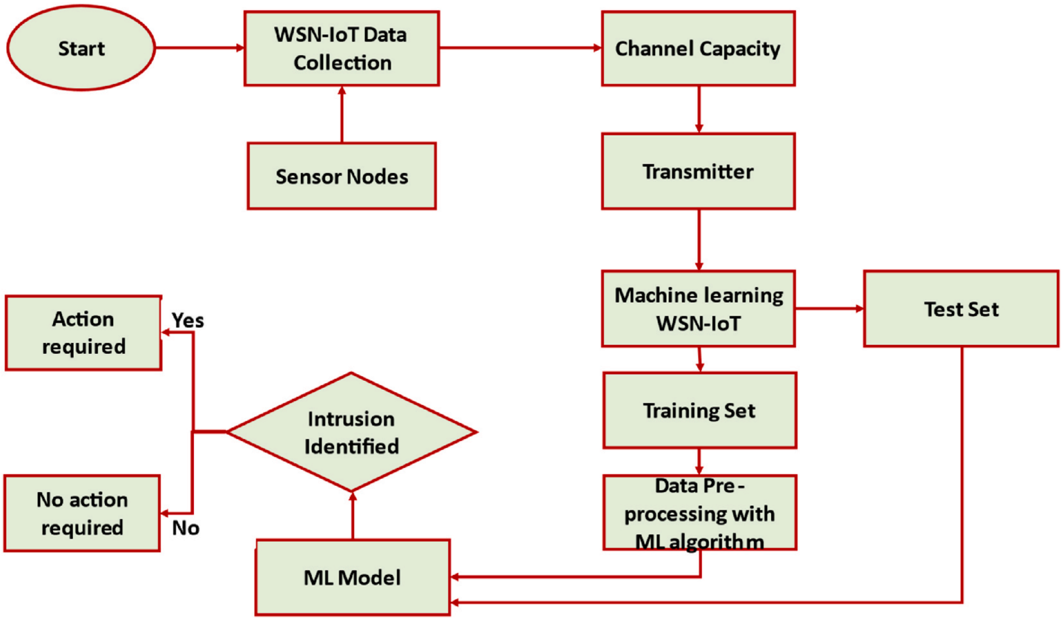

Fig. 2. Machine Learning based WSN.

3. Implementation of machine learning IN WSN

The nodes in a WSN are constrained by stringent energy requirements and have limited computing capability. Therefore, it's crucial to manage the sample rate. Not only should the sample rate be updated by the rate control method,but should do it in a way that is energy-efficient. The nodes must possess the ability to learn on their own in order to regulate the sample rate in an energy-efficient way. Additionally, the learning system used in the context of WSN should have a minimal spatial and temporal complexity. LA is such a learning system. In order to control the packet sampling rate effectively in our proposed algorithm and make it suitable for use in resource-constrained WSN, we developed a straightforward LA-based solution.It is impossible to predict how an attacker will act. A complicated monitoring process is necessary for any mechanism to precisely predict how many packets the attacker will send in the following instant. There will also be a sizeable amount of processing power to pinpoint the attacker's network attack pattern. The cost of carrying out this procedure in a WSN is very high. Nevertheless, certain traits of the attacker canbe simple to locate and put to use in enhancing the system's performance. The learning functions determine the sampling rate that the automaton should apply during the subsequent instant. In theory, increasing the sampling rate does not ensure that all malicious packets will be intercepted. The machine learning-based WSN is shown in Fig. 2. Lower sampling efficiencies could result from increasing the sampling rate.

The iterative channel selection to reduce energy consumption is addressed by the offline learning algorithm based on reinforcement learning. This approach emphasizes the learning capability that each sensor learns its behavior and makes the best decisions while convergent to an acceptable and stable solution. Each sensor can learn from a sequence of its individual feedback history and adjust its behavior towards the expected target. The offline decision is distinct from the online. The selection behavior of a node can be changed by a learning algorithm over time rather than immediately. In the past few years, wireless localization in indoor environments has received a lot of attention. With the spread of Wireless Sensor Network (WSN) applications, this interest is predicted to increase further. Localization is a key component of managing and real-time monitoring in the sensor networks. In actuality, location determination is essential for many management tasks, including monitoring, location-based routing, and fault detection. One of the well-known solutions to the localization issue is the Global Positioning System (GPS), but its applicability in indoor settings is still up for debate. Alternative positioning and tracking methods utilising WSNs have been adopted as a result. Localization has made use of a variety of measurement parameters, including angle of arrival, time of arrival, and impulse responses. However, the implementation of such parameters necessitates expensive hardware, rendering them useless for many applications. The proposed procedure of flow chart is shown in Fig. 3.

The power measurement of a received radio signal is referred to as received signal strength indicator (RSSI). Since it can be found in the majority of commercial wireless devices without incurring any additional costs, this radio parameter has been widely used in localization techniques. Signal propagation inside buildings, however, is subject to fluctuations brought on by fading, interference, and a variety of other environmental factors. Several machine learning solutions have been developed to address this problem. a strategy have been put forth. Researchers have been inspired to create better solutions to increase positioning's robustness and accuracy as a result. The area of artificial intelligence known as machine learning is concerned with creating algorithms and other techniques that let systems learn models and rules from data. Learning by Example techniques are frequently used in WSN localization to map the intricate relationships between the target position and the RSSI behavior. Support Vector Regression (SVR), neural networks, fuzzy logic, and other learning techniques have all demonstrated their suitability for understanding the intricate connection between RSSI and position estimation is shown in equation [1–4].

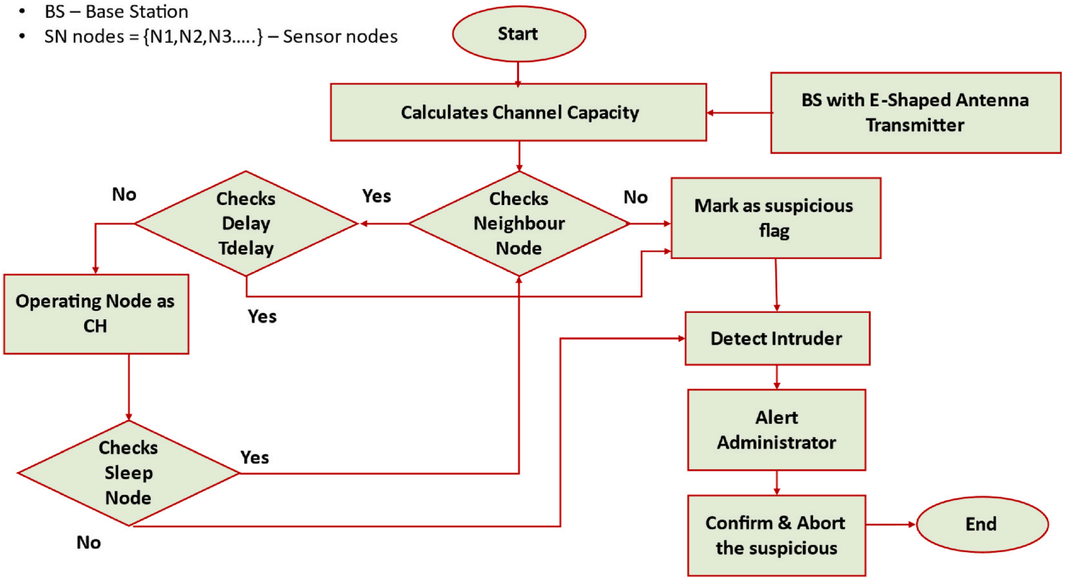

Fig. 3. Flow chart of the proposed system.

$$P_V = \frac{f(x/V_0)}{f\left(x/V_0 + R_i + R_j\right)} \tag{1}$$

$$V = \varphi * \ F_{mv} * \ PF(C + W) \tag{2}$$

$$P'_{vd} = \frac{P_{id} + \alpha\ e_j}{1 + \alpha(|S_k| - 1)} + V_d \tag{3}$$

$$P'_{ij} = \frac{1 - qe_j}{\sum_j^{|V_k|} qe_j} + r_d \tag{4}$$

Where.

i,j – Node Initialization.

Vo- Initial Velocity.

R- Residue.

E– Energy.

C-Capacity.

W- Weight.

The development of an RSSI-based method that works for both static localization and target tracking is the key contribution of this study. In order to increase the resilience and accuracy of the current based localization technique with lessened computational cost, an ensemble learning localization approach is applied. In order to get the best location approximation, the suggested method is based on segmenting the training input set into several subsets and applying an RT localization algorithm to each subset. Anchor nodes, which are nodes with known positions and are utilized as reference points to estimate the locations of sensors with unknown positions, are used to carry out the localization procedure. The most accurate anchor node choice has been shown to increase localization accuracy. In order to choose the best anchors close to the target, a K-nearest neighbour (KNN) classifier has been suggested. Accuracy, robustness, and complexity are measured as performance metrics for the suggested method. It has been shown that the location and choice of the anchors has a significant impact on the localization accuracy and efficiency in the context of anchor-based systems. New anchor node selection methods were suggested by many academics to enhance localization performance. A small number of anchors were chosen using a clustering approach based on Euclidean distance between anchor nodes. For the target localization, the subset of anchors transmitting at the highest RSSI is chosen as the reference. Considerable RSSI values, however, are not purely associated with because of the high unpredictability of the RSSI behavior. A unique approach based on the well-known classifier KNN has been suggested in earlier work. With the use of categorization and RSSI data, the closest anchor in each subarea is to be chosen. The third node is then picked as the one with the least distance between the two KNN-selected nodes. The anchor nodes may be arranged most effectively using this strategy.

```
1. Initialization
   (a) Total Budget for the system is configured
   (b) Initialize
         (i) Penalty Threshold
        (ii) Step value
       (iii) Reward Constant (Z)
        (iv) MIN RATE
   (c) sampleRate = MIN RATE
   (d) MAX BUDGET = MIN RATE
   (e) Balance Budget = Total Budget
2. Function
   (a) Perform sampling process
   (b) DetectionRatio= (No. of Malicious Packets caught)/(No. of Packets Sampled)
   (c) if (DetectionRatio > penaltyThreshold)

   Penalize The node.
   {
   else.
   Reward the node.
   }
```

4. Function

```
(a) if (request<(MAX RATE + stepValue))
```

```
        (i) sampleRate = request
       (ii) MAX RATE = request
    (b) else if (request > MIN RATE)
      (iii) MAX RATE + = stepValue
       (iv) sampleRate = MAX RATE
    (c) else
        (v) sampleRate = MIN RATE
       (vi) MAX RATE = MIN RATE

  Algorithm for Reward Function
  expr = 1.0 - (Balance Budget/TOTAL BUDGET)
  request = Z * sampleRate * expr
  RateControl (request)
  Algorithm for Penalization Function

expr = (Balance Budget / TOTAL BUDGET) + Detection Ratio + 1

  request = Sampling Rate * expr
  RateControl (Request)
```

The creation and debugging of network protocols, as well as network efficiency improvement, depend on network monitoring and protocol analysis. On the basis of common network protocols, several network monitoring tools have been created for wired networks]. Channel conflict and connection instability in wireless networks make monitoring and analysis more challenging. Due to the absence of network design and protocol standards and the resource limitations on network nodes, wireless sensor networks (WSN) provide significant difficulties for monitoring and analysing sensor networks. Network monitoring in a WSN may be split into active and passive monitoring. To gather comprehensive data on the network and node parameters during active monitoring, a monitoring protocol must be installed on the network protocol stack in the nodes. However, it is challenging to create, implement, and modify the monitoring protocol in WSN since there is no industry standard for monitoring protocols. Furthermore, in a sensor network with limited resources, the monitoring flow, which is mixed with network data flow, may significantly affect network performance. An extra monitoring network is set up during passive monitoring.

$$Residual = Sv_i * \left[\frac{1 - YXE_{r(i)} - E_{avg}}{E_{avg}}\right] \tag{5}$$

$$E_{avg} = {}^1/_L \sum_{i=1}^{L} E_{res}(i) E_{res}(j) \tag{6}$$

$$F_1 r = E_1 \rho(s,t) + E_2 \rho(s,t) \tag{7}$$

$$F_2 r = V * E_1 + E_2(s,t) \tag{8}$$

The value by the sampling rate is to keep efficiency and extend lifetime. This enables a more gradual rise in sampling rate. This is advantageous because it prevents the system from using a large portion of the budget all at once. In essence, we control the rate of the sampling rate increase using the rate control algorithm. The system determines whether it is profitable to increase the sampling budget each time (i.e., the detection rate exceeds the threshold for a penalty). The system can ensure that it is operating in an energy-efficient manner. It would be excellent to measure the system's performance in networks without energy restrictions based on the total number of malicious packets found or the percentage of harmful packets captured. But the need of energy-efficiency in sensor networks has to be emphasized further. The effectiveness of the system's sampling should thus be taken into consideration when assessing its performance. Sampling budget used in effectively identifying malicious packets is measured by sampling efficiency is shown in equation [5–8]. An 80 percent sampling efficiency indicates that 80 malicious packets were discovered for every 100 packets tested. As was already noted, any system sampling at high rates will be able to identify all the malicious packets that travel through it. This has the benefit that detection and removal of malicious packets are done in an energy-efficient way when performance is evaluated based on sampling efficiency. However, this approach is not energy-efficient.

As a result, upcoming technologies like radio frequency identifiers (RFIDs) and wireless sensor networks as well as smaller devices like smartphones and PDAs, 3G and 4G mobile communications, will be able to carry out high-level security operations. Additionally, by carrying out these two tasks at once, we may save resources like time and energy since the work will be completed faster. As a result, signcryption is an excellent choice for key management in wireless sensor networks and other situations with limited resources. Since the creation of the signcryption primitive, many other constructions have been suggested, and the majority of them are based on three different types of cryptographic assumptions is shown in equation [9–13].

$$ReW(t) = \frac{W_1 * E_1}{E_{max}} + \frac{W_2 * E_2}{E_{max}} + \ldots \frac{W_n * E_n}{E_{max}} \tag{9}$$

$$S(t) = \frac{S_{ij}}{\sqrt{S_{ij} .\ S_{ji}}} \tag{10}$$

$$S_{ij} = \sum m^2 - \frac{(\sum m)^2}{V} \tag{11}$$

$$S_{ji} = \sum v^2 - \frac{(\sum v)^2}{t} \tag{12}$$

$$S_{ij.ji} = \sum m^2 v^2 - \frac{(\sum m).\ (\sum v)}{V.t} \tag{13}$$

5. E-SHAPED structure based WSN

The microstrip patch is an inexpensive, low-profile antenna. It has a broad range of uses, including those for GPS systems, RFID tags, and satellite communication. The patch antenna's main drawback is its limited bandwidth. As a result, this article describes how to create patch antennas with greater bandwidth by giving the patch slots. The rectangular patch has two parallel slots, giving it the appearance of an E shape. There are additional specifics concerning the microstrip patch's feeding procedures. The fundamental issue with a microstrip patch is its narrowband, hence one technique to enhance the bandwidth is to add slots to the patch. Slots may have the shape of an S, U, L, E, or H. However, research indicate that the E shape provides more increased bandwidth than other shapes. Two parallel slots are offered and positioned symmetrically with regard to the feed point for the rectangular patch size (L, W, h) supplied by coaxial probe at (X & Y). Slot length, slot width, and slot location for the E shape patch are crucial characteristics for increasing the bandwidth. The E-Shaped based Intrusion detection system is shown in Fig. 4.

The amplitude of currents fluctuates with low resonant frequencies and high resonant frequencies when the effects surrounding the slots are analyzed. At high frequency, the current amplitudes around the slots are almost equal to those at the left and right edges. As a result, at high frequencies, it functions like a regular patch and is based on patch width. The current amplitude is greater at lower frequency than at lower frequency. An additional series inductance effect is produced by slots. Therefore, slots control the lower frequency, and slot width controls the higher frequency. As the slot's length, width, and position affect the E-shaped patch antenna, when these conditions are altered. It demonstrates that the slot length, position, has a greater impact on the resonance frequency than the slot width. When the slot width was changed, the inductance rose as the width did, lowering the resonant frequency. The current around the slot will be more intense as the slot length and inductance are both increased. As a result, the resonance frequency drops. Since the E-center shape's arm functions as a tuning capacitor, widening it will increase capacitance but decrease resonant frequency.

This antenna has the ability to guide the beam in various directions. Polarization reconfigurable antennas are the third kind. This may increase signal reception in environments with multipath fading. E-slot microstrip patch antenna design that is suggested made using photolithography. This technique produces the required pattern by chemically etching away undesirable metal regions of the

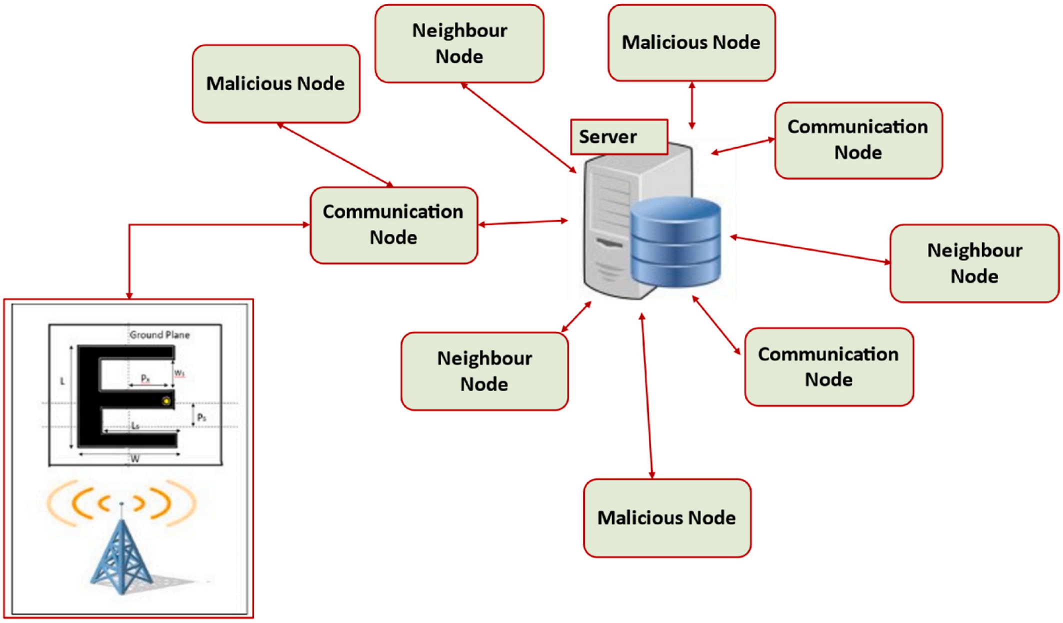

Fig. 4. E-Shaped based Intrusion detection system.

metallic coating. Choose the right substrate material for the suggested antenna design before beginning this operation. Antenna feed and ground are joined together via a female SMA connection (made of brass metal). SMA stands for sub micro version A, which gives an antenna electrical performance. Low reflections and consistent 50 Ω impedance are features of this connection. After construction, a spectrum analyzer is used to measure each parameter of the proposed antenna. The antenna parameters is used to calculate the formula is shown in equation [14–18].

$$W = \frac{v_o}{2f_r}\sqrt{\frac{2}{\in_r + 1}} \tag{14}$$

$$\in_{\mathrm{eff}=\frac{\in_{\mathrm{r}+1}}{2}+\frac{\in_{\mathrm{r}-1}}{2}\left[1+12\frac{\mathrm{h}}{\mathrm{w}}\right]}^{-1/_2} \tag{15}$$

$$\Delta L = 0.421h\frac{(\in_{ff} + 0.3)}{(\in_{ff} - 0.258)}\frac{\left(\frac{w}{h} + 0.264\right)}{\left(\frac{w}{h} + 0.8\right)} \tag{16}$$

$$L = \frac{1}{2f_{r\sqrt{\in_{eff}}\sqrt{\mu_o \in_o}}} - 2\Delta \mathrm{L} \tag{17}$$

$$W0 = \frac{c}{2 * f_0 * \sqrt{\frac{\varepsilon_{r+1}}{2}}} \tag{18}$$

This work aims to provide an overview of the most significant works for protecting CWSNs. Additionally, a discussion of unresolved research concerns is included at the conclusion of this article.With applications ranging from smart home control and assisted living to construction monitoring and intelligent transportation, WSNs are becoming more and more prevalent in our daily lives. The emergence of interoperability and commercial solutions has been made possible by the development of novel communication standards over the past few decades, including IEEE 802.11, Zigbee, and IEEE 802.15.4. However, these systems often have rigid deployment design and inadequate scalability. The stability of WSNs is a crucial issue for their widespread acceptance in important applications like smart metering, as opposed to luxury or experimental ones.

Additionally, the optical clarity and turbidity of the water affect optical communication. With devices like the Teledyne marine 900 series, acoustic communications are an alternate and well-liked communication technique in underwater sensor networks. These systems enable long-range communication distances using sensor nodes between 2 km and 4 km is shown in Fig. 5. Acoustic communications have communication speeds of between 90bps and 16,360 bps, which is much slower than optical and RF communications. The ability to create mesh topology networks utilising acoustic communications allows each node to connect with numerous nodes through a single communication channel. Since at least ten years ago, wireless sensor networks (WSNs) have continuously caught the interest of the telecommunications industry.

First, a small-size sensor node-appropriate AoA localization system idea is presented. The system is then shown with a full performance study that demonstrates its great promise even under challenging propagation circumstances. A novel heuristic weighting function is also suggested to improve a well-known least-squares technique. It makes it possible to more efficiently combine data from each anchor while minimising location mistakes. A realistic propagation model and sensor characteristics common for MICAz motes

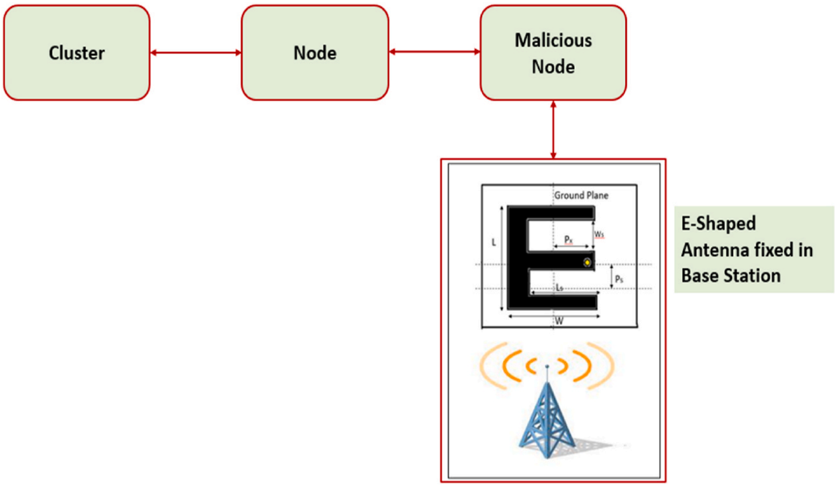

Fig. 5. E-Shaped based Sensor Node.

are used in Monte-Carlo simulations to verify the technique. To the best of the authors' knowledge, this is the first article in which the simulations take into consideration the effect of the Signal-to-Noise Ratio on the AoA localization.Finally, examples, analyses, and discussions of the trade-offs between accuracy, localization speed, and anchor count are provided. The E-Shaped Transceiver is shown in Fig. 6.

The EAP's antenna system is designed to provide better coverage while constructing a WSN network for irrigation management. This antenna system is suggested to offer switching narrow beams that scan the whole irrigation area to be managed as well as to facilitate communication between sensors and actuators on the ground and the global sink aboard EAP. Concentric circular antenna arrays are selected for the antenna array because they have various benefits over other types of antenna designs, including more uniform beam coverage across large angles and simpler feeding via windowing operations.

Different irrigation control methods have been developed in recent years, particularly for areas with few water resources, to enhance water usage. Some of these control systems schedule irrigation and employ water-saving irrigation methods. In,a number of irrigation control system designs with different hardware and software capabilities were put forward. The difficulty of covering large areas, particularly in isolated places that span great distances, like in deserts and hilly regions, is a concern when implementing wireless sensor networks for irrigation management. However, ground wireless sensor networks suffer significantly from a number of limitations, such as fading and fast signal degradation brought on by physical barriers. One effective way to boost communication performance is via satellite communications; however this option requires specialised infrastructure and high transmitting power, both of which are unsuitable for irrigation sensor and actuator systems. High-altitude platforms (HAP) are aerial stations that fly in the stratosphere, particularly at 20 km altitude, and can provide the same performance as satellite systems, such as wide area coverage, at a much lower required transmitted power. This concept has recently gained attention in several communications applications. By using adaptive antenna arrays to focus the radiation pattern on the desired locations, the system performance may be further enhanced. As a result, in this paper, the performance of wireless sensor networks for irrigation control purposes is enhanced by combining EAP technology with switched beam antenna and the suggested system can close the deployment gap for networks, particularly in remote areas with weak communications infrastructure.

Distinct radiation patterns result from the many concentric circular rings of the CCA's element arrangement, each of which has a different radius and element count. A set of link equations that take into account the environment in which the sensors are located, the AP coverage diameter, the transmission frequency, the bit rate, and the length of the connection distance characterize the communications link between AP and irrigation sensors on the ground is shown in Fig. 7. Additional connection factors including transmit power, transmit and receive antenna gains, and atmospheric variables all have an impact on how well the system works. The proposed switched-beam antenna design offers a number of benefits for this application, including strong antenna gain for communications with far sensors and reduced out-of-coverage power gain (side lobe levels) to lessen interference from nearby broadcasters HAP irrigation control stations. The proposed E-shaped Antenna structure is shown in Fig. 8.

As shown at various feeding profiles, the use of the suggested switched beam has enhanced both the received power levels and the quality of the communications connection. Table 1 gives the parameters of proposed E-shaped antenna structure.

The traditional alternative to the suggested irrigation management system is ground control, although this has very few advantages because of the topography and is further hampered by problems with terrestrial communications.

i. The suggested system has achieved wide area coverage, with a single EAP situated at a height of 22 km being able to cover a circle with a circumference of 1200 km. This is a relatively vast area compared to terrestrial irrigation management systems, which essentially only cover a few kilometers.
ii. The proposed irrigation control EAP system has channel propagation characteristics that are superior to those of conventional terrestrial wireless sensor networks. In the latter, the path loss is inversely proportional to the square of the slant distance between the EAP and receiver, whereas in the former, excessive multipath propagation occurs and the path loss is inversely proportional to the distance raised by an exponent of 4.
iii. Three different feeding strategies have been discussed, beginning with the simplest a consistent feeding profile. In comparison to other beam forming techniques, this feeding profile has the smallest beam width, but it suffers from greater side lobe levels, which are crucial to prevent miscommunications with other sensors in nearby irrigation zones.

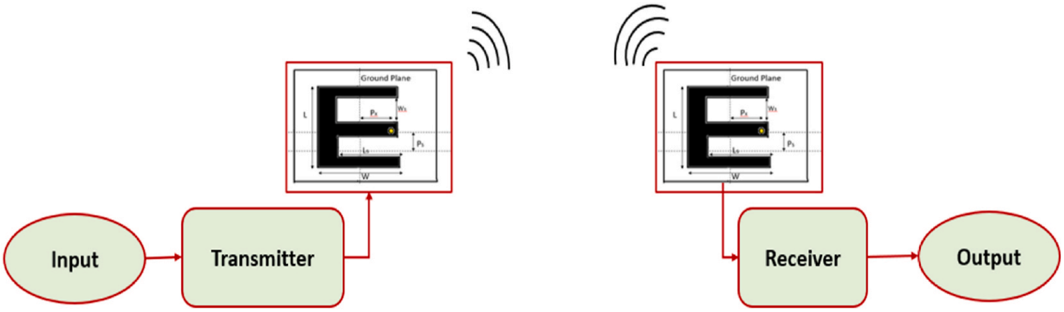

Fig. 6. E-Shaped antenna transmitter and receiver.

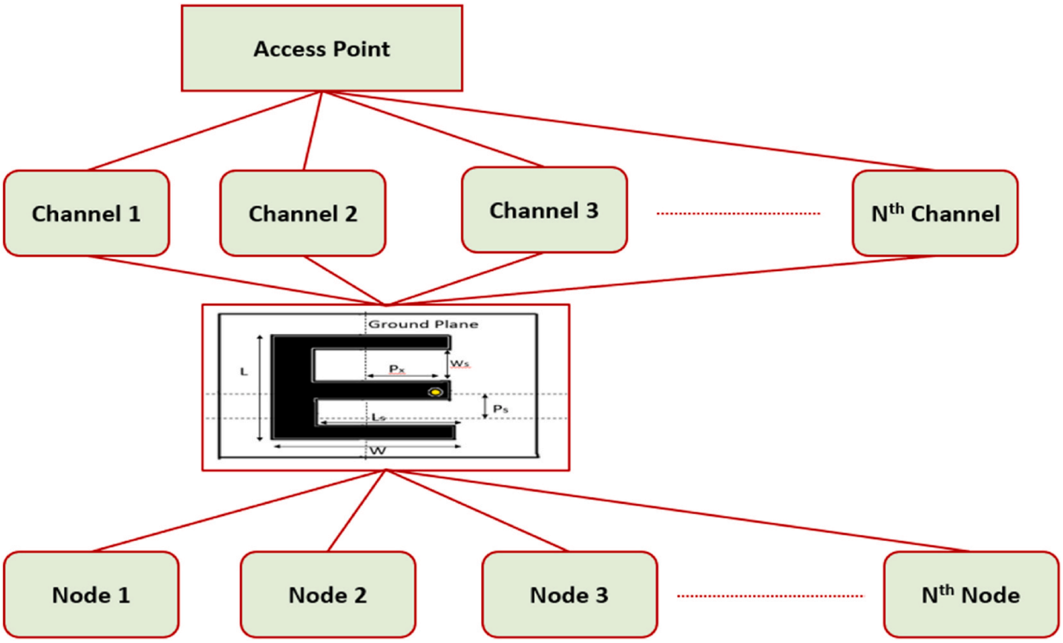

Fig. 7. E shaped antenna with access point.

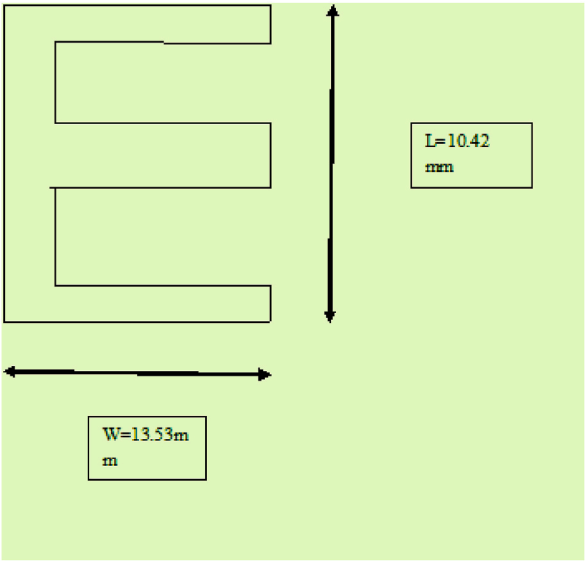

Fig. 8. E-Shaped antenna structure.

Table 1
Parameters of proposed E-Shaped Antenna Structure.

Sl.No	Parameters	Value
1	Substrate	FR4
2	Dielectric Constant	2.4 mm
3	Dielectric Height	1.6 mm
4	Loss Tangent	0.0002
5	Length	10.42 mm
6	Width	13.53 mm
7	Antenna Size	22X16X3.2

iv. The findings revealed that the communications connection performed well even in the worst-case scenario of uniform feeding, where the value of Eb/No is larger than 57 dB within the coverage cell border, and its dispersion eventually decreases, because of the greater amounts of sidelobes.

v. The communication performance within the cell is improved even at the end-of-coverage scanning beam, but the constant, progressive decline in Eb/No is still a significant issue.

vi. Using tapered beamforming methods such Hamming and Cosine profiles, as, the issue of progressive deterioration of Eb/No beyond the coverage cell, which may cause interference to other sensors, has been resolved.

vii. Using tapered feeding profiles has a negative impact on the Eb/No level within the coverage beam border but a positive impact outside the cell owing to decreased sidelobe levels.

6. Results and discussion

According to the research done, shortest-path routing protocols choose a set of pathways whose lengths follow a log-normal distribution. They develop an anomaly detection technique based on this discovery by deriving tolerance limits from the log-normal distribution of route lengths in the absence of an attacker.Therefore, while improving the performance of WSN routing protocols, energy efficiency and extended network longevity are of the utmost importance. Two categories of routing protocols are distinguished. Applications that call for regular data monitoring should use proactive routing protocols. Sensor nodes continually sense the environment, collect data, and transfer it to the Cluster-Heads (CH). Whether necessary or not, the CHs then send the data they have gathered to the Base Station (BS). Time-critical applications including intrusion detection, explosion detection, temperature, floods, and earthquakes may benefit from reactive routing protocols. Only in the event of a significant change to the detected value will the aggregated data be sent to the BS.When designing a WSN, cluster-based routing protocols will be employed to reduce energy consumption and improve network stability. The sensor nodes that make up the clustering network's structure carry out operations including data aggregation, memory management, data routing, and data processing. Clusters of sensor nodes are used for organization. Every cluster has a CH, which aggregates and collects local data from member nodes on a regular basis.

Among other ways, clustering is thought to be a superior way for energy-efficient WSN-based IoT to attain high performance in terms of the lifespan of the network. The clustering algorithm carries out operations such data gathering, processing, routing, and memory management. The proposed Enhanced Threshold Sensitive Distributed Energy Efficient Clustering (ETSDEEC) routing protocol is described in this section. The two thresholds HT and ST are used in the suggested protocol, which is implemented similarly to the optimization protocol TEEN on an improved version of DEEC. The proposed ETSDEEC has two key benefits. (1) The routing protocol is reactive. This indicates that data transmission will occur after obtaining the detected value and applying the thresholds rather than on a periodic basis as in TDEEC, EDEEC, or DEEC protocols. (2) It exhibits multi- and three-level heterogeneity. It also describes a hierarchical routing protocol for heterogeneous WSNs based on a clustering technique. The setup phase and steady-state phase are the two distinct stages of each cycle in the suggested ETSDEEC's.

As a consequence, it has been shown that the suggested ETSDEEC protocol has a longer stability period than the EDEEC and TDEEC protocols. a network with dead nodes. It demonstrates that nodes degrade more gradually under the proposed ETSDEEC protocol than under EDEEC and TDEEC. From the results, we deduced that the suggested ETSDEEC extends the stability period by 18.8 % and 29.4 % when compared to EDEEC and TDEEC, respectively. For EDEEC, TDEEC, and the planned ETSDEEC, the tenth node expires after several rounds respectively. the proposed ETSDEEC has a longer lifespan than the other two protocols. The proposed protocol ETSDEEC makes advantage of node energy and CH probability to help the network sustain for more rounds, same as it does during the clustering stages. For EDEEC, TDEEC, and the planned ETSDEEC, all nodes terminate after several rounds, respectively. In comparison to EDEEC and TDEEC protocols, the simulation demonstrates that the proposed ETSDEEC protocol increases network lifespan by around 59.8 % and 37.7 %, respectively.

The network packet that was transmitted to the BS. More data than in EDEEC and TDEEC is supplied to the BS in the ETSDEEC. As a result, the suggested ETSDEEC is more effective in terms of data transmission success. The network's remaining node energy. In comparison to previous routing protocols, the proposed ETSDEEC protocol exhibits a slower drop in energy consumption with an increase in the number of rounds. The suggested ETSDEEC used some energy for sensing, but data transmission is only carried out under certain circumstances when the measured value approaches or exceeds HT.The fourth-generation (4G) wireless communication technology already exists, and the fifth-generation (5G) wireless communication technology is a significant evolution of that technology. It offers a very high-speed connection with low latency and increased capacity. Reliable high-speed wireless communication has been essential for rapidly growing mobile subscribers over the past few decades. By linking and managing the devices, machines, and objects, 5G technology improves the 4G mobile networks. For increasing system capacity, the 5G systems recommend orthogonal frequency-division multiplexing (OFDM) as a significant method. To lessen crosstalk and interference, OFDM is a digital modulation technology in which an input data stream is split into several frequency narrow band channels.

Terminals using multichannel communication may broadcast concurrently on many channels without interfering with one another. To handle large and dense networks, it has been extensively employed in Wireless Sensor Networks (WSNs) or the Internet of Things (IoT). Channel selection is important in multichannelWSNs because different channels can produce different transmission qualities. In order to execute channel selection, centralised procedures are often taken into consideration due to the restrictions of the energy budget and memory capacity of WSN nodes. In these methods, a central node, such as an access point (AP) or sink node, completes all required calculations and provides information toreasonable choice of channel for the benefit of other sensor nodes. In order to switch to a channel with the least amount of interference, Wu et al. adopt a static tree-based channel selection approach where the sink node can operate on the attribute sensor node. However, centralised methods perform poorly in large-scale networks. As a result, distributed approaches have garnered more interest because node deployment can be done with greater flexibility and scalability. A counter-based approach is created by Tang et al. in which nodes choose the channels.

The approaches based on game theory and reinforcement learning have been introduced to improve channel selection or other resource allocation problems, for example] in order to implement self-decision and self-learning. Decentralized networks can be modelled effectively using game theory to find an equilibrium state. Its primary flaws are the enormous instant computational costs. In this paper, we propose a hybrid architecture-based intelligent channel selection strategy that makes use of both distributed and centralized methods. Our work does not require exchange or centralised controlor messages used during sensor negotiations. Most importantly, we use intelligent techniques to solve the application limitation problem of optimal channel selection with different communication overhead, such as game theory and reinforcement learning. We develop two algorithms the online decision algorithm and the offline learning algorithm from the viewpoint of sensors in order to accomplish this. We believe the suggested online and offline strategies have merits of their own and areaimed at a variety of application scenarios. When the network can meet the demands of energy and computational costs, the online decision algorithm based on non-cooperative game is to help each individual sensor immediately select optimal channel. The online strategy is less complex than the cooperative game in terms of computation because it is based on the non-cooperative game. Here, the term "online" refers to real-time computation from which sensors can obtain results instantly. This method focuses on how to use local computation by each individual sensor to determine the ideal equilibrium state.

In this study, we address these issues and create PMSW, a passive monitoring system for WSN, to analyse traces gathered by passive monitoring. This enables us to study the aforementioned issues using passive monitoring on active networks. The monitoring area has four different kinds of devices: a workstation, a sniffer node, a monitoring node, and a sensor node. A monitoring node is connected to by each sniffer node. The monitoring node examines the communication picked up by its sniffing node before sending it to the workstation for analysis. Three parts make up the workstation: (1) the merging component, which unifies network traces from various monitoring nodes; (2) the inference component, which tries to infer the missing packets and determines whether each packet was received by its destination; and (3) the analysis component, which assesses network performance and finds network faults.

Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision

$$Precision = \frac{TP}{TP + FP}$$

Geometric Mean

$$Mean = \sqrt{\frac{TP \bullet TN}{(TP + FN) \bullet (TN + FP)}}$$

Recall

$$Recall = \frac{TP}{TP + FN}$$

A wireless sensor network is made up of many inexpensive micro-sensor nodes that are placed across the monitoring region. It creates a multi-hop self-organizing network system using wireless communication. Its goal is to collaboratively detect, gather, and analyse data from sensing objects in the network's networked region, then deliver that data to the observer. WSN's three components are sensors, sensing objects, and observers. Sensor networks provide various advantages over conventional wireless networks, including high-precision monitoring, extensive coverage, distant monitoring, and other benefits brought forth by distributed processing.They have great fault tolerance, self-organization, and can be deployed fast. Networks that focus on data and applications are wireless sensor networks. Data from a wireless sensor network is similar to a distributed network database in that it may be accessed from all or some of the nodes. In the sensor network, each sensor node serves as both an end node and a router. The role of information gathering and processing is realised by the sensor node by receiving a query or control command from the sink point.

The routing function is simultaneously accomplished by analysing and forwarding data that has been received from other nodes. Sensor networks concentrate on information with certain characteristics. There are a lot of sensor nodes, and they are randomly deployed. As a result, sensor nodes do not necessarily need to adopt IP addresses; they might instead employ locally distinct labels. In sensor networks, neighbour nodes may keep an eye on the same event, such as pressure, fire, etc. From many monitoring sites, one may get pertinent information about the same occurrence. The data of neighbour nodes are comparable. Data from neighbour nodes may include redundant information. These data may be combined to efficiently save network resources. In today's wireless sensor networks, data fusion techniques face challenges such low fusion efficiency, subpar denoising performance, and high packet loss rates. In wireless sensor networks, data fusion techniques must be studied.

Due of its limitless potential, Wireless Sensor Networks (WSN) are now the focus of much study. As these systems are still in their infancy, there are still numerous research difficulties to be solved, one of which is the processing and fusion of sensors with constrained resources. The TX/RX antenna of a sensor is its most crucial component for 5.33–5.71 GHz frequency band wireless local area networks and other wireless communication systems. Microstrip antennas have drawn attention in this frequency range because to their low profile design. To address the issues, the microstrip antenna was created. It combines the benefits of compactness with the affordability and low profile of a patch antenna. With the use of High Frequency Analysis, the essential variables affecting the antenna optimization have been identified usingSoftware for Simulation (HFSS). Therefore, the 22X16 × 3.2 mm wide, 7.5 GHz microstrip antenna that was constructed on duroid with these performance metrics is very attractive for autonomous distributed sensor network applications that need a compact sensor node volume and great power efficiency.

To monitor physical or environmental factors like temperature, sound, vibration, pressure, mobility, or pollution and to jointly send their data across the network to a central point, a Wireless Sensor Network (WSN) is made up of geographically dispersed autonomous sensors. Modern networks are bidirectional, allowing for the management of sensor activity as well. Military uses of wireless sensor networks, such as battlefield surveillance, served as the impetus for their development. Today, these networks are used in a wide range of industrial and consumer applications, including traffic control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and monitoring of industrial processes.Due to their low profile, light weight, comfort on planar and nonplanar surfaces, ease of manufacture using current printed circuit technology, mechanical robustness when mounted on rigid surfaces, compatibility, and growing demand in wireless communication system applications, microstrip patch antennas have gained significant attention.

The amount of cross-polarization is decreased via probe feeding. Capacitances are introduced by the horizontal regions of the probe that are combined with the radiating patch and the ground plane. Low cross-polarization may be attained using these capacitances, which can reduce part of the inductance that the vertical sections of the probe contribute. Additionally, the slots' existence limits the patch currents at resonance frequencies that have a lower resonance on the design.The dimensions of the model were determined through parametric analysis and optimization in Ansoft HFSS using the initial circumstances and restrictions indicated above.optimise aspects like antenna gain, return loss, and lowest volume all at once. Prior to modelling the antenna, the substrate material of duroid was chosen, and an air box was made. The antenna's coaxial probe was employed to feed at its centre. To examine the microstrip antenna, frequency sweep analysis was carried out, and far field reports were kept.

Therefore, compared to the microstrip patch antenna, the wideband E-shaped patch antenna is more resilient in terms of reflection coefficient. Additionally, demonstrates that an omnidirectional antenna's reflection coefficient surpasses −10 dB after being detuned by cement board but stays below −10 dB when mounted to a brick. We have limited influence over these antennas' tuning as they are readily accessible commercial antennas. The detuning that happens when the antenna is put against the material is one of the most important findings in the context of this article. The E-shaped patch antenna performs better, whereas the omnidirectional and microstrip patch antennas suffer the most. Even though these improvements are modest in terms of efficiency, they have a significant impact on antenna gains. The observed E-plane dB radiation patterns of the omnidirectional antenna, microstrip patch, and E-shaped patch in free space and when mounted on brick and cement board.

Using a network analyzer and a reference E-shape patch antenna, measurements were taken on a rooftop range that was exposed to the elements. At 7.5 GHz, the E-shaped patch antenna outperforms both the common microstrip patch antenna and the omnidirectional antenna in terms of gain in open space. The Current distribution of E-shaped patch antenna shown in Fig. 9 provides stronger directivity than the microstrip patch antenna and omnidirectional antenna when affixed to either the brick or cement board. The radiation pattern of the microstrip patch antenna suffers greatly when mounted to brick, however the E-shaped patch antenna maintains its radiation pattern that was seen in free space. Furthermore, the omnidirectional antenna transmits more power into the materials than it does into free space since free space has a larger impedance than brick and cement board do. As a result, when

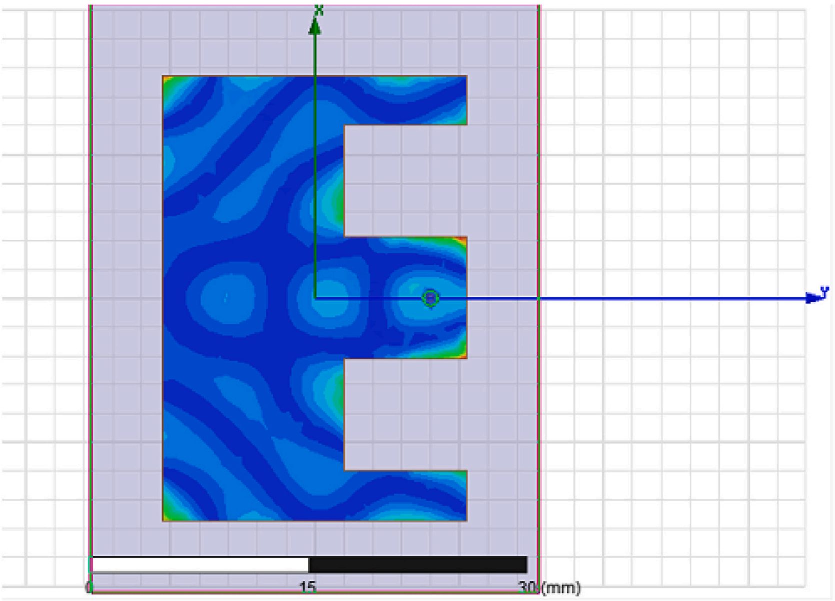

Fig. 9. Current distribution of the proposed structure.

mounted to the materials, omnidirectional antenna has better gain than microstrip patch antenna. We use the median of the RMSE obtained for all six trials carried out using one kind of antenna in order to compare the localization performance of each antenna.

For comparison, the lowest possible median RMSE using a 1 foot squared pixel is 0.4 feet for the brick home and 0.45 feet for the cement board house. We note that in both the brick home and the cement board house, the E-shaped patch antenna obtains a lower median RMSE than the other antennas using MARTI and VRTI. When comparing the Shaped patch antenna to the omnidirectional and microstrip patch antenna, the % reduction in median RMSE. In the brick home with the microstrip patch antenna, the E-shaped patch antenna decreases the median RMSE by more than 20 % utilising either RTI approach.The cement board home has more obvious localization benefits. When MARTI and an E-shaped patch are used, the median RMSE is reduced by 47 % an omnidirectional antenna and 53 % versus a microstrip patch antenna. We see that the omnidirectional antenna works almost as well as the E-shaped patch antenna when we employ MARTI in the brick home as shown in Fig. 10. But given that the material's size and its dielectric qualities often interact against one another to unintentionally create a resonance at the intended operating frequency, this discovery is not all that unexpected. A narrowband antenna should sometimes have a low median RMSE across a variety of construction styles and materials, according to what we would anticipate. However, the E-shaped patch antenna was specifically created to record a variety of geometries and dielectric characteristics.

The median RMSE attained by the E-shaped patch antenna in the brick and cement home using either RTI approach, according has a maximum difference of only 0.6 feet. The difference, on the other hand, is 1.8 feet for the omnidirectional antenna and 1.9 feet for the microstrip patch antenna. Comparing the E-shaped patch antenna to the omnidirectional and microstrip patch antennas, we can show that through-wall RTI localization is more reliable using the E-shaped patch antenna regardless of the size and kind of home. The observed reflection coefficient and the radiation patterns provide a good explanation for the findings. The reflection coefficient of the proposed structure is shown in Fig. 11. The gain of the proposed structure is shown in Fig. 12. The VSWR of the proposed structure is shown in Fig. 13.When the microstrip patch antenna is set against either brick or cement board, we see that its centre frequency changes away from 7.5 GHz after falling out of tune. The efficiency of the proposed structure is shown in Fig. 14.Table 2 shows various parameters resulting for various frequencies in GHz.

As a consequence, among all the antennas, its median RMSE suffers the most. Another intriguing finding is that for all antenna types, the median RMSE was lower in the brick home compared to the cement house. The fact that the brick home has a smaller footprint than the cement board house and that the reflection coefficients for the antennas at 7.5 GHz are lower in the brick house than the cement board house validate our experimental findings. These findings imply that localization accuracy is influenced by both the size of the monitored area and the kind of structure.

Although we use 20 nodes in our trials, we also want to demonstrate how the median RMSE changes when we use fewer nodes. To achieve this, we calculate the median RMSE for an overall iterations by iterating through all permutations of the 20 a nodes for a (16, 17, 18, 19, 20). In, we display the outcomes. According, the E-shaped patch antenna works better than the other antenna types for any

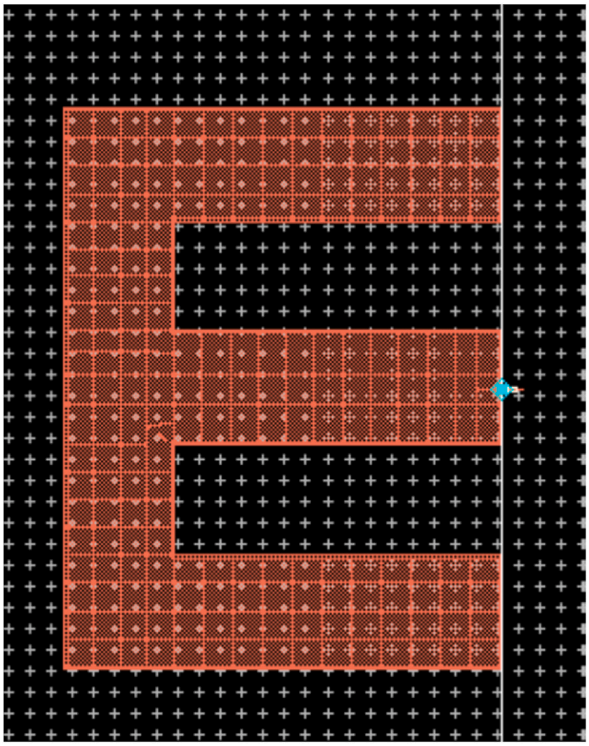

Fig. 10. Proposed Structure of E-shaped antenna.

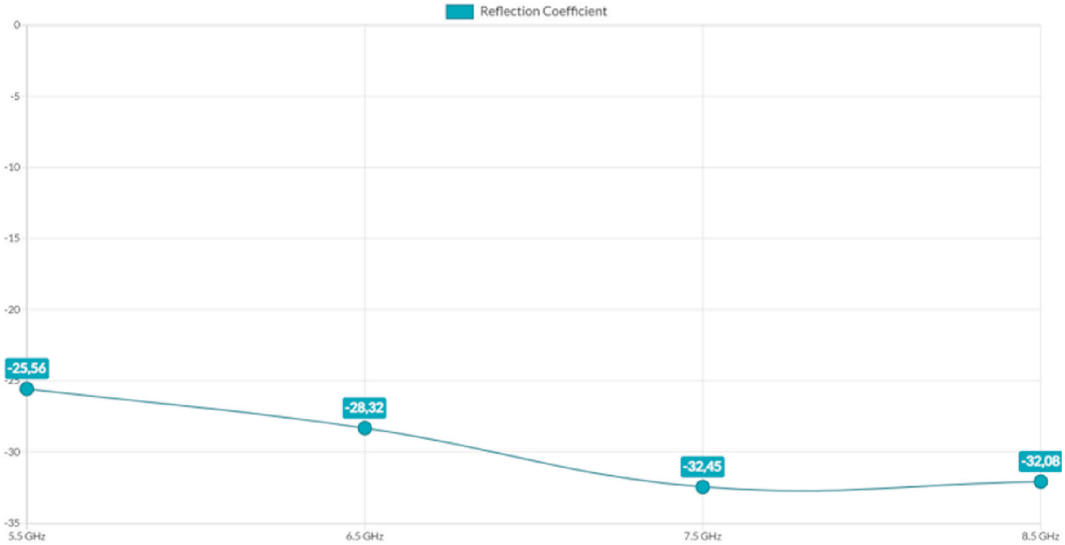

Fig. 11. Reflection coefficient of the proposed system.

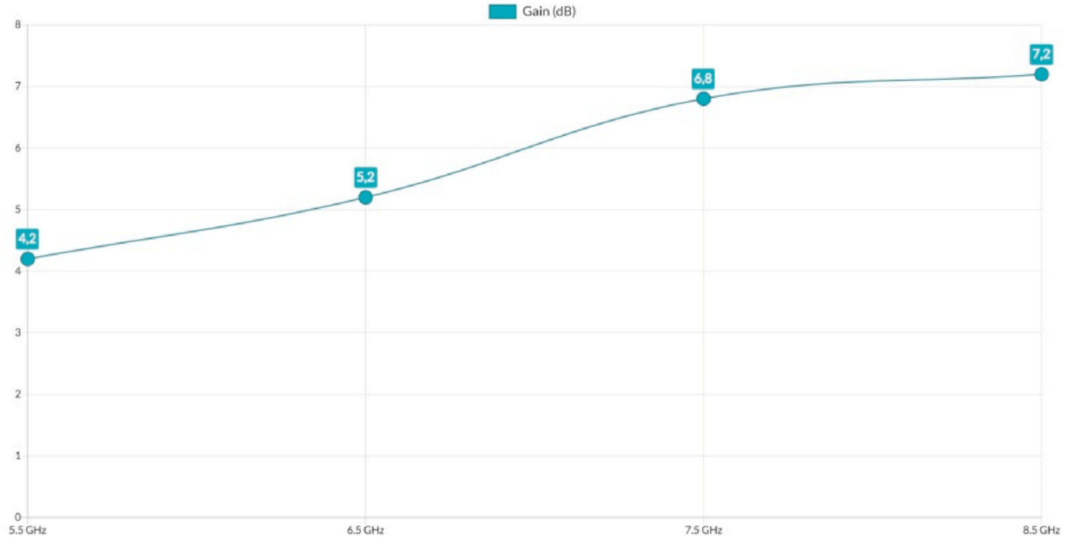

Fig. 12. Gain of the proposed system.

deployed number of nodes, both RTI techniques, and both kinds of building materials. Additionally, we see that as the number of nodes drops, VRTI beats MARTI for all antenna types and construction materials. The radiation pattern of the proposed E-Shaped structure antenna is shown in Fig. 15 (a&b). The figure also demonstrates that employing MARTI over VRTI for the brick home with sixteen nodes results in a 35 % increase in the median RMSE for the microstrip patch antenna, a 28 % increase for the omnidirectional antenna, and a 12 % increase for the E-shaped patch antenna. Instead, if the cement house is used, the microstrip patch antenna's percent increase drops to 10 %, the omnidirectional antenna's to 14 %, and the E-shaped patch antenna's to 15 %. According to our experimental findings, compared to the microstrip patch and omnidirectional antenna, the E-shaped patch antenna's % increase in median RMSE is considerably less reliant on the kind of construction material and RTI technique. The radiation pattern for E-Shaped antenna is shown in Fig. 15 (a & b).

Another intriguing finding is that for the cement board home, the patch and omnidirectional antenna gets the same median RMSE with twenty nodes using either RTI technique as the E-shaped patch antenna does with sixteen nodes with VRTI and seventeen nodes with MARTI. The E-shaped patch antenna can nevertheless achieve equivalent or better localization performance than the other two antennas despite the cement board house's huge size and reduced number of nodes. No of Channels with Median RMSE is shown in Fig. 16. Consequently, we may consume less and utilize fewer nodes. Our nodes are programmed to conduct measurements in our studies on four 7.5 GHz band channels. But what interests us is how the number of channels utilized affects the median RMSE. To

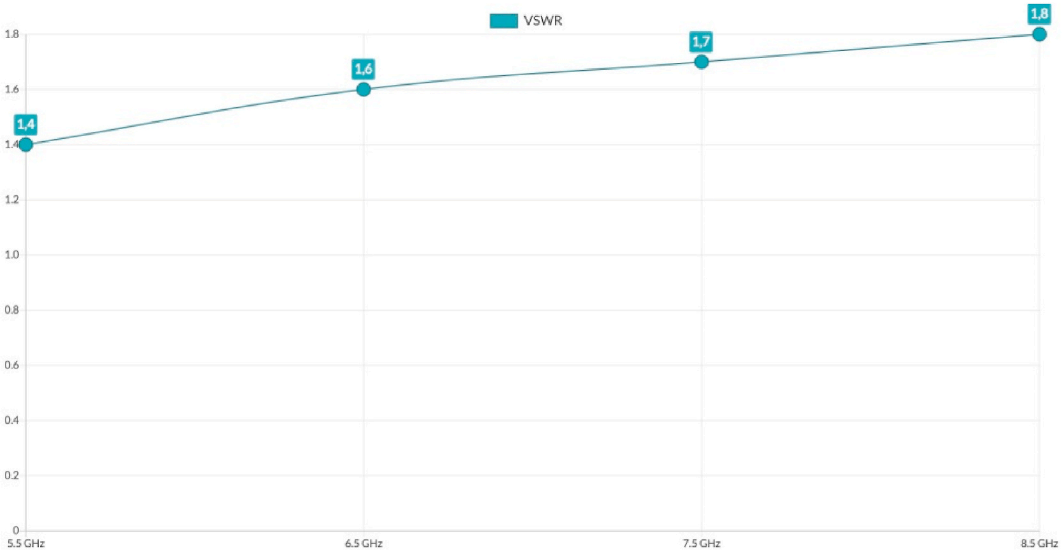

Fig. 13. Vswr of the proposed system.

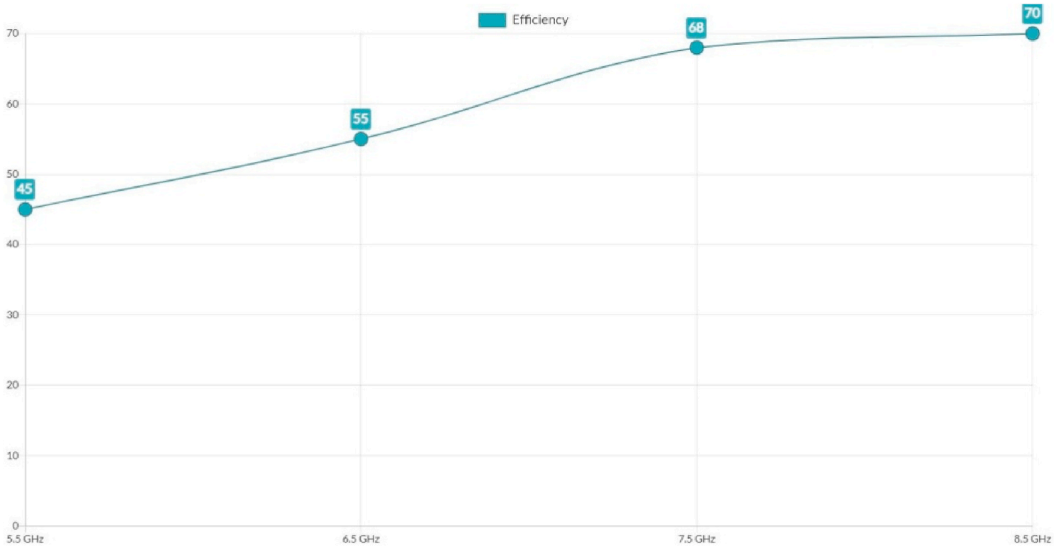

Fig. 14. Efficiency of the proposed system.

Table 2
Performance analysis of proposed E-shaped antenna.

Sl.No	Frequency (GHz)	Reflection Coefficient (dB)	Gain (dB)	VSWR	Efficiency (%)
1	5.5	−25.56	4.2	1.4	45
2	6.5	−28.32	5.2	1.6	55
3	7.5	−32.45	6.8	1.7	68
4	8.5	−34.08	7.2	1.8	70

achieve this, we calculate the median RMSE for Cover all iterations by iterating through all combinations of 4C channels for C 1, 2, 3, 4. The E-shaped patch antenna outperforms the omnidirectional and microstrip patch antenna in terms of median RMSE. No of Nodes with Median RMSE is shown in Fig. 17. Table 3 shows Median RMSE for various nodes and Table 4 shows Median RMSE for various channels.

Table 5 shows the Performance Metrics for various nodes. Additionally, when we measure RSS on fewer channels than VRTI, MARTI is a more reliable localization technique overall. No of Nodes with Accuracy is shown in Fig. 18.

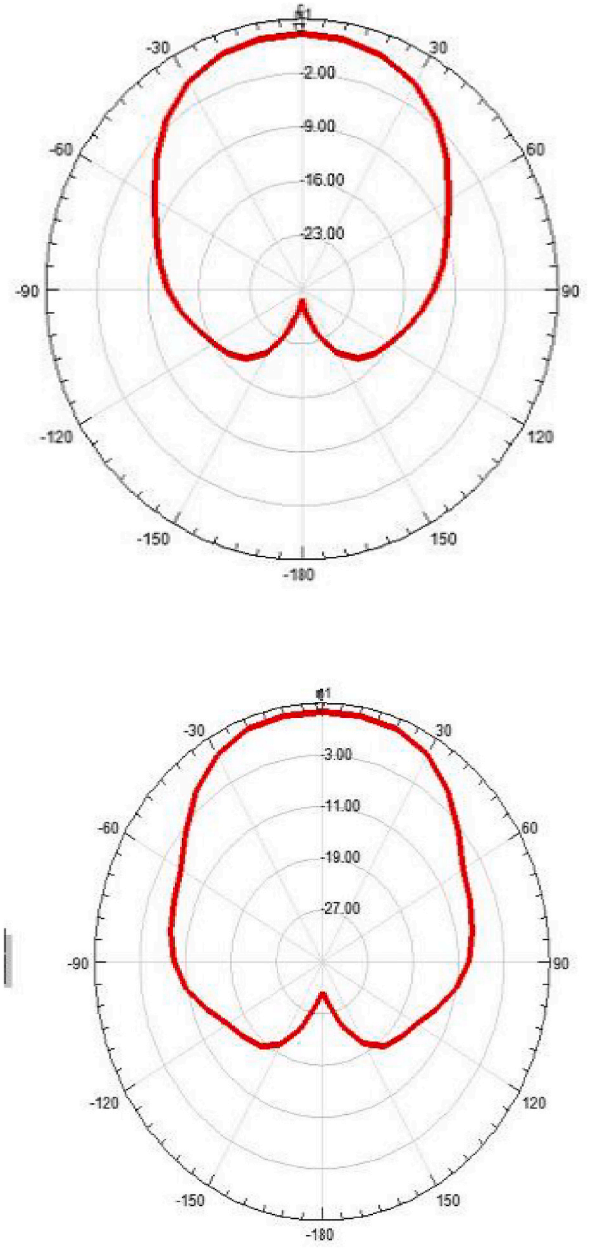

Fig. 15. (a and b): Radiation Pattern of proposed E-shaped antenna.

We discover that, depending on the RTI approach, we may measure on only one channel in the cement board home and outperform the omnidirectional and microstrip patch antenna by 0.85 feet–1.85 feet. The E-shaped patch antenna may achieve a reduced RMSE while conserving power and bandwidth in a power-limited application by simply measuring on one channel. If we take into account both RTI techniques and different dwelling types while using simply the E-shaped patch antenna, we can still observe these power reductions. No of Nodes With precision is shown in Fig. 19. We note that in this instance, employing two channels as opposed to four only results in an increase in the median RMSE of up to 0.4 feet with a halving of the power and bandwidth use. No of Nodes with Recall is shown in Fig. 20.

At VSWR 2, the impedance bandwidth of 32.6 % from 7.5 to 8.5 GHz is attained. The wideband feature is a result of the suggested design's usage of low permittivity substrate and the significant distance between the radiating patch and the ground plane. The greatest gain that can be achieved is 6.6 dB at 7.5 GHz, and 7.8 dB at 8.5 GHz the gain performs consistently across the working range. Over the operating frequency, the proposed antenna's observed overall efficiency averages 90 %. Good broadband radiation patterns are shown by the constructed antenna. Antenna has improved cross-polarization. Because acceptable cross polarization levels in both planes are obtained across the impedance bandwidth, it is noteworthy that the proposed microstrip antenna's radiation characteristics

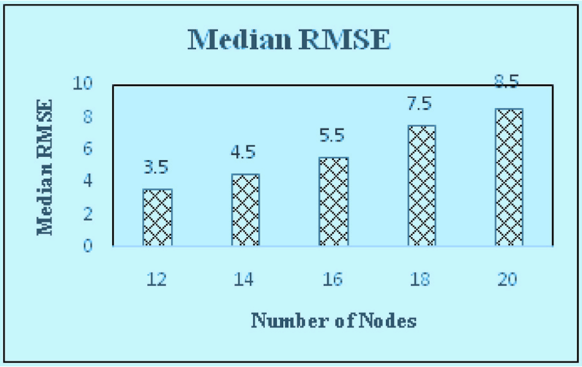

Fig. 16. No of nodes with median RMSE

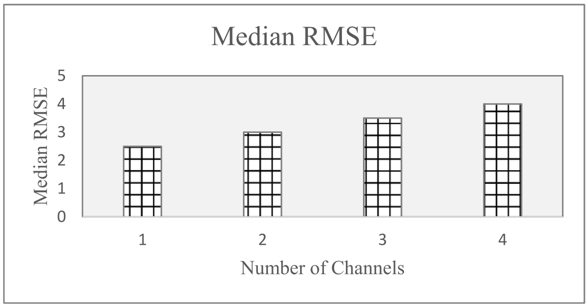

Fig. 17. No of channels with median RMSE

Table 3
Median RMSE vs Number of Nodes.

Sl.NO	Number of Nodes	Median RMSE
1	12	3.5
2	14	4.5
3	16	5.5
4	18	7.5
5	20	8.5

Table 4
Median RMSE vs Number of Channels.

Sl.NO	Number of Channels	Median RMSE
1	1	2.5
2	2	3.0
3	3	3.5
4	4	4.0

Table 5
Performance Metrics for various nodes.

No of Nodes	Accuracy	Precision	Recall	Mean
5	82.56	81.65	83.99	82.56
8	84.25	82.68	85.65	84.68
10	82.68	81.68	84.59	85.55
13	88.65	88.62	88.54	86.88
15	85.67	85.78	86.25	88.25
18	91.25	90.25	90.85	90.25
20	92.85	91.85	91.82	91.25

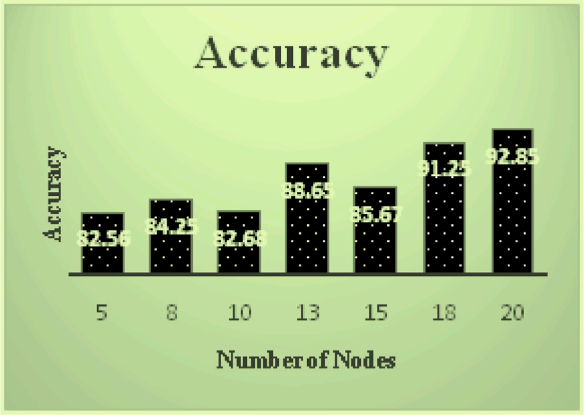

Fig. 18. No of nodes with accuracy.

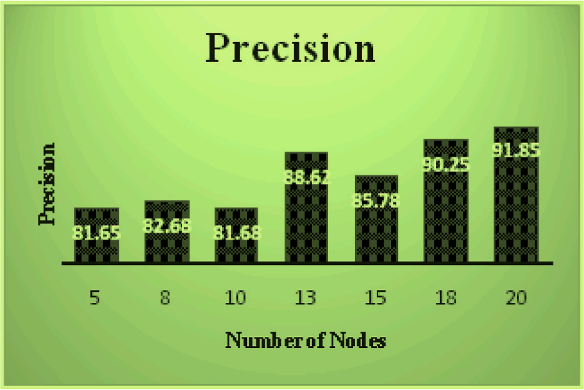

Fig. 19. No of nodes with precision.

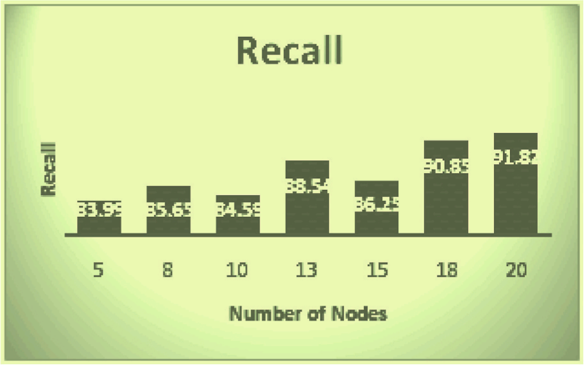

Fig. 20. No of nodes with recall.

are superior to those of the traditional microstrip antenna. High-speed wireless communication systems have been built using a wideband E-shaped microstrip patch antenna. From 7.5 to 8.5 GHz, the reflection coefficient is less than −10dB. Performance exceeds the strict bandwidth requirements to span the 7.5–8.5 GHz frequency spectrum. The measurement results showed that the antenna's radiation performance was stable across its full operational bandwidth. No of Nodes with mean is shown in Fig. 21. By using a substrate material with a low dielectric constant, the antenna is also thin and small. These characteristics are crucial for making wireless communication equipment portable over the globe. The second resonant mode's resonance frequency may be set without changing the basic resonant mode's resonance by placing the feed point at the base of the centre arm rather than its tip. Shortening the middle arm's length makes it simple to adjust the bandwidth. Antenna engineers will find the suggested antenna's improved performance useful for

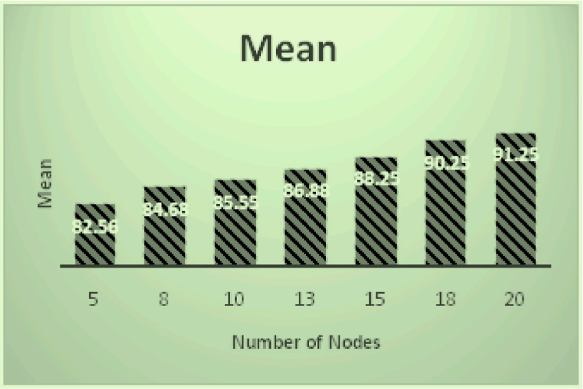

Fig. 21. No of nodes with mean.

designing and refining antennas for indoor wireless applications. Tables 6 and 7 shows overall performance metrics for various nodes.

7. Conclusion

Using a brand-new E-shaped patch antenna, we demonstrated improvements to through-wall RTI systems in this study. To prevent impedance mismatches while in touch with an outside wall, we created the E-shaped patch. The E-shaped patch may radiate its power down the connection line and enhance localization by avoiding impedance mismatches and having a directionality. The E-shaped patch is more suited for usage in security and first aid situations where the antenna must be fastened to an outside wall than conventional omnidirectional and microstrip patch antennas. At a brick-built home and another constructed of cement board, we showed that the E-shaped patch antenna decreased the median RMSE by up to 53 % when compared to a microstrip patch antenna and an omnidirectional antenna. In two examined RTI approaches, the E-shaped patch antenna performed better than the other antennas. We demonstrated that even when utilising fewer nodes and doing RSS measurements on fewer channels, the E-shaped patch antenna achieves a reduced localization RMSE. These performance improvements showed that the E-shaped patch antenna may decrease localization mistakes while operating under a more constrained power and bandwidth budget.

In this study, a switching adaptive beamforming approach combining E-shaped antenna and high-altitude platforms are used to give a novel and effective system. Through enhanced communications connection performance across larger distances, this cutting-edge method has been presented for developing wireless sensor networks employing aerial platforms. Additionally, the newly developed antenna technology makes use of a narrow primary lobe that is pointed towards sensors on the ground to extend the battery life of these sensors, particularly in areas with limited energy sources. The first hypothesis is that nodes may not be correctly orientated when positioned up against a wall in hostage or security situations. In this study, we use an E-shaped patch antenna that is linearly polarised. During the studies, we were able to regulate the antenna direction such that polarization was not an issue. But in other circumstances, the antennas can unintentionally be orientated in a manner that does not match the antenna's linear polarization, which would result in losses. A circular polarised E-shaped patch antenna that may have its antennae orientated in any direction on the outer wall is one potential option.

The relationship between localization accuracy with RTI and link budget is another area that needs further research. The E-shaped patch antenna performed the best in terms of localization accuracy and had the least amount of power loss when put up against a dielectric material. Future study may easily lower the transmit power of the nodes and carry out a comparable localization comparison of other antenna types to demonstrate that localization accuracy is a function of antenna design and not just received signal strength.

Table 6
Overall performance metrics of the proposed system.

No of Nodes	Frequency (GHz)	Reflection Coefficient (dB)		VSWR		Gain(dB)		Efficiency	
		Existing Work	Proposed Work	Existing Work	Proposed Work	Existing Work	Proposed Work	Existing Work	Proposed Work
5	5.5	−22.05 [12]	−25.56	1.2 [17]	1.4	3.2 [27]	4.2	35 [42]	45
10	6.5	−18.25 [18]	−28.32	1.4 [22]	1.6	3.8 [34]	5.2	50 [44]	55
15	7.5	−19.25 [22]	−32.45	1.5 [23]	1.7	4.8 [36]	6.8	60 [46]	68
20	8.5	−25.05 [16]	−34.08	1.6 [40]	1.8	5.2 [38]	7.2	65 [48]	70

Table 7
Overall performance metrics for Median RMSE, Accuracy, Precision, Recall and Mean.

No of Nodes	Median RMSE		Accuracy		Precision		Recall		Mean	
	Existing Work	Proposed Work	Existing Work	Proposed Work	Existing Work	Proposed Work	Existing Work	Proposed Work	Existing Work	Proposed Work
5	1.8 [7]	2.5	81.25 [42]	82.56	80.52 [34]	81.65	82.55 [16]	83.99	81.25 [18]	82.56
10	2.5 [19]	3.0	83.25 [40]	84.25	81.25 [36]	82.68	85.25 [18]	85.65	82.56 [22]	84.68
15	3.0 [22]	3.5	80.25 [38]	82.68	80.56 [38]	81.68	83.25 [22]	84.59	84.56 [28]	85.55
20	3.5 [24]	4.0	85.32 [36]	88.65	85.68 [40]	88.62	85.36 [32]	88.54	85.25 [30]	86.88

Data availability statement

No data were used in this article.

CRediT authorship contribution statement

S.Kannadhasan: Writing – review & editing, Writing – original draft, Methodology, Formal analysis, Data curation, Conceptualization. **R.Nagarajan:** Writing – review & editing, Writing – original draft, Validation, Formal analysis, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] F. Zhang, H.A.D.E. Kodituwakku, W. Hines, J.B. Coble, Multi-layer data-driven cyber-attack DetectionSystem for industrial control systems based on network, system and process data, IEEE Trans. Ind. Inform. 15 (2019) 4362–4369.

[2] A.H. Hamamoto, L.F. Carvalho, L.D.H. Sampaio, T. Abrão, M.L. Proença Jr., Network anomaly detectionsystem using genetic algorithm and fuzzy logic, Expert Syst. Appl. 92 (2018) 390–402.

[3] S.S.S. Reddy, P. Chatterjee, C. Mamatha, Intrusion detection in wireless network using fuzzy LogicImplemented with genetic algorithm, in: Computing and Network Sustainability, Springer, Singapore, 2019, pp. 425–432.

[4] Y. Zhang, P. Li, X. Wang, Intrusion detection for IoT based on improved genetic algorithm and deep BeliefNetwork, IEEE Access 7 (2019) 31711–31722.

[5] C. Azad, V.K. Jha, Decision tree and genetic algorithm based intrusion detection system, in: Proceedingof the Second International Conference on Microelectronics, Computing & Communication Systems (MCCS 2017), Springer, Singapore, 2019, pp. 141–152.

[6] J. Ren, J. Guo, Q. Wang, Y. Huang, X. Hao, J. Hu, Building an E_ective intrusion detection systemby using hybrid data optimization based on machine learning algorithms, Secur. Commun. Netw. 2019 (2019) 7130868.

[7] A.D. Wood, J.A. Stankovic, Denial of service in sensor networks, IEEE Comput 35 (2002) 54–62.

[8] G. Li, J. He, Y. Fu, Group-based intrusion detection system in wireless sensor networks, Comput. Commun. 31 (2008) 4324–4332.

[9] M.R. Parsaei, S.M. Rostami, R. Javidan, ″A hybrid data miningapproach for intrusion detection on imbalanced NSL-KDD dataset,'', Int. J. Adv. Comput. Sci. Appl. 7 (6) (2016) 20–25.

[10] K.A. Taher, B. Mohammed Yasin Jisan, M.M. Rahman, ″Networkintrusion detection using supervised machine learning techniquewith feature selection,'', in: Proc. Int. Conf. Robot., Electr. Signal Process.Techn. (ICREST), Jan. 2019, pp. 643–646.

[11] A. Tesfahun, D.L. Bhaskari, ″Intrusion detection using random forestsclassi_er with SMOTE and feature reduction,'', in: Proc. Int. Conf. Cloud Ubiquitous Comput. Emerg. Technol., Nov. 2013, pp. 127–132.

[12] A. Chandra, S.K. Khatri, R. Simon, ″Filter-based attribute selectionapproach for intrusion detection using k-means clustering and sequentialminimal optimization techniq,'', in: Proc. Amity Int. Conf. Artif.Intell. (AICAI), Feb. 2019, pp. 740–745.

[13] N. Qazi, K. Raza, ″Effect of feature selection, SMOTE and undersampling on class imbalance classi_cation,'', in: Proc. UKSim 14th Int.Conf. Comput. Modeling Simulation, Mar. 2012, pp. 145–150.

[14] A.I. Al-issa, M. Al-Akhras, M.S. Alsahli, M. Alawairdhi, ″Usingmachine learning to detect DoS attacks in wireless sensor networks,'', in: Proc. IEEE Jordan Int. Joint Conf. Electr. Eng. Inf. Technol. (JEEIT), Apr. 2019, pp. 107–112.

[15] A. Javaid, Q. Niyaz, W. Sun, M. Alam, ″A deep learning approachfor network intrusion detection system,'', in: Proc. 9th EAI Int. Conf. Bio-Inspired Inf. Commun. Technol. (Formerly BIONETICS), 2016, pp. 21–26.

[16] P. Torres, C. Catania, S. Garcia, C.G. Garino, ″An analysis of recurrentneural networks for botnet detection behavior,'', in: Proc. IEEE Biennial Congr. Argentina (ARGENCON), Jun. 2016, pp. 1–6.

[17] W. Wang, M. Zhu, X. Zeng, X. Ye, Y. Sheng, ″Malware traf_cclas-si_cation using convolutional neural network for representation learning,'', in: Proc. Int. Conf. Inf. Netw. (ICOIN), 2017, pp. 712–717.

[18] D. Kwon, H. Kim, J. Kim, S.C. Suh, I. Kim, K.J. Kim, ″A surveyof deep learning-based network anomaly detection,'', Cluster Comput. 22 (2019) 949–961.

[19] B.A. Tama, M. Comuzzi, K.-H. Rhee, ″TSE-IDS: a two-stage clas-si_er ensemble for intelligent anomaly-based intrusion detection system,'', IEEE Access 7 (2019) 94497–94507.

[20] P. Jeatrakul, K.W. Wong, C.C. Fung, ″Classi_cation of imbal-anced data by combining the complementary neural network and smotealgorithm,'', in: Proc. Int. Conf. Neural Inf. Process., Springer, 2010, pp. 152–159.

[21] B. Yan, G. Han, ″LA-GRU: building combined intrusion detectionmodel based on imbalanced learning and gated recurrent unit neural net-work,'', Secur. Commun. Netw. 2018 (Aug. 2018) 1–13.

[22] R. Abdulhammed, M. Faezipour, A. Abuzneid, A. AbuMallouh, ″Deep and machine learning approaches for anomaly-based intrusiondetection of imbalanced network traf_c,'', IEEE sensors Lett 3 (1) (Jan. 2019). Art. no. 7101404.

[23] Wendi RabinerHeinzelman, Anantha Chandrakasan, Hari Balakrishnan, Energy-efficient communicationprotocol for wireless microsensor networks, in: Proceedings of the 33rd Annual Hawaii International Conferenceon System Sciences, IEEE, 2000, p. 10.

[24] Huafeng Liu, Liang Li, ShiyaoJin. Cluster number variability problem in leach, in: International Conferenceon Ubiquitous Intelligence and Computing, Springer, 2006, pp. 429–437.

[25] Wendi B. Heinzelman, Anantha P. Chandrakasan, Hari Balakrishnan, An application-specific protocolarchitecture for wireless microsensor networks, IEEE Trans. Wireless Commun. 1 (4) (2002) 660–670.

[26] David H. Wolpert, William G. Macready, No free lunch theorems for optimization, IEEE transactions onevolutionary computation 1 (1) (1997) 67–82.

[27] Pamela K. Douglas, Sam Harris, Alan Yuille, Mark S. Cohen, Performance comparison of machine learningalgorithms and number of independent components used in fmri decoding of belief vs. disbelief, Neuroimage 56 (2) (2011) 544–553.

[28] Zhenghui Ma, Ata Kaban, K-nearest-neighbours with a novel similarity measure for intrusion detection. In2013 13th UK Workshop on Computational Intelligence (UKCI), IEEE, 2013, pp. 266–271.

[29] Thomas Cover, Peter Hart, Nearest neighbor pattern classification, IEEE Trans. Inf. Theor. 13 (1) (1967) 21–27.

[30] Sotiris B. Kotsiantis, I. Zaharakis, P. Pintelas, et al., Supervised machine learning: a review of classificationtechniques, Emerging artificial intelligence applications in computer engineering 160 (1) (2007) 3–24.

[31] K. Jaiswal, S. Yadav, N. Yadav, et al., Analysis of different feeding techniques of butterflyshaped patch antenna with defected ground for UWB application, IETE J. Res. (2022) 3647–3656, https://doi.org/10.1080/03772063.2020.1773947.

[32] G. Geetharamani, T. Aathmanesan, A metamaterial inspired tapered patch antenna for WLAN/WiMAX applications, Wirel Pers Commun (2020), https://doi.org/10.1007/s11277-020-07283-5.

[33] S.A. Tazehabadi, S. Jam, X-band reflectarray antenna with arbitrarily (elliptical) polarization for high-power microwave applications, Eng Sci Technol an Int J (2020), https://doi.org/10.1016/j.jestch.2019.08.004.

[34] Kiourti A, Volakis JL, Roy BVB. Simorangkir and Syed Muzahir Abbas, UWB Antennas on Conductive Textiles, 2016 International Symposium on Antennas and Propagation (APSURSI), ISSN. 978-1-5090-2886-3, pp. 1941-1942.

[35] Shikder K, Arifin F. Design and Evaluation of a UWB Wearable Textile Antenna for Body Area Network, International Conference on Electrical Information and Communication Technology (EICT 2015),ISSN-978-1-4673-9257-0, pp. 326-330.

3[6] Troester G. KlemmM, TextileUWBantennas for wireless body area networks, IEEE Trans Antennas Propag. 54 (11) (2006) 3192–3197.

[37] Holland SA, Baiya D, Elkhouly E, et al. Ultra Wideband Textile Antenna Development for Indoor Localization, IEEE MTT-S International Microwave Symposium Digest(MTT), ISSN. 978-1-4673-2141-9, 2013.

[38] M. Alibakhshi-Kenari, M. Naser-Moghadasi, R.A. Sadeghzadeh, et al., Bandwidth extension of planar antennas using embedded slits for reliable multiband RF communications, AEU - Int J Electron Commun. 70 (7) (2016) 910–919, https://doi.org/10.1016/j.aeue.2016.04.003.

[39] K. Meena alias Jeyanthi, E. Thangaselvi, A.S. Prianga, Simulation of rectangular microstrip antenna using nylon fabric material, Int J Emerg Technol Adv Eng 3 (1) (Jan 2013) 645–647.

[40] S. Maria Glammi, K. Meena Alias Jeyanthi, Design of wide band and rectangular microstrip patch antenna for breast tumor detection, Int. J. Recent Technol. Eng. 7 (5S3) (February 2019).

[41] Md Gazi, Habibul Bashar, Mohammod Abul Kashem, Liton Chandra Paul, "Intrusion detection for cyber-physical security system using long short-term memory model", Sci. Program. (2022) 11, https://doi.org/10.1155/2022/6172362, 2022, Article ID 6172362.

[42] Liton Chandra Paul, Sarker Saleh Ahmed Ankan, Tithi Rani, Md Tanvir Rahman Jim, Muharrem Karaaslan, Sk A. Shezan, Lulu Wang, "Design and characterization of a compact four-element microstrip array antenna for WiFi-5/6 routers", Int. J. RF Microw. Computer-Aided Eng. (2023) 13, https://doi.org/10.1155/2023/6640730, 2023, Article ID 6640730.