Lifetime Escalation and Clone Detection in Wireless Sensor Networks using Snowball Endurance Algorithm(SBEA)

V. Sathya[1*], and Dr. S. Kannan[2]
[1]Assistant Professor, Department of CSE, S.A Engineering College, Chennai, Tamil Nadu, India- 609305
[Email: saro.sath@gmail.com]
[2]Professor, Department of CSE, E.G.S Pillai Engineering College, Nagapattinam, Tamil Nadu, India- -611002
[Email: kannan@egspec.org]
Corresponding author: V. Sathya

Received May 8, 2021; revised August 25, 2021; accepted February 21, 2022; published April 30, 2022

Abstract

In various sensor network applications, such as climate observation organizations, sensor nodes need to collect information from time to time and pass it on to the recipient of information through multiple bounces. According to field tests, this information corresponds to most of the energy use of the sensor hub. Decreasing the measurement of information transmission in sensor networks becomes an important issue.Compression sensing (CS) can reduce the amount of information delivered to the network and reduce traffic load. However, the total number of classification of information delivered using pure CS is still enormous. The hybrid technique for utilizing CS was proposed to diminish the quantity of transmissions in sensor networks.Further the energy productivity is a test task for the sensor nodes. However, in previous studies, a clustering approach using hybrid CS for a sensor network and an explanatory model was used to investigate the relationship between beam size and number of transmissions of hybrid CS technology. It uses efficient data integration techniques for large networks, but leads to clone attacks or attacks. Here, a new algorithm called SBEA (Snowball Endurance Algorithm) was proposed and tested with a bow. Thus, you can extend the battery life of your WSN by running effective copy detection. Often, multiple nodes, called observers, are selected to verify the reliability of the nodes within the network. Personal data from the source centre (e.g. personality and geographical data) is provided to the observer at the optional witness stage. The trust and reputation system is used to find the reliability of data aggregation across the cluster head and cluster nodes. It is also possible to obtain a mechanism to perform sleep and standby procedures to improve the life of the sensor node. The sniffers have been implemented to monitor the energy of the sensor nodes periodically in the sink. The proposed algorithm SBEA (Snowball Endurance Algorithm) is a combination of ERCD protocol and a combined mobility and routing

http://doi.org/10.3837/tiis.2022.04.008 **ISSN : 1976-7277**

algorithm that can identify the cluster head and adjacent cluster head nodes.This algorithm is used to yield the network life time and the performance of the sensor nodes can be increased.

Keywords: Clone detection, Compressive Sensing, Life time escalation, Sleep and wake-up technique, SBEA, Wireless Sensor Network.

1. Introduction

A wireless sensor network (WSN) refers to a group of spatially distributed dedicated sensors used to monitor and record the physical condition of the environment and organize the collected data in a central location.WSN measures environmental conditions such as temperature, sound, pollution level, humidity and air. In a sense, it resembles a wireless ad-hoc network, relying on wireless connectivity and spontaneous network development, allowing sensor data to be transmitted wirelessly. The WSN is a spatially distributed autonomous sensor used to monitor physical or environmental conditions such as temperature, sound, pressure, etc.Modern networks are bidirectional and can collect data from distributed sensors and control sensor activity. The development of wireless sensor networks is driven by military applications such as battlefield monitoring. Today, these networks are used in a variety of industrial and consumer applications, including industrial process monitoring and condition monitoring of control machines.

A WSN consists of several to hundreds or even thousands of "nodes", each of which is connected to one (and in some cases many) sensors. Each of these network nodes usually has many components. Energy is used for interfering with wireless transceivers, microcomputers, electronic circuits, sensors with internal antennas or connected to external antennas, standard batteries or containing energy collectors[1]. The size of the sensor node can vary from the size of a shoebox to the size of a particle of dust, but the actual microscale "motive" that works has not yet been created.The cost of sensor nodes also varies and ranges from a few dollars to hundreds of dollars depending on the complexity of each sensor node. Due to the size and cost constraints of the sensor node, resources such as energy memory calculation speed, communication bandwidth, etc. are limited.WSN topologies range from simple star networks to advanced multi-hop wireless mesh networks. Propagation technology between network hops can be routine or flooding.

The main application areas of WSN are as follows:

- Area checking
- Health care checking
- Environmental/Earth detecting
- Air contamination checking
- Forest fire recognition
- Land slide recognition
- Water quality checking
- Natural catastrophe avoidance
- Industrial checking
- Machine wellbeing checking
- Data logging

- Water/squander water checking
- Structural wellbeing checking
- Wine creation
- Threat recognition

Energy gathering is the cycle by which energy is derived from outside sources caught, and put away for little, wireless self-governing gadgets, similar to those utilized in wearable hardware and wireless sensor networks[11]. Energy collectors give a limited quantity of intensity for low-energy gadgets. Fuel fuel in information consumes a lot ofassets (petroleum, coal, etc.) to a certain extent, but energy collectors 'energy hotspots can still be used as a basis for their environment[2].For example, there is a large amount of electronic energy in the climate due to the combustion of electric motors and in large cities the temperature gradient caused by radio and television broadcasts. The main operations of energy harvesters can be given as

- Accumulating energy
- Storage of power
- Use of the power

An aggressor tries to add a node to a current sensor network by duplicating the ID of a current sensor hub. A hub cloned in this methodology can seriously upset a sensor network's presentation. Bundles can be rebuilt or even misrouted. This can be given as clone attack. There are of several types such as: Replication attack, sybil attack etc. This paper has been organized in such a way that section-II describes the related work to the research article. Section -III describes the architecture and working principles of SBEA (Snow Ball Endurance Algorithm). Section – IV describes the implementation details and Section – V gives about the conclusion and future work.

2. Related Works

2.1. Data collection method with sink node

Each node in the sensor network contains 3 subsystems. One is the first subsystem of the sensor that detects climate, the other is the second subsystem of processing that conducts proximity calculations to the detected data, and the other is responsible for message transactions. In antiquated occasions, just a single versatile sink node travel in detecting territory and gather data from the sensors[4]. Versatile sink node gather the data legitimately utilizing one expectation transmission from the sensor or some time utilizing multi-jump transmission. Sometimes bunch method is utilized for the data assortment from sensor. In this method, a portable receiver node collects data from the beamhead and stores the data in a database (base station). Data gathered from sensor is put away on the doors then versatile sink gets that data and put away on the Database (Base station) this is again one procedure for data assortment cycle and some time data assortment is accomplished utilizing the steering convention.

2.2. Clone attack detection

WSN can be static or portable. For static WSN sensor nodes, the sensor nodes are sent randomly and their location does not change after transmission. With the portable WSN, sensor nodes can move their own sensors after transmission.The 2 batches, accessible from static WSNs, are centralized and decentralized. When another node joins the organization in a unified way to identify node replication, a zone guarantee is passed to adjacent nodes,

including those zones and attributes.At this time, at least one nearby to send the local warranty to the base station. The base station can easily differentiate between pairs of nodes with similar characteristics in each region using the data of all nodes in the organization[5].The biggest obstacle to this method is that if the base station is damaged or interferes with the base station path, the enemy may contain multiple copies in the organization. The distributed method of identifying cloned nodes depends on field data from nodes placed on at least one observer node in the organization. When another node joins the organization, its local endorsement is transferred to the comparison observation node. If an observer node receives 2 distinct kingdom declarations with similar node IDs, the presence of a clone is recognized at this point. Both methods use different rules to identify replication attacks.

2.3. MCMS Problem

In a directional sensor network (DSN), the maximum objective coverage and minimum number of sensor nodes (called MCMS issues) is a big problem. The directional sensor network (DSN) [3] consists of a number of directional sensor widgets that send reports of detected events to recipients. In contrast to unidirectional sensors, the directional sensors have restricted scope of detecting and correspondence points[6]. They advance detecting and correspondence characteristics by centering transmission one way and consequently upgrade the organization execution by expanding the detecting quality and diminishing impedance and blurring. For ensured inclusion and occasion revealing, the basic component must guarantee that all objectives are secured by the sensors and the subsequent organization is associated. an energy-effective answer for the MCMS issue through the disseminated bunching instrument in directional sensor networks can be resolved in TCDC (Target Coverage through Distributed Clustering) algorithm which consists of four phases such as: cluster formation, gate-way selection, target coverage and improvement.Eventhough it has been analyzed the data cant’t be selected dynamically.

2.4. Intrusion detection

Intrusion Detection Systems (IDS) scans network traffic for suspicious behaviour and alerts on the framework or leaders of the organization. IDS can respond multiple times to unusual or malicious traffic and do so to prevent customers and resources of IP addresses from entering your organization. SCADA a successful framework utilize a wired or remote sensor networks as a vehicle climate for social event telemetry data and sending orders to execute gadgets[7]. However, because of interior powers the intruders may endure as opposed to the outside powers.

2.5. Multiple Static Sink Model(MSSM)

The portable client communicates with the receiver through the sensor network to combine data such as victim area data into victim area to navigate sensor area. Different static receivers interact with the inherited tissue and divide the sensor field into the number of different recipients[8]. By owning an organization to share queries and data, different static recipients provide high throughput through a combination of periodic data, and the transmission of data through Short jumping can reduce inactivity. Various static sinks convey the aggregated data to the distant clients by means of the heritage organizations. at the point when a portable client moves around, it gets the accumulated data from the closest static sink. networks in the edges of sensor organize and discuss legitimately with one

another through the inheritance networks. It permits the various static sinks to play out the capacity as entryways for clients in different networks by means of the inheritance networks.

2.6. Clone detection approaches in static wireless sensor networks

There are two types of wireless sensor networks, fixed and mobile. Static wireless sensor networks do not change state even after sensor nodes by the organization. The position of the sensor node is essentially static. In the following types (mobile wireless sensor network), the sensor node can change the state as needed[9,10]. So the sensor node is essentially portable. Static and portable remote sensor organizations have many ways to distinguish between replica node attacks. Static WSNs have two methods for identifying between replica nodes. It is intensive and decentralized. There is direct planning in a unified way, set the delivery contract pair of continuous discovery contract circle robin communication contract deterministic multicast (DM) contract random multicast (RM) contract and multi-line options.

2.7. Compressive Sensing

The compression detection technique can be used to realize continuous data transmission over the wireless sensor network. This can reduce the amount of close counting and sensor data that needs to be sent to complex locations over long distances via wireless channel. Scattered sensors are sent over huge sensor fields and impart wirelessly to the combination community. Far off sensor frequently depend on battery power and are energy compelled. Data tests at distant sensor exhibits subsequently should be packed before sending to the combination place to preserve energy expended for wireless correspondence [19]. Compressive Sensing (CS) innovation misuses the common meager property of practically a wide range of sign and reproduces it from significantly diminished arbitrary estimation of high dimensional crude sign with high likelihood. CS performs measurement decrease with projection figuring. This has been accomplished by the two methods (i) random compressed sampling and (ii) 1-bit compressive sensing.

2.8. Energy efficient routing techniques

To extend the life of the sensor node, steering energy production limits the maintenance cost and puts the overall expansion of the node display. Directing conventions are characterized into three classes: Flat-based steering (Flooding), Hierarchical based directing (Clustering) and Location-based directing (Geographic), contingent upon the organization structure in WSNs. In flat - based routing it is unimaginable to expect to dole out worldwide identifiers to every node in wireless sensor networks due to thick arrangement and dynamic climate of sensor nodes [20]. Despite the fact that flooding is exceptionally simple, it has a few downsides like collapse, cover and asset visual deficiency issue. Turning rules override these shortcomings, but it is unclear whether the data can be expected to reach the target, and a high density of dispersion even if the data active node is far from the source and will not be affected by the node between the resource and the target. Not helpful if you need nodes. Triggered by data, this data is never transferred to the target in any imaginable way. Coordinated Diffusion requires nonstop data conveyance. So it isn't appropriate for ecological observing. Energy-mindful steering needs to trade nearby data between neighbor nodes and all nodes have a bound together location, which augments the cost of building directing ways. MIN is the energy proficient plan as it builds the likelihood that a node with higher remaining energy is chosen regardless of whether its good ways from objective is to some degree more when contrasted with that for another node with a lesser incentive for

leftover energy. Various leveled steering keeps up the energy utilization of sensor nodes and performs data accumulation which helps in diminishing the quantity of sent messages to base station. In hierarchical basedclustering LEACH, PEGASIS and TEEN conventions can been utilized to course the data. In area based steering area data is needed to ascertain the separation between two specific nodes based on signal quality so energy utilization can be assessed. MECN, GEAR and GAF conventions are utilized here.

3. Architecture And Working Principles Of Snow Ball Endurance Algorithm (SBEA)

3.1. Snow Ball Endurance Algorithm

In this section, we introduce our life time escalation and clone detection algorithm, namely SBEA, which can accomplish a high clone recognition likelihood with practically zero negative effect on network lifetime and restricted prerequisite of cradle stockpiling limit. This SBEA is the combination of ERCD convention and joint-mobility routing algorithm. The ERCD convention comprises of two phases:

- Witness selection
- Legitimacy verification.

The joint-mobility routing algorithm consists of two stages:

- Optimal hop count routing.
- Minimum power over progress routing.

Turning rules override these shortcomings, but it is unclear whether the data can be expected to reach the target, and a high density of dispersion even if the data active node is far from the source and will not be affected by the node between the resource and the target. Not helpful if you need nodes. Triggered by data, this data is never transferred to the target in any imaginable way. When the witness receives a confirmation message, all messages are sent to the witness header because the inspection request is sent from the source centre to the witness containing the personal data of the resource centre. If the witness receives the inspection message, all messages are sent to the witness header for verification. Here, the witness header is responsible for determining whether the source of the node is legitimate or not by displaying messages collected from all witnesses.If the received message is not the same as an already logged message, or if the message ends, the monitor header reports the victim of the clone attack, triggering the cancellation method.

With optimal hop transfer, whenever you select an adjacent centre that holds the current central point, the gap between the current centre and the adjacent centre point is closest to the perfect partition. That is, the neighbours closest to the perfect place are selected. People only think of neighbours who are closer to the object than the current centre. If not like a neighbour, of course, the reason for the failure is calculated from the current central point. The route calculation starts at the source.

In minimum power over progress routing stage it restricts the transmission energy of unit advance in picking a sending neighbour. The basic idea of our second routing calculation is to limit the submission of submission orders to each continuous development. Route calculation begins at 'source. Whenever the current central point u of the path is as follows: If nothing is closer to "u" itself, "u" reports "root failure" in "s". The difference is to select the middle point "v" where the'u 'is limited.

3.1.1. Algorithm: Snow Ball Endurance Algorithm

This Snow Ball Endurance algorithm is the combination of Energy-Efficient Ring Based Clone Detection algorithm and Joint Mobility Routing Algorithm. This algorithm will benefits the WSN in the following ways.

- Initialize the ring list of each sensor center point.
- Exchange the overall data with neighbors.
- Route affirmation.
- Minimum power utilization.

3.2. STAGE I: Witness selection

STEP 1: Generating the private key **'K_a'** and witness ring index of node **'A'** (ie) **'J^w_a'** by encrypting and pseudo randomizing **ID_a, l_a**and **h_a**.

Where,

ID_a →The personality data of 'a'.

l_a→ The location 'a' cases to involve.

h_a→ The bounce range from 'a' to the sink.

STEP 2: When the ring index of **'a' (**ie) '**J_a'** is not equal to **'J^w_a'** assign the randomly selected node on incremented ring index to cloned node **(A').** Otherwise assign the randomly selected node on decremented ring index to cloned **(A').**

STEP 3: Accelerate the generated key **'K_a'** to the cloned node **(a').**

STEP 4: Randomly choose another two nodes **'B'** and 'C' on witness ring index of **'A'**. Then record the values of**ID_a, l_a, τ_a**from the private key **'K_a'** to **'B'.**

Where,

τ_a → The timer of **'A**'s**'** verification from private key.

STEP 5: When node 'C' is not equal to node 'B' then record the values of**ID_a, l_a, τ_a**from the private key **'K_a'** to **'C'.** Include **'C'** to the set of witness (ie) **'W_a'**. Then **'C'** is considered as the farthest node from the witness ring index of **'A'.**

3.3. STAGE II: Legitimacy Verification

STEP 1: Generating the private key **'K_a'** and witness ring index of node **'a'** (ie) **'J^w_a'** by encrypting and pseudo randomizing **ID_a, l_a**and **h_a**.

Where,

ID_a →The personality data of 'a'.

l_a→ The location 'a' cases to involve.

h_a→ The bounce range from 'a' to the sink.

STEP 2: Assign the ring index of 'A' to the first node just as the cloned node.

STEP 3: When the cloned node's response value is less than the witness ring index of **'A'** and the value of **'J^w_a+2'** is not equal to the original node and when **(J')** value is less than witness ring index of **'A'** incremented by 2, then select the next node in ***STAGE I o***n **(J+1)th** ring. Increment **'J'**. Otherwise decrement **'J'**.

STEP 4: When the value of **(J)** is equal to (or) incremented (or) decremented to the value of witness ring index of **'A'** then transmit **'Ka'**.

STEP 5: For all individual witness **'w_i'** belongs to the set of witnesses then check whether **'K_a'** hears the individual witness **'w_i'** then direct **'K_a'** to **'S_a'** in the **'B's'** node.
Where,

S_a → Witness header of **'A'.**

STEP 6: When witness header value is not equal to the parameters **(ID_a, l_a)** in private key and time is greater that the timer verification value of private key the trigger the repudiation procedure.

3.4. STAGE III: Optimal hop count routing

STEP 1: Calculate the distance between the two nodes of **'B'** and **'C'**. And it can be **d(B,C).**

STEP 2: Then round the calculated value (ie) **d(B,C)* ((α–1)/t)1/ α** to the nearest integer **'k'**.
Where,

d → Communication remoteness.
α → Signal decline factor.
t → Constant.
k → Integer.

STEP 3: Compute the optimal separation of adjoining nodes by partitioning the closest integer**'k'** with the remoteness value.

STEP 4: When the integer value is less than or equal tozero and the distance value is less than or equal to **'r'**, then **'B'** transmits directly to **'C'**.
Where,

r → route breakdown.

STEP 5: When **'C'**is not reached and route breakdown is not found, then check the distance between current node to the new node and new node to the destination node.
Where,

B → Source node.
C → Destination node.
u→ Current node.
v → New node.

Then **'u'** reports failure to **'B'**.

STEP 6: In any case current node chooses new hub with the end goal that **(d(u,v)- d(B,C)/k)** is limited. 'u' communicates 'v' a course revelation packet joined with **d(B,C)/k**.

3.5. STAGE IV: Minimum power over progress routing

STEP 1: When **'C'** is not reached and route breakdown is not found check whether the remoteness between **'u'** and **'v'** is less than or equivalent to **'r'** and the remoteness between **'v'** and **'C'** is less than or equal to the distance between **'u'** and **'C'**.

STEP 2: **'u'** reports route breakdown to **'B'**.

STEP 3: Otherwise **'u'** selects neighbour **'v'** such that **(d(u,v) α+f)/(d(u,C)-d(v,C)))** is minimized.

STEP 4: **'u'** communicates **'v'** a course discovery packet joined with area of **'C'**

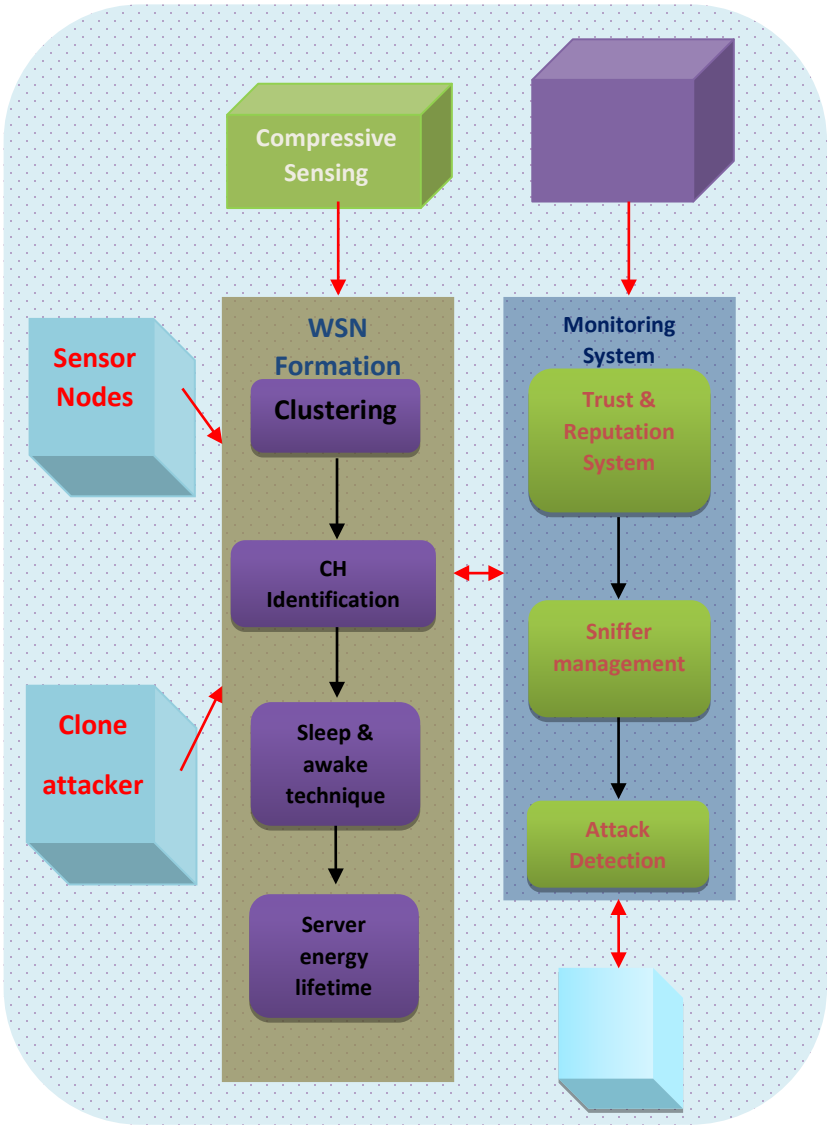

Fig. 1. Architecture of SBEA

3.6. Compressive sensing

By significantly reducing the amount of close computational and sensor information that must be transmitted over a remote coupled area to a wireless channel, compression sensing can be used to realize the specific transmission of information to the wireless sensor network.

It expresses that a sparse sign might be arbitrarily inspected at sub-Nyquist rate and be recreated perfectly.

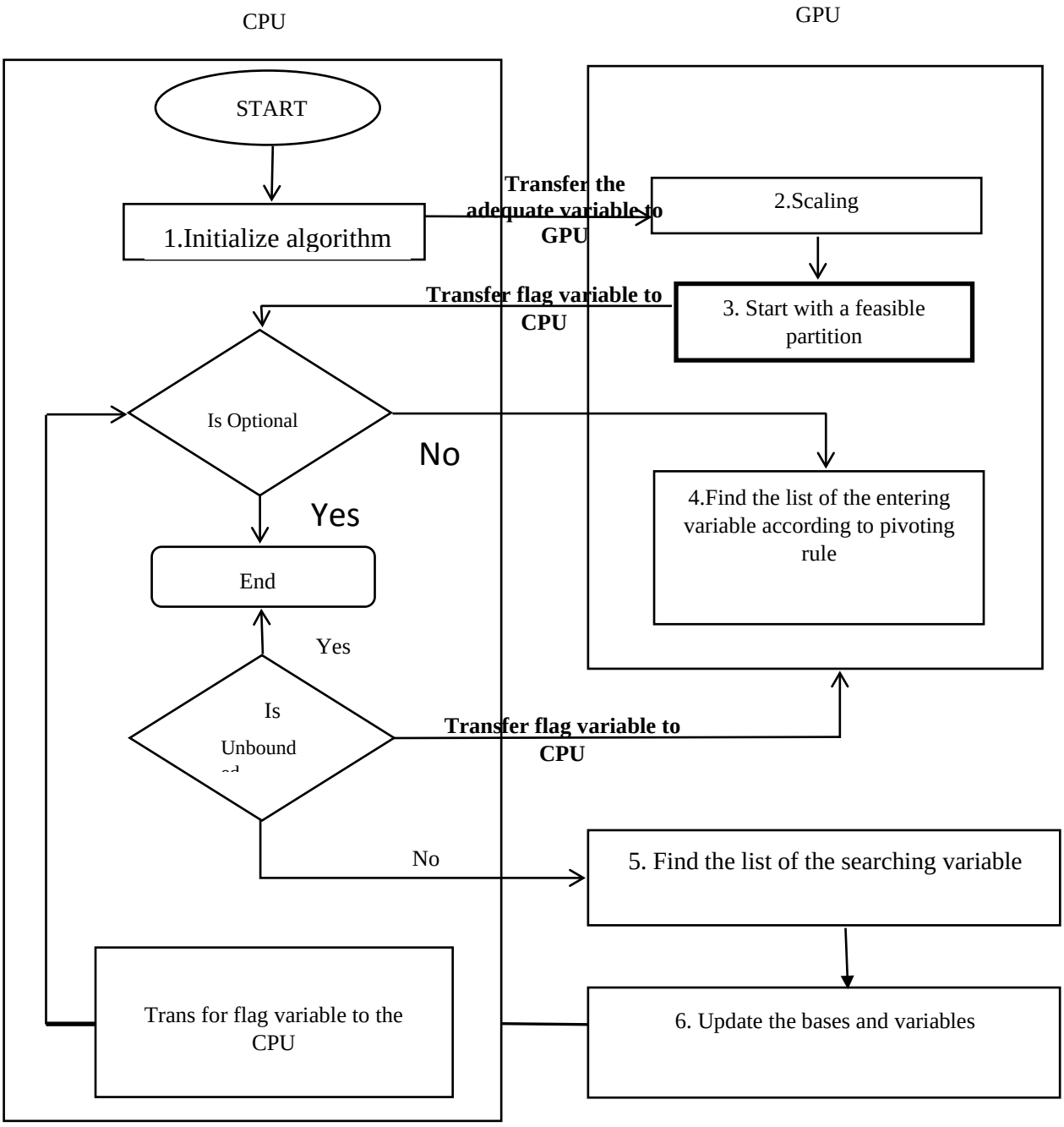

Fig. 2. Compressive sensing: (Matrix free interior point method)

3.7. Iterative Filtering

Iterated filtering algorithms are an instrument for most extreme probability deduction on halfway watched dynamical boundaries is utilized to investigate the boundary space. Applying successive Monte Carlo (the molecule channel) to these all-inclusive model outcomes in the choice of the boundary esteems that are more predictable with the information. Suitably built strategies, emphasizing with progressively lessened bothers, combine to the most extreme probability gauge. The boundary bothers help to defeat mathematical troubles that can emerge during successive Monte Carlo.

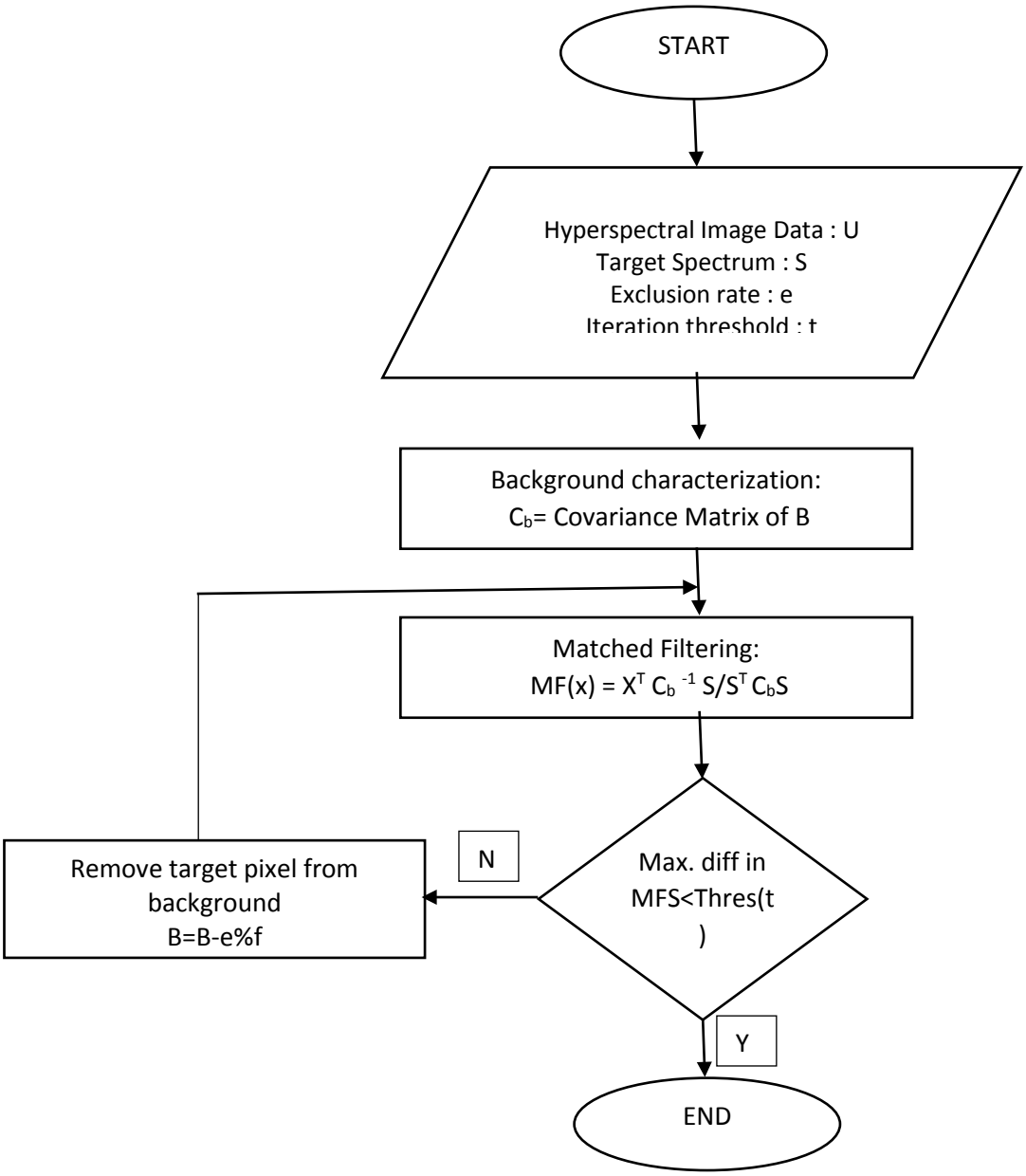

Fig. 3. Iterative matched filtering

3.8. Wireless Sensor Network formation

A wireless sensor network consists of fineless deployed, geographically dispersed sensors in a specific internal (external) environment (most of which are determined in advance). A Wireless Sensor Network plans to accumulate ecological information and the node gadgets arrangement might be known or unknown from the earlier.

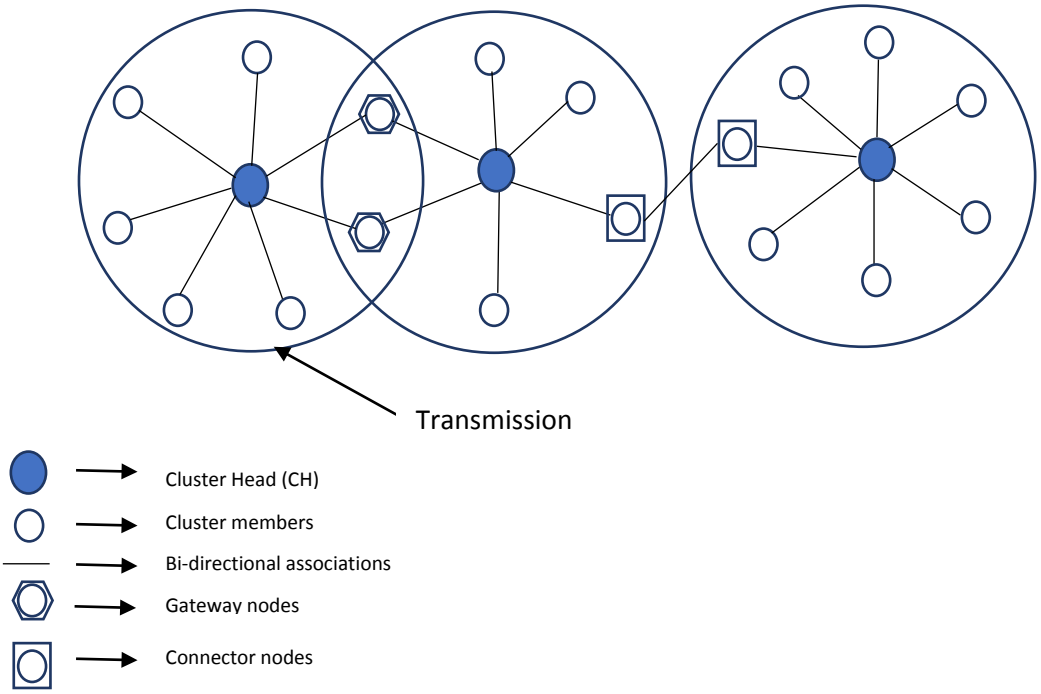

Fig. 4. Wireless Sensor Network Formation

3.8.1. Clustering

A wireless sensor network is an independent sensor distributed in a space, it is used to monitor physical (or) environmental conditions such as temperature, sound, pressure, etc. and work together to accelerate that data Through a wireless sensor network, individual sensors that fit into a space can protect physical (or) natural conditions such as temperature, sound, pressure, etc. A wireless sensor network consists of hundreds (or thousands) of nodes in a single node, with each node connected to a different sensor. Clustering is an important strategy for extending the life of wireless sensor networks.Here you can collect sensor nodes in one cluster and select the cluster head (CH) of all clusters. To collect information from a specific cluster node and transmit all the information to the base station, efficient energy clustering is an important improvement issue. This issue is widely recognized to extend the life of wireless sensor networks and has been decided by the cluster head. There are many types.

Fuzzy-rationale based cluster head political race.

i. Efficient rest obligation cycle for sensor nodes.
ii. Hierarchical clustering.
iii. Estimated energy harvesting.

3.8.2. CH identification

The CH could be sure that they are extraordinary nodes with heartier energy saves, however a more powerful methodology is to have the nodes themselves assume the part of Cluster Head, turning the function in the sensor bunch to some degree like passing a token. Clustering will likewise empower the sensor nodes to pre-cycle and pack their information stream, further decreasing energy. Framing the divisions of the nodes and allotting the cluster-head, requires exchange between the nodes and in this way adds overhead to the communication protocol.

(i) Sleep & Wake-up technique

The Wireless Sensor Network is worked of "nodes" from a couple to a few hundreds (or) even thousands, where every node is associated with one (or) now and again a few sensors. Each such sensor network nodes has ordinarily a few sections.

(ii) Server energy life time

The Wireless Sensor Network is built of “nodes” from a few to several hundreds (or) even thousands, where each node is connected to one (or) sometimes several sensors. Each such sensor network nodes has typically several parts.

1. A radio handset with an inward receiver (or) association with an outer reception apparatus.
2. A miniature regulator.
3. An electronic circuit for interfacing with the sensors and an energy source.

Generally a battery (or) an implanted type of energy collecting. A sensor node may fluctuate in size from that of a shoebox down to the size of a grain of residue, albeit working "motes" of certifiable minuscule measurements.

3.8.3. Monitoring Systems

Wireless Sensor Network a notable solution for observing natural status. With an assortment of sensors, Wireless Sensor Network can recognize changes in various boundaries which is used to deliver a geo-mechanical model of the incline including temperature, water stream, development speed and humidity[12]. The checking framework can assemble and deal with a lot of information from the earliest starting point of observing and oversee clones radiation, neighbouring nodes message conveyance and sending proportion dozing and wake-up framework and time battery reinforcement source and sink radiation, when clone has been identified. It improves the framework execution give a helpful and proficient strategy and furthermore satisfy useful necessities. **Fig. 5** describes the monitoring system’s architecture and it’s working flow.

(i) Trust and reputation system

Trust and reputation system are pointed toward taking care of the issues by empowering administration shoppers to solid evaluate the Quality of Service and the dependability of elements before they choose to utilize specific help or to collaborate with or rely upon a given element. In the same manner it speaks to a critical pattern in choice help for web

intervened administration position [18]. Reputation framework can likewise be called as cooperative endorsing frameworks to mirror their collaborative regular and are identified with community oriented separating framework. It is as of now utilized in business online applications.

(ii) Sniffer management

A sniffer is a program that screens and breaks down network traffic, recognizing bottleneck issues. Utilizing this data a network administrator can keep traffic streaming productively.

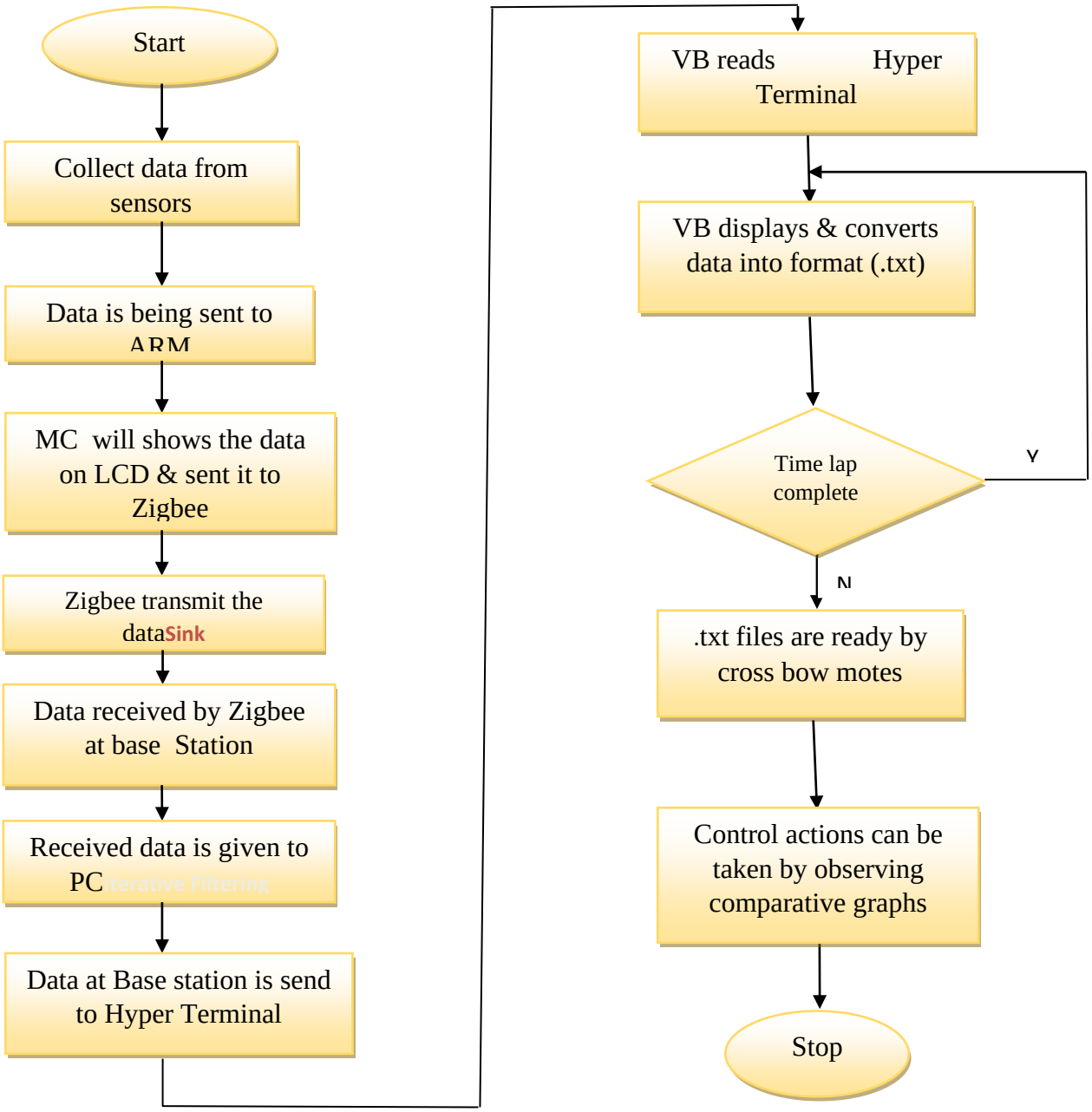

Fig. 5. Monitoring Systems

A sniffer can likewise be utilized truly or misguidedly to catch date being communicated on a network. A network switch peruses each packet of information passed to it, deciding if it is proposed for an objective inside the switch's own network or whether it ought to be passed further along the web. A switch with a sniffer, anyway might have the option to peruse the information in the packet just as the source and objective locations. Sniffers are regularly utilized on scholastic networks to forestall traffic bottlenecks brought about by record sharing applications. The utilization of packet sniffers is best in observing and investigating PC networks against weaknesses generally undermine information security and integrity.

(iii) Attack detection

The attack identification happens while recognizing an anomalous conduct of the network node (or) deviations from its typical activity[17]. The drawback of this methodology is that an off base carrying on node might be influenced by different variables that are not identified with the attacks, for example, programming, equipment (or) sensor disappointment[16].

As of now utilized standards of information transmission in wireless networks give the chance of making the four kinds of effects:

- ✓ Interception.
- ✓ Interruption.
- ✓ Modification.
- ✓ Fabrication.

Attacks on sensor network nodes conducted by

- ✓ Changing the firmware, drivers and programming of mechanical regulators (PLC-Programmable Logic Controller) and terminal sensor nodes. RFD (Reduced Function Device).
- ✓ Injection assaults by satirizing (or) substitution of the Wireless Sensor Network nodes, liable for gathering and handing-off information in the network. FFD (Fully Function Device) to catch or divert network traffic.

a) The results of intrusion detection in Wireless Sensor Network

There are three ways to detect attacks in network. They are:

1) Detection by the signatures.
2) Detection of the anomalous behaviour.
3) Combined detection by the specifications.

3.8.4. Sink

Sink node is utilized to gather information in wireless sensor network, information assortment may one jump, multi-bounce, all sensor gather information is ship off the base station called sink node. This might be diminishing correspondence traffic by utilizing versatile sink node information assortment. **Fig. 6** portrays the working of MSSM.

- ✓ Sparse network.
- ✓ CAG method (or) algorithm. { It is a query and response method}

There are two sink nodes available. It is also called dual sink. The dual sinks are:

- ✓ Static sink node.
- ✓ Mobile sink node.

Information mules gather information from sensor sent in sensing field and store at passageway.

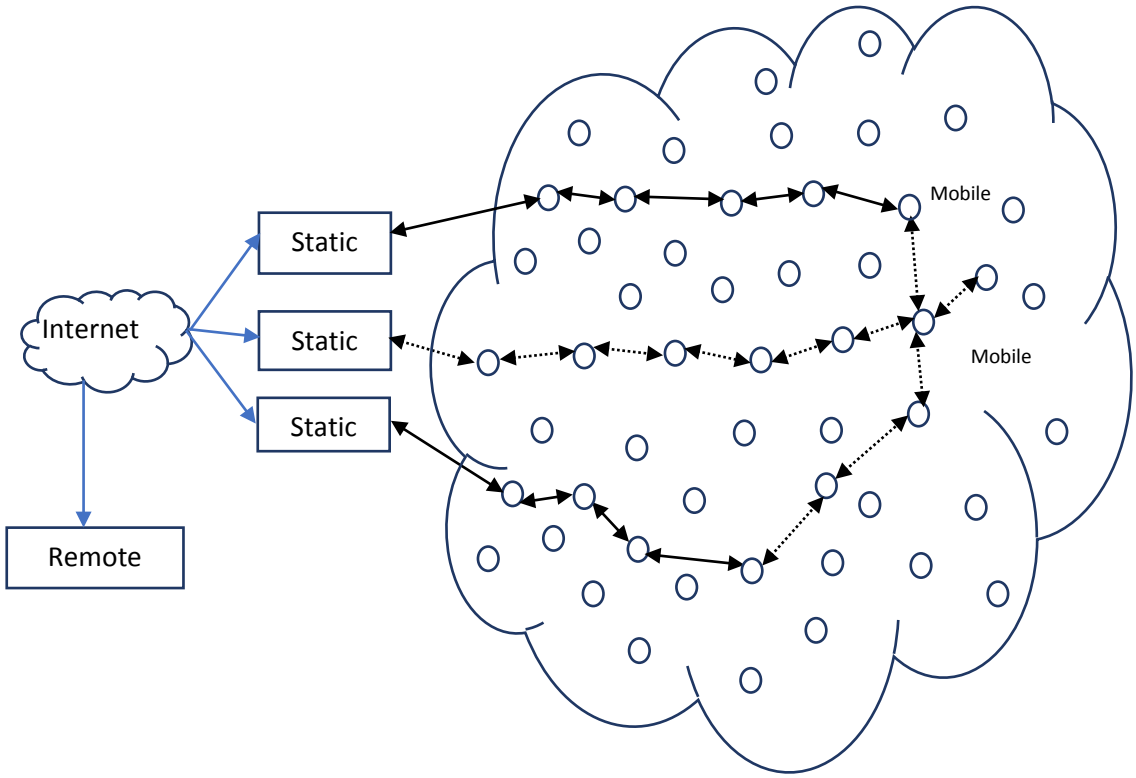

Fig. 6. Multiple Static Sink Model [MSSM]

3.8.5. Sensor nodes

Wireless sensor nodes are the focal components of a Wireless Sensor Network. Every node is responsible for acquiring data, preparing it, and conveying (or) sending it to it'sneighbors and it additionally stores and executes correspondence conventions and information handling calculations.

Energy storage for Wireless Sensor Network

Power to the Wireless Sensor Network is usually provided through primary batteries.

(i) Primary batteries

At the point when an essential battery is the single power source of a sensor node, the measure of at first put away energy decides the node's lifetime.

(ii) Secondary energy storage elements

Energy collecting from surrounding sources is a useful answer for reduce this issue. Since stable force can't be given through encompassing sources, battery-powered batteries going about as an auxiliary stockpiling components are used to store collected energy.

Sensor Communication model

Regular correspondence of Wireless Sensor Network comprises of clients, sinks and various sensor nodes. The clients are distant from Wireless Sensor Network and they assemble information from the sinks through heritage networks. There are two kinds of clients. They are:

1. Traditional remote users.
2. Mobile users.

Mobile clients move around the sensor field and they speak with the sinks just through the sensor networks so as to assemble information like area data of casualties in catastrophe zones.

3.8.6. Communication model design

Multiple static sink communication model is commenced with the following two problems. The problems can be described by the following manner.

Problem 1:

Reduction of network life time because of quick energy depletion of sensor nodes close to the sink.

Problem 2:

Long delay and low information conveyance proportion about inquiry and information dispersal because of long way from the static sink.

3.8.7. Clone attacker

An adversary can catch a sensor node and take out it's key materials [15]. When a node is caught, the assailant can reinvent it and produce a clone of a caught node. These clones or replicas can be conveyed in all network zones. These replica node attacks are extremely dangerous to the activity of sensor networks. With a solitary caught sensor node, the aggressor can make the same number of duplication nodes as he needs. The duplication nodes are illegal by the enemy, however have keying materials that permit them to seem like approved members in the network. So it is a lot of hard to recognize a clone attack.

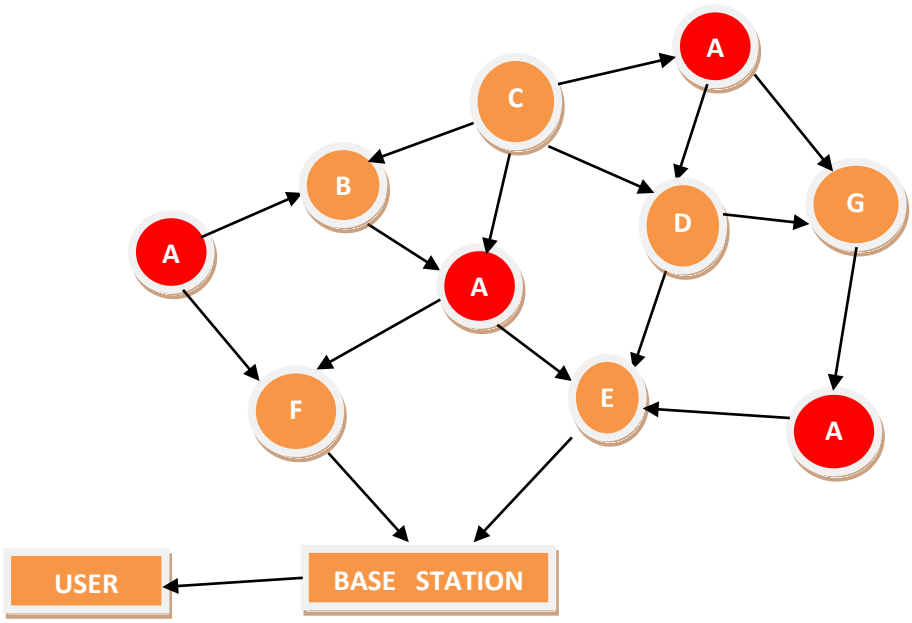

Fig. 7. Clone attacker

4. Implementation Of SBEA

This SBEA has been implemented using crossbow motes and the step by step procedure has been given here. The Crossbow processor/radio boards, all the more regularly known as motes, permit numerous sensors conveyed over a wide zone to wirelessly communicate their information back to a base station appended to a PC. The motes run the working framework TinyOS,[13] which handles power, radio transmission and networking straightforward to the client. The network shaped is adhoc, which means the motes sort out some way to frame the most productive network without anyone else. The network likewise underpins multihopping, permitting a bit out of scope of the base station to pass its data from bit to bit until the information arrives at the base station. With these errands set up, you can focus on building sensing applications.

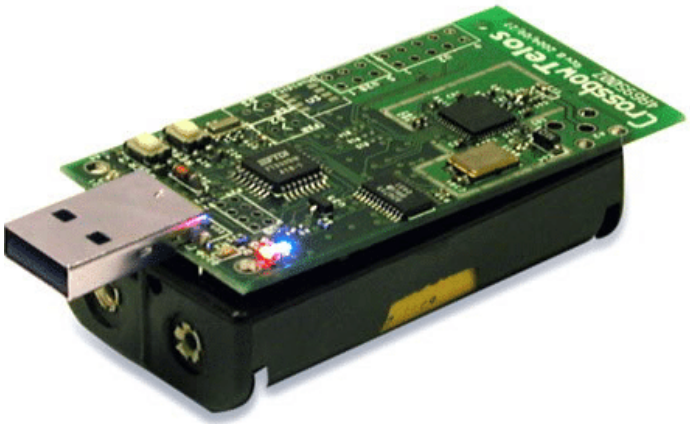

Fig. 8. Crossbow motes

Spot stage used for execution is Crossbow IRIS bit. IRIS pieces are little in size, lightweight, ZigBee pleasant and controlled with two AA betters. IRIS was gotten together with the MDA300CA sensor and data making sure about board which has a precision thermistor, a light sensor/photocell and general prototyping zone. MDA300CA is arranged as a general assessment stage for the MICAz and MICA2. They can be used for energy saving shows for a large portion of a month.

WSN application execution in crossbow pieces is done with the help of nesC programming language and TinyOS working System. [14] TinyOS is an open-source improvement condition that gives irrelevant structure sponsorship to make WSN applications. It is more like a library and allows fine grained resource the board. It gives possible code reuse. Undertakings are written in Network Embedded System C (nesC) language. It has two kinds of sections Modules-that decide and execute interfaces, Configurations (Wiring)-partner interfaces, used fragments to interfaces gave by others. Modules and Configurations license a structure organizer to fabricate applications.

Step 1: Data can be collected from the outside region by the sensors.
Step 2: Through crossbow motes it can be given for processing.
Step 3: The collected data have to be compressed through CS methodology.
Step 4: In WSN formation the collected data will be clustered on the basis of it's range and distance.
Step 5: For each cluster Cluster Head (CH) have been formed to monitor the nodes in it's clusters.
Step 6: Sleep and wake-up technique is implemented in the clusters. The nodes which are not collecting the data will be in the sleep mode through this step.
Step 7: Nodes will be wake-up by the neighbour node when it wants to sleep.
Step 8: Periodical change of CH. Goto step 5.
Step 9: Sniffers will be attached through iterative filtering.
Step 10: Attack detected through sink node implementation.
Step 11: Goto step 3.
(The above process is the processing steps for a single set of data. This process will be continued throughout the working time of the device)

5. Results And Discussions

By implementing the Snow Ball Endurance Algorithm using crossbow motes, we have analyzed the following advantages over other algorithms which we have compared earlier. The optimal route could be found in when life time of the battery has been enhanced in WSN using SBEA. Compared to other protocols the network life time has more extended and it is more advantageous than others. It lasts for a long time and the lifetime of the battery in WSN could be doubled. This is achieved by incorporating the sleep and wake-up technique in SBEA. The resources that are used in WSN could create more awareness by using this algorithm as like other protocols. This SBEA uses ABS technique for using the meta-data storage and retrieval of data. It has a best energy efficiency ant the size of the network consists of up to 600 nodes in the entire network.

While using this algorithm the sensor network would have limited scalable property. That is the inclusion of resources in the WSN while using this algorithm is limited to an extent. The time delay is very large and it could be classified based on clustering. It consists of cluster head which controls and co-ordinate the other nodes in the cluster. The cluster

head is responsible for data transmission and controlling activities. The cluster method followed here is hybrid and it has variable Base Station (BS) mobility. The number of clusters may vary according to the requirement of the work which it undertakes. Based on the participation of negotiation the choice of clusters would be rational based selection and has guaranteed number of groups. The data aggregation technique used in SBEA are centralized. That is the data could be recovered and posted in a centralized manner, so that any cluster head or cluster node in the WSN could be accessed. It has random nodes of deployment. It has high load balancing capability and the complexity is also high. **Table 1** shows the comparison of other routing protocols with our proposed SBEA.

Table 1. Comparison of LEACH, SPIN and PEGASIS routing protocols with SBEA

S. No	Criteria	LEACH	SPIN	PEGASIS	SBEA
1.	**Optimal route**	NO	NO	YES	YES
2.	**Network Lifespan**	Very good	Good	Extended life-time	More extended lifetime
3.	**Resource Awareness**	YES	YES	YES	YES
4.	**Use of Meta- Data**	Does not use any meta data	Uses resource adaptive negotiation algorithm	Data advertisement procedure is used	Uses ABS technique.
5.	**Energy efficiency**	GOOD	BETTER	BEST	BEST
6.	**Network size**	100m*100m	$40m*40m^2$	(0,0) to (100,100)	Up to 600 nodes
7.	**Scalability**	medium	Limited	Poor	Limited
8.	**Delay**	Very small	Small	Large	Very large
9.	**Classification**	Cluster based	Data-centric	Chain based	Cluster based
10.	**Data transmitter**	Cluster based	Each and every node participates in negotiation.	d Leader node	Leader node.
11.	**Clustering method**	Distributed	Not applicable	Hybrid	Hybrid.
12.	**Mobility**	Fixed BS	Each and every node acts as BS.	Fixed BS	Variable BS
13.	**Number of clusters**	Multiple	Not applicable.	Single	May vary.
14.	**Data aggregation**	5E-9j/bit	Tree based	NO	Centralized data aggregation technique.
15.	**Query based**	NO	NO	NO	NO
16.	**Choice of clusters**	Based on the probabilistic approach	Not applicable	Based on the distance from the base station	Rotational basis and based on the participation of negotiation.

17.	**Number of groups**	Not Guaranteed	Guaranteed	Guaranteed	Guaranteed
18.	**Deployment of nodes**	Random	Random	Random	Random
19.	**Load balancing**	Low	Medium	Medium	High
20.	**Complexity**	Low	Medium	High	High
21.	**Service**	NO	NO	NO	NO
22.	**Link detection**	NO	NO	Partially detected	Fully detected
23.	**Scheduling and detection**	Scheduled	Scheduled	Scheduled and detected	Scheduled and detected

6. Performance analysis of SBEA

In various dimensions the performance of the Snow Ball Endurance Algorithm has been analyzed. This has been done by implementing the SBEA in crossbow motes. When compared to the algorithms such as LEACH, PEGASIS and SPIN, SBEA has a well defined and better performance that other routing algorithms. **Table 1** shows the performance analysis of SBEA, by comparing with LEACH, PEGASIS and SPIN routing protocols. Here are some graphical analysis for the performance of SBEA.

Fig. 9 represents the performance analysis of SBEA for the parameters of resource awareness, energy efficiency and scalability. These performance has been analyzed and compared with the performance report of LEACH, SPIN and PEGASIS routing protocols. The performance has been analyzed based on three criteria. Time has been calculated with respect to number of nodes and number of resources. The graph shows that compared to other routing protocols SBEA servers more number of nodes and resource utilization is also in an efficient manner with respect to a particular time.

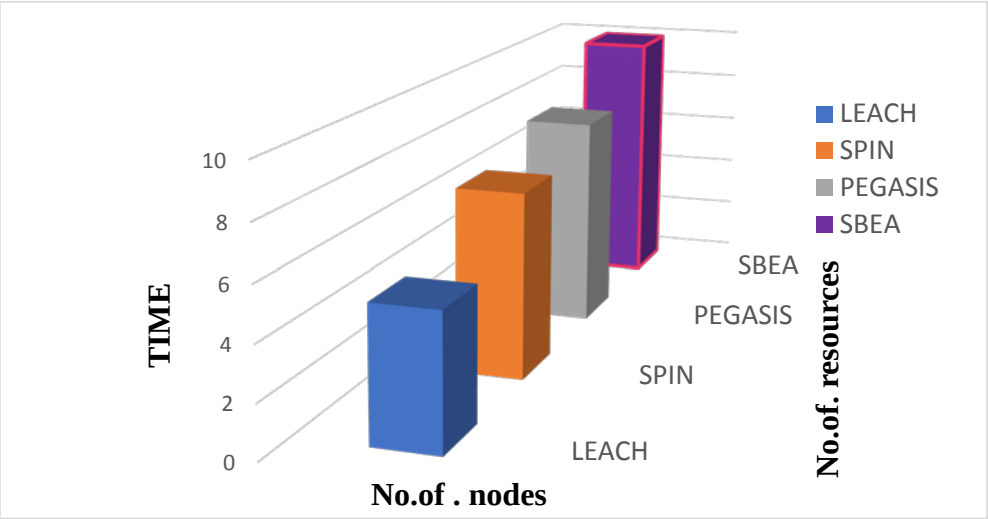

Fig. 9. Comparison of resource awareness, energy efficiency and scalability

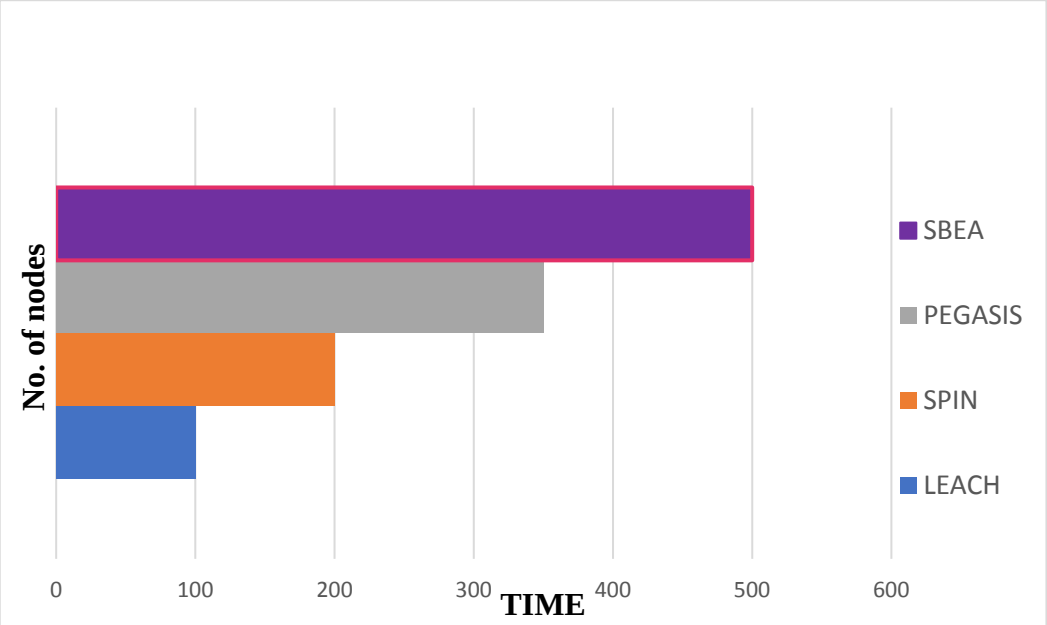

Fig. 10. Comparison of network lifetime, load balancing and mobility

Fig. 10 represents the performance analysis of SBEA for the parameters of network lifetime, load balancing and mobility. These performance has been analyzed and compared with the performance report of LEACH, SPIN and PEGASIS routing protocols. The performance has been analyzed based on two criteria. Time has been calculated with respect to number of nodes. The graph shows that compared to other routing protocols SBEA retains it's network lifetime with the nominal amount of nodes. The load balancing of SBEA is also retains with the high number of nodes with a stipulated time. The mobility of nodes in WSN has also give a very nominal amount of percentage and it is very network friendly to move the nodes in WSN.

Fig. 11 represents the performance analysis of SBEA for the parameter of battery back-up. The performance has been analyzed and compared with the performance report of LEACH, SPIN and PEGASIS routing protocols. The performance has been analyzed based on two criteria. Time has been calculated with respect to battery back-up. The graph shows that compared to other routing protocols SBEA retains it's battery back-up for a long time that other routing protocols. Hence the charging time and charging interval of the battery has been reduced. Also the lifetime of the device's battery is also extended in WSN. This has been clearly viewed in the **Fig. 11**.

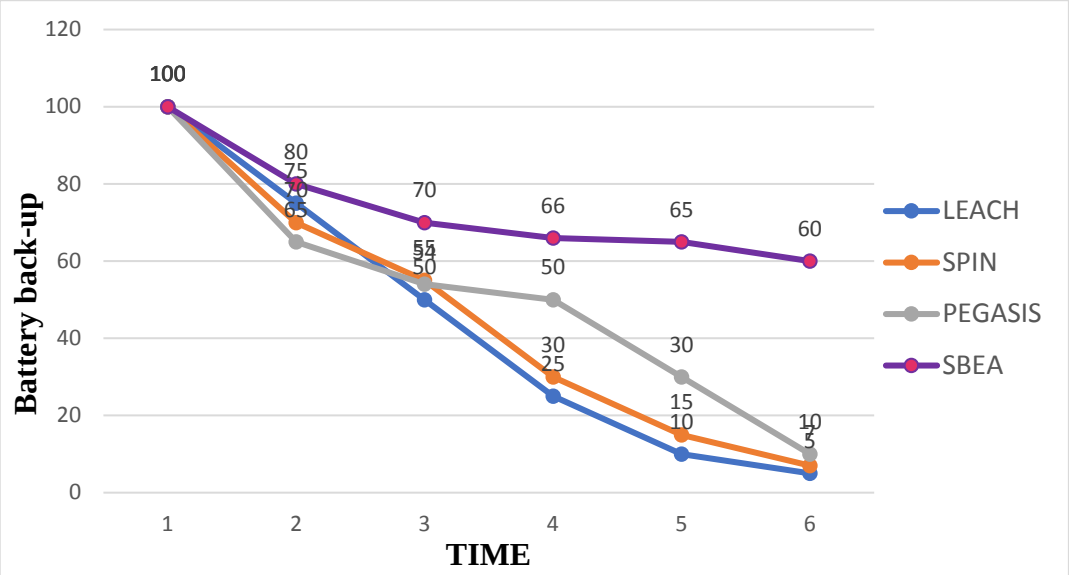

Fig. 11. Comparison of battery back-up in WSN nodes

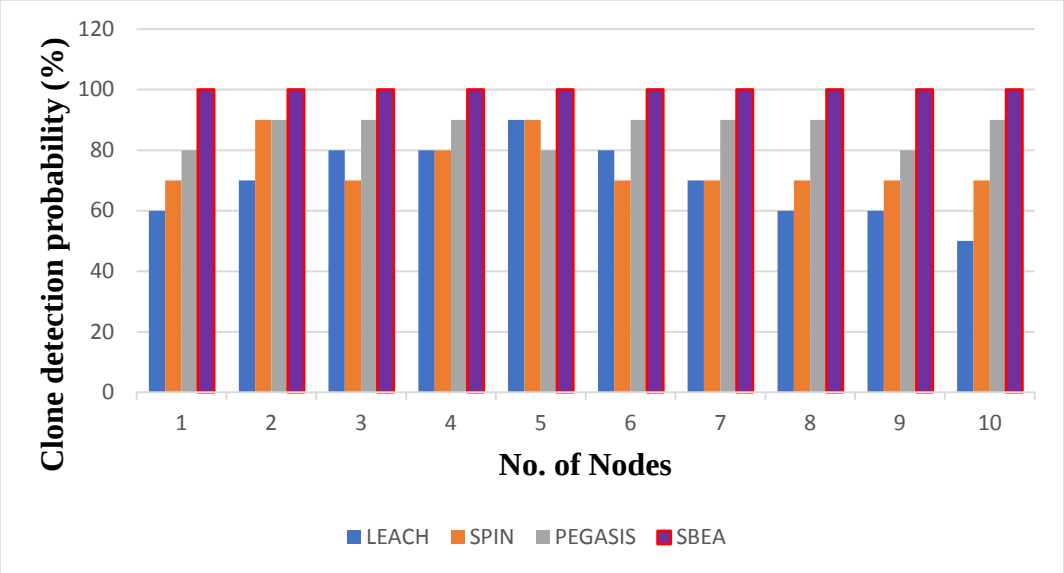

Fig. 12. Comparison of clone detection in WSN

Fig. 12 represents the performance analysis of SBEA for the parameter of clone detection. This has been shown here in percentage. The probability of the clone detection in SBEA is much more higher than the other routing protocols. The performance has been analyzed and compared with the performance report of LEACH, SPIN and PEGASIS routing protocols. The performance has been analyzed based on two criteria. Number of nodes has been calculated with respect to clone detection probability. The graph shows that compared to other routing protocols SBEA has high clone detection probability. This has assured that the SBEA could found any number of clones even with a bulk amount of clustering nodes in WSN.

7. Conclusion And Future Work

This paper has presented an effective novel based algorithm called SBEA. This algorithm tells the methodology for detecting the clone node in wireless sensor network for effective and novel data transmission. Along with that it also gives the way to improve the life time of the battery in sensors using sleep and wake-up technique. This has been implemented and tested using crossbow motes, where it supports many sensors in it. Further this algorithm can be tested for large devices such as escalators by improving it's performance and it had been left for future work.

References

[1] SuchitaR.WankhadeandNekitaA.Chavhan, "A Review On Data Collection Method With Sink Node In Wireless Sensor Network," *IJDPS*, Vol.4, No.1, pp. 67-74, January 2013. Article (CrossRef Link).

[2] J.Anthoniraj and T.AbdulRazak, "Clone Attack Detection Protocols In Wireless Sensor Networks: A Survey," *International Journal of Computer Applications (0975 – 8887)*, Vol. 98, No.5, pp. 43-49, July 2014. Article (CrossRef Link)

[3] Md. Mofijul Islam, Md. Ahasanuzzaman, Md. AbdurRazzaque, Mohammad Mehedi Hassan, AbdulhameedAlelaiwi and Yang Xiang, "Target Coverage Through Distributed Clustering In Directional Sensor Networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, p. 167, 2015. Article (CrossRef Link).

[4] Nikolaos Ploskas and Nikolaos Samaras, "Efficient Gpu-Based Implementations Of Simplex Type Algorithms," *Applied Mathematics and Computation*, Vol. 250, pp. 552-570, 1 January 2015. Article (CrossRef Link).

[5] V A Kamaev, A G Finogeev, A AFinogeev and D S Parygin, "Attacks And Intrusion Detection In Wireless Sensor Networks Of Industrial Scada Systems," in *Proc. of International Conference on Information Technologies in Business and Industry 2016*, *IOP Conf. Series: Journal of Physics: Conf. Series*, vol. 803, p. 012063, 2017. Article (CrossRef Link).

[6] Euisin Lee, Soochang Park, Fucai Yu, and Sang-Ha Kim, "Communication Model And Protocol Based On Multiple Static Sinks For Supporting Mobile Users In Wireless Sensor Networks," *IEEE Transactions on Consumer Electronics*, Vol. 56, No. 3, pp. 1652-1660, August 2010. Article (CrossRef Link)

[7] KimonFountoulakis, Jacek Gondzio and Pavel Zhlobich, "Matrix-Free Interior Point Method For Compressed Sensing Problems," *arXiv:1208.5435v3[math.OC]*, 16 Nov 2013.

[8] Sachin Lalar, Shashi Bhushan and Surender, "Analysis Of Clone Detection Approaches In Static Wireless Sensor Networks," *Oriental Journal of Computer Science and Technology*, Vol. 10, No. 3, pp. 653-659, 2017. Article (CrossRef Link)

[9] Dong-Yu Cao, Kai Yu, Shu-GuoZhuo, Yu-Hen Hu, Fellow, and Zhi Wang, "On The Implementation Of Compressive Sensing On Wireless Sensor Network," in *Proc. of 2016 IEEE First International Conference on Internet-of-Things Design and Implementation*, 2016. Article (CrossRef Link).

[10] By JyotiSaraswat, Neha Rathiand ParthaPratim Bhattacharya, "Techniques To Enhance Lifetime Of Wireless Sensor Networks: A Survey," *Global Journal of Computer Science and Technology Network, Web & Security*, Vol. 12, No. 14, 2012. Article (CrossRef Link)

[11] NayanaHegde and SunilkumarS.Manvi, "Implementation Of Security Mechanism In Wireless Sensor Network Using Crossbow Motes," in *Proc. of 2014 International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, IEEE, 2014. Article (CrossRef Link)

[12] KriangsiriMalasri and Lan Wang, "Design And Implementation Of A Secure Wireless Mote-Based Medical Sensor Network," *Sensors*, vol. 9, pp. 6273-6297, 2009. Article (CrossRef Link).

[13] Miriam Carlos-Mancilla, Ernesto Lopez-Mellado and Mario Siller, "Wireless Sensor Networks Formation: Approaches And Techniques," *Hindawi Publishing Corporation Journal of Sensors*, Vol. 2016, 18 pages, 2016, Article ID 2081902. Article (CrossRef Link).
[14] Joel Trubilowicz, KanCai and Markus Weiler, "Viability Of Motes For Hydrological Measurement," *water resources research*, vol. 45, 2009. Article (CrossRef Link).
[15] G. Tuna and V.C. Gungor, "Energy Harvesting And Battery Technologies For Powering Wireless Sensor Networks," *Industrial Wireless Sensor Networks*, pp. 25-38, 2016. Article (CrossRef Link).
[16] HaafizahRameezaShaukat, FazirulhisyamHashim, Muhammad ArslanShaukat and Kamal Ali Alezabi, "Hybrid Multi-Level Detection And Mitigation Of Clone Attacks In Mobile Wireless Sensor Network (MWSN)," *Sensors*, vol. 20, p. 2283, 2020. Article (CrossRef Link).
[17] M.Bhavana and B.Vijay Kumar, "Data Efficient And Clone Detection In Wsn Using Ercd Convention," *International Journal for Modern Trends in Science and Technology*, Vol. 03, No. 06, June 2017. Article (CrossRef Link).
[18] Osamah Ibrahim Khalaf, GhaidaMuttasharAbdulsahib and MuayedSadik, "A Modified Algorithm For Improving Lifetime In Wsn," *Journal of Engineering and Applied Sciences*, Vol. 13, No. 21, pp. 9277-9282, 2018. Article (CrossRef Link).
[19] Leonardo M. Rodrigues, Carlos Montez, Gerson Budke, Francisco Vasques and Paulo Portugal, "Estimating The Lifetime Of Wireless Sensor Network Nodes Through The Use Of Embedded Analytical Battery Models," *Journal of Sensors and Actuators, J. Sens. Actuator Netw.*, vol. 6, p. 8, 2017. Article (CrossRef Link).
[20] RamadhaniSinde, Feroza Begum, KaroliNjau and ShubiKaijage, "Refining Network Lifetime Of Wireless Sensor Network Using Energy-Efficient Clustering And Drl-Based Sleep Scheduling," *Journal of Sensors*, vol. 20, 2020. Article (CrossRef Link).

V.Sathya is currently an Assistant Professor of Computer Science and Engineering at S.A Engineering College (Autonomous), Affiliated to Anna University. She has completed his Masters in Computer Science and Engineering at PRIST University. Her main research interests are Wireless Sensor Networks, Network Security, Sandboxing Technology, Block chain Technology, Wireless Communication. She has published more than 20 papers in IEEE digital xplore, SCOPUS, SCI journals, Springer and Elsiever publications. Also she has presented around 50 papers in international and national conferences and published in the proceedings. She is a reviewer in IET journal and IJCRT journal.

Dr. S.Kannan is working as Professor in the Department of Computer Science and Engineering at E.G.S Pillai Engineering College (Autonomous), Affiliated to Anna University. He received his PhD degree at Anna University. His research interests are in the areas of wireless sensor networks, soft computing and data mining. He has published more than 50 research articles in reputed international journals in engineering sciences.