Soft Computing (2019) 23:10623–10634
https://doi.org/10.1007/s00500-019-03962-z

FOUNDATIONS

Enhanced analysis of border surveillance using intruders' crossing strategies

N. Bhalaji[1] · S. Venkatesh[2]

Published online: 5 April 2019

Abstract
External border surveillance has become one of the most trending topics of research today. The problem of automating the detection in a big and Hercules terrains using WSN is one way to do. In first half of the paper, we have focussed on the chess queen-crossing strategy adopted by the intruder in order to cross the international border. In the other half, we have used milky-way deployment strategy of sensors to automate the process of detection to a particular zone and then forwarding that detected information to the nearest base station using homogeneous zone routing protocol. The relationship between the sensor detection and energy balancing is that in our work, the focus is on shifting the load of the task of the sensor node equally thereby reducing the burden of the nodes the energy spent in sensing, detecting and communication of the information regarding the movement of the direction of the intruder to a certain region and the base station deployed in that region is responsible for alerting the border action team to crack down on the unauthorized intruders especially during the night. To achieve this objective, we have classified the monitoring zone called border region into three zones and allocating three base stations for each zones. The simulations of work show that HZR protocol performs better in terms of network lifetime for this application.

Keywords Intruder · Chess queen-crossing strategy · Milky-way deployment · Base station

1 Introduction

A wireless sensor network consists of a set of sensor nodes which collaborate among themselves wirelessly all the information happening around its region of monitoring. They have the ability to sense, detect and collect any abnormal event happening in any region of interest. Due to their distributed operation ability and scalable coverage ranges, WSN are quite adaptable to be used for sensing activities over large areas (Akyilidz and Stuntebeck 2006). In some of the applications, the main goal is to monitor a set of target nodes called target coverage. In such regions, the objective is to cover a network area fully or partially (He et al. 2011). Coverage problems deal with finding the best optimal locations for the deployment of sensors so as to increase the coverage area in the field of interest (Guerriero et al. 2011). Work done in Alkhathami et al. (2015) focussed on mesh and cluster deployment of sensor nodes along the US–Mexico border using Opnet Modeller 17.5, where it was proved that mesh topology is better than the cluster topology to interact seamlessly over large areas. However, in some of the cases, some authors have favoured stochastic deployment of sensors in case when the field of interest to be monitored is hostile and inimical (Jin et al. 2009; Hung and Lui 2010; Lin and Chen 2008; Lazos and Poovendran 2006). While there are many researches in the field of border surveillance, the success of such missions is largely dependent on the optimality of the deployment patterns, i.e. many of the works done in this area covering the points in a plane are done using minimum number of geometric bodies (Kershner 1939; Hochbaum and Mass 1985; Melissen and Schuur 1996; Nurmela and Ostergard 2006), but they have focussed on only coverage not connectivity. An effective border surveillance that has to be designed must have a proper deployment strategy such that to cover the border with an optimal number of

Communicated by A. Di Nola.

✉ N. Bhalaji
bhalajin@ssn.edu.in

[1] SSN College of Engineering, Chennai, Tamil Nadu, India

[2] SRM Valliammai Engineering College, Chennai, Tamil Nadu, India

sensors using which it can have the ability to determine the path or crossing strategy adopted by the intruders, routing the monitored information swiftly to the nearby base station so as to enable the Border Action Team deployed there to track down the intruders who may be terrorists and smugglers, especially during night. The scenario which is the climax of this application is how the detected information reaches the base station. How we are balancing every sector of the region inside and in between the regions such that there is a uniform distribution of load on the network traffic and how detection rate is increased using this deployment strategy are the main focus of our work.

Our proposed work in this field uses a deployment strategy called a milky-way deployment where the sensors are arranged in a spiral fashion covering a region under surveillance. In this scenario, we shall deploy three sink nodes in each of the categorized zone at different layers such that no two sink nodes must directly establish the communication between themselves, but they can collaborate indirectly with the intermediate nodes. To enhance the lifetime of the network, we are deploying three base stations on the either ends away from the area of deployment. The motive behind using this concept is distribution of load transmission equally along various directions instead of putting pressure on one particular region and one sink node as generally done in several applications scenario. So, we have categorized them as Zone A, Zone B and Zone C. The idea behind using this strategy was to give a better profile of the path so that early detection of the intruder can take place and his path alongwith his direction can be depicted appropriately. Hence, we have designed our problem as follows: Given a set of sensor nodes deployed heterogeneously, how to schedule the mode of detection by dividing the load of detection into different sectors/zones equally so as to maximize the lifetime of the network nodes that is involved in the scenario. So, the main focus of our work is to maximize the lifetime of the network by distributing the sensed information equally in different directions and to the respective zonal base stations.

2 Related works

In the literature, there are many works done by the researchers across the globe in this direction. Ghosha and Das (2008) in their work have chosen to place the sink on coordinates that are outcome of a uniform random distribution, which is similar to their choice of their sensor coordinate distribution. Researchers in Alkhathami (2015) have focussed on using a greedy algorithm approach so that energy consumption takes place across all the sensor nodes in all the directions. Researchers from the USA (Subir et al. 2009) explain how to track the movement of the intruders and thereby calculate the amount of power consumption done by the sensors for performing this work. A detailed study of the challenges of the linear topology and identification of an appropriate metric to measure the quality of border cross-detection using the topology was carried out by experts (Mostafaei 2018). Work done in this area have used several models like uniform distribution and Gaussian distribution of sensors to measure the probability of detection of the effect of the deployment deviation of the number of sensors, and some critical parameters including intrusion detection are studied (Wang et al. 2008). Further, in addition to the previous work, a work was carried out using two models, namely homogeneous and heterogeneous, by deploying 500 sensors across 1000*1000 square metres (Wang et al. 2013). A novelty concept was introduced in this field using a technique called three-dimensional mechanism in the form of 3D intruders, 3D sensors, 3D environments using OPNET 14.5 and NS-2 Simulators (Said and Elnashar 2015). Researchers in Tiegang et al. (2014) focussed their work on major factors pertaining to the energy model, cost model, aggregation model and lifetime of WSN. They used a structure called regular hexagon-based structure and used a uniform load routing to split the load of the network into different directions. In many of the literature works done, a common research problem observed in every paper included the problem of sink hole routing, where the nodes nearer to the sink node bear the burnt of excessive load due to handling of the data for communication where excessive dissipation of energy takes place; as a result, the data sent from the source cannot reach the base station. To fix this problem, they had established a relationship between node deployment and the quality of the network service such that connectivity of communication is maintained in a network. A further study in this direction was focussed on a routing protocol called RELBAS for determining the safest path of transmitting the data to the destination (Chakraborty et al. 2015). One such recent work in this direction used multiple base stations by keeping them in a mobile state using the concept of mixed integer programming framework to enhance the lifetime of WSN (Cayirpunar et al. 2017). A very recent work on this area was done by taking into consideration about the barrier coverage, and the authors proved by means of simulations about reducing the network lifetime of WSN by using the concept of learning automata theory where the sensor nodes shall know about the energies of their corresponding nodes that are involved in the surveillance scenario and then if there is any kind of a breach in the barrier to detect the trespasser (Mostafaei and Meybodi 2013). In many of the research works that were done in this area, it was primarily focussed on deployment, routing protocols and other factors pertaining to the barrier

coverage as well as connectivity scenario, but the work done by Cheng and Wang (2018) focussed the scenario of how to conserve the energy of the sensor nodes, while the intrusion is taking place by the intruders' favourite paths. In Bellazreg and Boudriga (2013), Ramzi et al. focussed on the architectural issues required to ensure good detection as well as better tracking of the targets by using the proper deployment as well as the use of the routing protocols.

3 System model and problem formulation

In this section, we present the milky-way region that is under surveillance. Our main aim is to show how the technique of inside-loop region load balancing and consecutive-loop region load balancing along with the use of more than one base station helps in maximizing the network lifetime of the wireless sensor network.

3.1 Network model

In this region, we present the milky-way-shaped deployment strategy that is under surveillance. Our main objective is to show how our deployment strategy minimizes the load on the network and maximizes its lifetime. The area to be monitored is placed in consecutive milky-way model by making the following assumptions:-

(i) Assume that N_T be the total number of sensors that are deployed in spiral fashion of radius R. In this scenario, we are assuming a two-dimensional environment for using the surveillance applications.

(ii) Assume L_1, L_2, L_3,…, L_N be the different regions as shown in spiral deployment of sensors in Fig. 1, where r <=Optimum ($\text{limit}_{\text{comm}}$)

(iii) In our case, we have assumed the sensor nodes as well as the three base stations as the stationary nodes. Every node must make some adjustment during the transmission of the detected information.

(iv) In our model, sink nodes are placed at the different zones of the milky-way model.

(v) We are taking an assumption that if the intruders I_1, I_2, I_3 enter into the mouth of the milky-way deployment, then it should be evident that his entry should be intimated to the nearby sensors, but in this process, a point that must keep in mind is the proper utilization of the sensor nodes, and there must not be any kind of imbalance in utilization of energy as this would drastically affect the performance of the sensor nodes.

(vi) Milky-way deployment helps in finding the trajectory of the path followed by the intruder.

(vii) The network lifetime is calculated depending upon number of data packets received by the sink node from every node.

(viii) We have assumed that the sensing range of all the sensors is the same.

(ix) The transmission range of every node is the same.

(x) The Distance between all the nodes is the same.

3.2 Analysis of intruders' border-crossing strategy

Suppose we are taking into consideration the path adopted by the intruders say the chess queen strategy in this case. In this scenario, we are taking into consideration the path adopted by the three intruders when they are crossing the path using two diagonal paths and one straight path. In our work, we are taking into consideration the three scenarios of the intrusion:

3.2.1 Scenario 1: when the intruder follows the path $\beta 1$ going in the left side of the border

In this scenario, the intruder if suppose follows the diagonal path on the left side of the border, then the detected scenario must be intimated to the nearest base station, viz. base station 1 as shown in Fig. 1. In this situation, we deploy a sink node in every zone and the regions in the milky-way deployment. These sink nodes transmit the intruder detected information to the nearer base station, i.e. base station 1 responsible for handling Zone A load.

3.2.2 Scenario 2: when the intruder follows the path $\beta 2$ going in the intermediate region of the border

In this scenario, the intruder follows a straighter path that shall be handled by the base station 3 as shown in Fig. 1. In this situation, the sink nodes responsible for the intrusion detection shall transmit the information to the base station 3 present in zone C (Fig. 2).

3.2.3 Scenario 3: when the intruder follows the path $\beta 3$ going in the left side of the border

In this scenario, the intruder follows the path $\beta 3$; this intrusion detection in this zone is handled by the base station 2 present in the zone B.

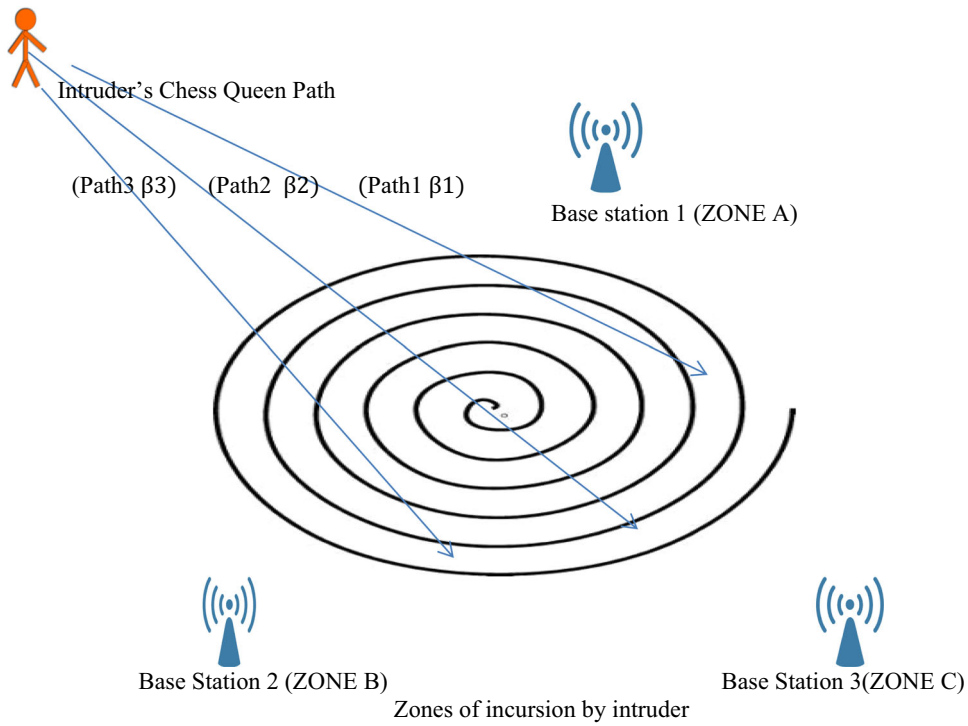

Fig. 1 Border management using milky-way deployment

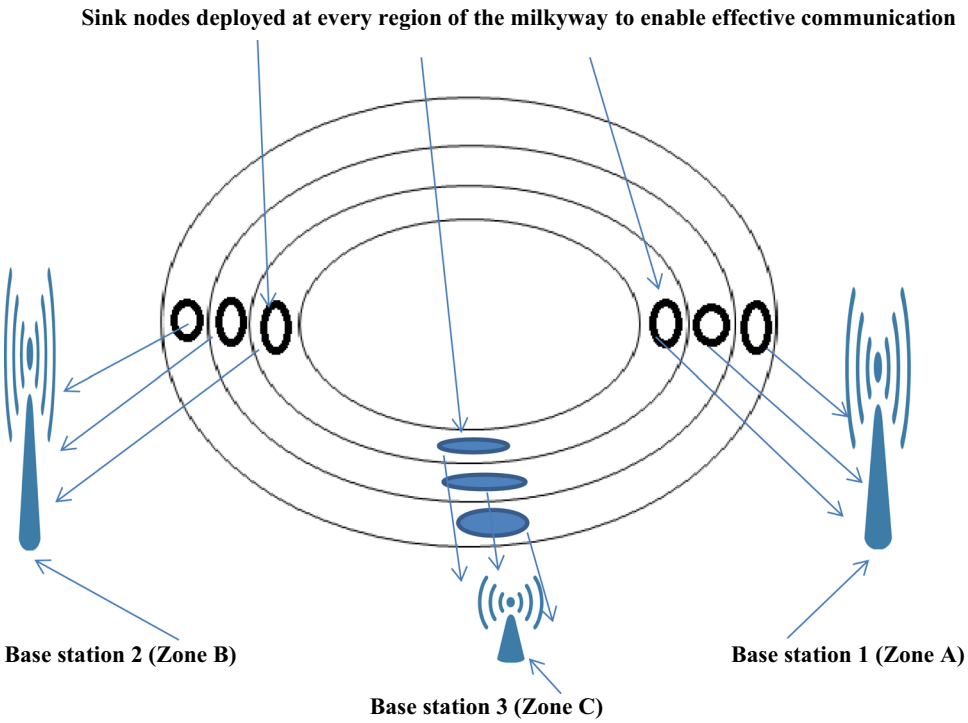

Fig. 2 Deployment of sink nodes scenario to enable communication to the base station

- The biggest advantage of our proposed technique is that the intruder information is quickly transferred to the nearest base station in that particular zone and the routed information need not traverse a longer path to reach the base station. This in turn saves the energy consumption of other nodes, and all the nodes need not be involved in the intrusion detection scenario and that too the monitoring of the intruder path could be monitored form his arrival to the direction he is in.
- In the first step, when the intruder enters inside the monitored region which is sandwiched between the two borders, a set of sensors nearby gets activated after it

sensed an intrusion activity. In the second step, in our case, we have defined the intruders' movement through the chess queen strategy; then, here, in this case, using this scheme activates the nearby sensors, predict his direction and reports it to the base station which is controlling that region. In the last step, calculation is done of how much of power dissipation is done and how effective is the routing mechanism in this scheme.

- During this process, the nodes that are deployed in the place where the intrusion takes place gets activated, and as we have assumed the diagonal path followed by the intruder, so the tracking of the intruder takes place diagonally by the sensor nodes deployed in that direction, and the information is routed to the nearest base station. The type of routing protocol we are using here is the homogeneous zone routing (HZR) as it involves delivering the detected activity to the nearest base station. Suppose N be the total number of sensors that have detected the activity; hence, they shall follow a diagonal line along with the intruder, while the remaining shall be in an inactive state. The main points here are to determine the number of hops taken by the node and what is duration of the connectivity between the nodes that exist.
- We have used hundred sensor nodes for deployment but have used three random nodes as a means of representation of how the communication takes for simplicity purpose. In fact, the sensors we have deployed are on the spiral fashion, and as a means of representation, we have randomly taken three nodes to highlight three nodes in each spiral represents a sensing node, interlocutor node, succession node, i.e. first, second and third nodes respectively. The role of the third node is that it acts as a succession node which takes up the responsibility of collecting the information and passing it to the nearby base station.
- The interlocutor node acts as a node which takes up the responsibility of transmitting the sensed and detected information to the node which is nearest to the base station and check if the successor node(s) has minimum threshold energy to send the information swiftly to the nearest base station so that the border action team can trap lay a trap on the intruders entering illegally.
- We have selected the spiral pattern of node deployment which we have given a name called milky-way deployment by using the homogeneous routing protocol as it is very useful when the area of monitoring in the border area is large and there. In this model, there are many possible alternatives to route the intruder detected information to the nearest base station instead of traversing a long path in case there is a single base station.

4 Scenario of power consumption taking place during intrusion into the monitored region (inside the monitored sensor region)

- In this scenario, during the crossing path of the intruder, the nodes involved in the detection are categorized in the form of different zones such that it must be in equal size as big zones/small zones disturb the equilibrium of the energy distribution. The node having high residual energy among other nodes is selected as a sink node that is responsible for transmitting the information to the nearest zone base station. Once sensor node sends the detected information, it must select the shortest path to reach the nearest zone base station.
- Then, the sensor nodes having higher residual energy are selected and scheduled according to the movement of the intruder.
- High residual energy of nodes is selected if the threshold energy value is above the minimum energy value of the network nodes.
- The first step is achieved by assuming that a set of sensors is configured at the predicted entry points of the border. As soon as the target crosses the entry point, a sensor, after sensing, detects it. But its detection efficiency is determined iff $(\mathrm{Sens}_{\mathrm{Rad}}) = \mathrm{Th}_{\mathrm{intruder}}$, where $\mathrm{Th}_{\mathrm{intruder}}$is the threshold distance at which the sensing radius of the sensor limit detects the intruder.
- The second step is used to determine the path and direction which the intruder is adopting so that the border action team in the base station can get appropriate time to nab the unauthorized intruder. Suppose at time T_0, let the position of the intruder be $P\ (i, j)$, then at time T_n, the position changes to $P\ (i + 1, j + 1)$ with respect to the direction as the prediction in this case requires both the magnitude and the direction. In this step is where we want to determine the routing mechanism to be followed by the sensors to pass the detected signal to the base station.
- In the third step, we have to analyse the amount of power consumption that had taken place in this process by the sensors and how effective is the routing mechanism using analytical and simulation results to determine the performance factor of the WSN in this scenario. This is the main objective of this paper.
- Suppose E_{Sink} be the total energy that has been dissipated at the sink node. The sink node is a node which is responsible for collecting all the information from the nearby sub nodes before delivering it to the base station. Suppose intruder 1 is intruding the monitored area, then let us assume he is intruding at the left diagonal side of the border end. Here, we are

considering a situation where only a single base station is being used. Now, after the intrusion, suppose the intrusions are detected by the sensors S_1, S_2, S_3, S_4 and S_5. Then, the sink node here is responsible for aggregating the information from these nearby sensors

- Total power dissipation for intruder 1 at any time t is given by,

$$P_{\text{sink}}(I_1(t)) = \{t_1S_1 + t_2S_2 + t_3S_3 + t_4S_4 + t_5S_5\} : t > 0 \quad (1)$$

where t_1s_1 = time taken by sensor 1 to detect the intrusion activity, t_2s_2 = time taken by sensor 2 to detect the intrusion activity, t_3s_3 = time taken by sensor 3 to detect the intrusion activity, t_4s_4 = time taken by sensor 4 to detect the intrusion activity and t_5s_5 = time taken by sensor 5 to detect the intrusion activity

- Now, let us suppose we take into consideration intruder 2, intruder 3.
- Hence, the total power consumption in case more than one intruder is involved in this scenario.

$$P_{\text{sink}}(I_n(t)) = \{t_n\};\ \min t > 0 \quad (2)$$

- Here, handling a single intruder may not add any pressure on the sink node. But the presence of more than one intruder may put an additional burden on the sink node. In other words, then it may reduce the lifetime of the sink sensor node because it is the one responsible for collecting the detected information and sending it to the nearby base station. So, it is this problem that we have focussed our research problem in this direction. In the diagram given below, we are highlighting the amount of work load allocated to the sink node in the presence of three base stations.
- We focus our work on assigning the higher residual energy of the nodes in an efficient manner.

$$P = 1 - e^{\alpha(E(\text{initial})/E(\text{energy dissipated}))};\ e \geq \text{Th}(\alpha) \quad (3)$$

5 Energy consumption model when the intruder takes side paths (β1andβ3paths)

Here, all the nodes must know about their energy levels and there must not be any type of connectivity issues among the nodes when they are being getting involved in the intrusion activity.

We here assume that pt_1, pt_2, pt_3,…, pt_n be the crossing strategies adopted by the intruders. When the intruder enters the spiral region L_1, then the sensing node tries to detect the intrusion activity and sends the information to the other node which in turn receives the information in a multi-hop fashion which is given by:

$$E_C = E_{C-\text{TX}} + E_{C-\text{RX}} \quad (4)$$

During the intrusion, if an intruder (say I_1) enters L_1, then suppose a node detects the intrusion, then it shall automatically form a group of clusters and sends the information to the cluster head which in turn sends that information to the nearby zone base station. The amount of energy dissipated by the sensor node during transmission is given by:

$$E_C - T_X = ID_0y^ka^y \quad (5)$$

On receiving a transmitted information, there shall be some amount of power dissipation that will be taking place in this scenario:

$$E_{C-\text{RX}} = ID_r \quad (6)$$

Hence, total energy dissipation that takes place during this scenario is given by:

$$E_C = ID_0y^ka^y + ID_r \quad (7)$$

Suppose T_N be the lifetime of the milky-way deployment. In this scenario, there are two ways in which the sensed information can be transmitted to the nearest base station. It is done in the following ways:

(i) Single hop
(ii) Multi-hop

These two factors play a very crucial role in determining the lifetime of the network. A node N_1 during transmission of detected intrusion takes hop-by-hop transmission to reach the base station. During this, there shall be another node which shall be in the process of reception.

$$E_{C-\text{TX}} = d_nE_{a\text{TX}-\text{dirTX}} + h_nE_{a\text{TX}-\text{HT}} \quad (8)$$

where $h_n = I_n + \text{Su}_n$

I_n = interlocutor node, Su_n = succession node

$$E_{C-\text{TX}} = d_nE_{a\text{TX}-\text{dirTX}} + I_nE_{a\text{TX}-\text{HT}} + \text{SU}_nh_nE_{a\text{TX}-\text{HT}} \quad (9)$$

The objective of Eq. (6) is to minimize the total energy consumption in the network. Our work is to balance the energy consumption in every region of the milky-way network before it reaches the base station. For this, the focus is on the following points:-

(i) To maintain an equilibrium in terms of the energy consumption between the nodes in each sub-region of the deployment.
(ii) To maintain the equilibrium of energy consumption of the regions in the milky-way deployment which are adjacent to each other.

(iii) To set the maximum limit threshold value of inter regions node communication.
(iv) Maintain network connectivity for the maximum time.

6 Energy consumption model in the intermediate region (β2path)

In this section, we shall discuss about the proposed solution and check how it works.

6.1 Within-region load handling in milky-way deployment

Let $C_P = \{pt_1, pt_2, pt_3, \ldots, pt_n\}$be the set of all the crossing paths an intruder can follow while crossing the monitored area. If an intruder I enters the region R_1, then the total amount of energy consumed by the sensors in Zone Z_1 will be:-

$$T(€) = \{€(t_1, pt_1, N_1), €(t_2, pt_2, N_2), \ldots, €(t_n, pt_n, N_n)\} \tag{10}$$

$$\text{Lifetime of Sensors}, L_T(P_n) = \{€(t_n, P_n, N_n); t > 0\} \tag{11}$$

In within-region load handling, we have assumed that all the nodes have different transmission energies. So, if there is any kind of energy imbalance taking place in any part, so it is a clear picture that energy is non-uniformly distributed in that areas. This mainly occurs when there are more than one intruder crossing the border which in turn adds a pressure near the sink nodes; as a result, the connectivity gets lost. During this process, we divide the deployment area into different equilibrium triangle zones that come under a cluster head. In this process, there is zone-to-zone interaction of detection information. This work will further be simplified if there is a nearby base station of a particular zone.

6.2 Consecutive region load balancing in milky-way deployment

During the intrusion, depending upon the path and the number of intruders, energy dissipated by the sensor nodes shall increase on the sensor nodes. Hence, the sink nodes in the region where the intruder is currently positioned shall experience large dissipation of energy from the nodes. This in turn creates an energy hole in the sink node that may affect the connectivity of the nodes when some intrusion activity is taking place, and as a result, the base station may not get the updated information about the presence of the intruder; as a result, the border action team may not take action at the right moment. Hence, keeping in mind about the trajectory of the intruder along with the energy consumption of the sensor nodes, we have set a threshold value of the energy consumption of the sink node which if reaches a limit will send the information to the base station in a hop-by-hop manner as it shall use the other corresponding node as a means of communication and not the other sink node, as this will mean a huge dissipation of energy. This is given as:

$$\text{Lim}_{\text{Threshold}}(N) = 1/N_T \sum_{j=1}^{N(T)} R * E(j) \tag{12}$$

To counter-balance the energy dissipated in each region, we are fixing Eq. (9) as the equation of the threshold. But note that the threshold limit shall not be the same for every region. Since in a milky-way deployment strategy, the inner region shall be denser, so we have fixed a higher threshold value as the successive nodes will be much nearer to each other, so it will be easier to share the distribution of load among the sensor nodes in the place since there shall be more number of sensor nodes which shall be easier to manage.

$$\text{Lim}_{\text{Threshold}}(N) \propto 1/s_d \tag{13}$$

7 Routing of detected information from sensor node to the nearest base station (from monitored sensor region to the base station)

In this section, our aim is to find the probability of at least one node in the border region to improve the performance of the network. We here have made an assumption that the nodes are distributed two dimensionally over the network with the density of the network given by μ. Therefore, the number of nodes present in the monitored region is given by:

$$\text{Number of nodes}, N = \mu * \text{ area of the region} \tag{14}$$

Using the Poisson process, if Y is the random variable representing the number of nodes in the monitored region whose area is given by A, then the probability of the number of nodes in the monitored region is calculated by:

$$P(Y = y) = \left((\mu A)^y * e^{-\mu A}\right)/y! \tag{15}$$

The probability of selecting n nodes out of y nodes is given as:

$$P(Y = y) = \sum_{y=n}^{\infty} \binom{y}{n} p^n (1-p)^{y-n} \tag{16}$$

In this way, the sensor node after detecting the intruder shall select the nodes close to the boundary nodes and route the detected information to the base station.

7.1 Calculation number of hops involved between source and destination

7.1.1 Case 1: if the destination node lies in the sensing range of source node

In this section, we are determining the number of intermediate nodes in the route of detected information from the source to the destination. Here, since our focus is on the power consumption, so we are trying to include minimum number of sensors in this process and minimize the number of hops possible. As a result, we can minimize the path loss as a result of this routing.

Here, we are using Poisson distribution model to determine that the node after detecting the intruder can pass to the destination node if the latter lies in its transmission range. Suppose S is the distance between the source node (involved in detection) and the node to which this information is to be routed. The probability density function between the source node and the next-hop node that is to be communicated is given by:-

$$f(S) = 2\pi\mu S * \text{epow}(-\pi\mu s_1^2) \tag{17}$$

The probability of one hop count can be calculated as:

$$P(1) = \int_o^R f(S) \cdot \mathrm{d}S = 1 - e\text{pow}(-\pi\mu s R^2) \tag{18}$$

which means the communication the source node wants to establish with the node nearer to the destination node that lies in its sensing range R. This is the particular case of any node which the source node wants to communicate while passing the intruder detected information.

7.2 Case 2: if the destination node does not lie in the sensing range of source node

Taking into case if the source node involved in the detection wants to communicate with another node which is out of its communicating range.

Probability if the node takes hop-by-hop approach to pass the intruder information to the base station, then we consider two-hop count which is given by:-

$$\begin{aligned} P(2) &= \int_R^{2R} 2\pi\mu S * \text{epow}(-\pi\mu S_1^2) \cdot \mathrm{d}S \\ &\quad * [1 - e\text{pow}(-\pi\mu s R^2)] \cdot \mathrm{d}S \\ P(2) &= \left[e^{-\pi\mu R * R} - e^{4\pi\mu R * R} \right] * \left[1 - e^{-(\mu/2) * A} \right] \end{aligned} \tag{19}$$

In the same case for three-hop count, four-hop count and remaining hop are measured.

Hence, in general, the number of hop counts H is measured using:

$$\begin{aligned} N_H &= \sum_{n=1}^{p} \text{HC(H)} = P(1) + 2P(2) + \cdots + nP(n), \\ &\quad \text{where } p \text{ is the possibility of the no of hop counts.} \\ &= H\left[1 - e^{\mu\pi s R * R}\right)] + 2[\left[e^{-\pi\mu R * R} - e^{4\pi\mu R * R} \right] \\ &\quad * \left[1 - e^{-(\mu/2) * A} \right]] + \cdots + n[\left[e^{-\pi\mu n R} - e^{n\pi\mu n R} \right]] \end{aligned} \tag{20}$$

7.3 Case 3: connectivity duration that exists between any nodes involved in communication

Connectivity duration is the time for which there is a direct transmission of information about the intruder still taking place as the involved communicating nodes are a part of the routing. It is quite important that the next hop in its transmission range must be ready to establish the communication link between the source node and the next-hop node. As we here have assumed that the transmission speed of the routing information is constant, so there will definitely be a path to route the information, and the communication shall always be maintained.

So, the approximate distance between the source node and the destination within a sensing Range R be S; then, the value of S is computed as:-

$$A_s = N * R_1/(N+1) \tag{21}$$

So, connectivity duration between the transmission node and the reception node is expressed as:-

$$C_D = A_s/\text{vel}_R = [N * R_1]/[\text{vel}_R * (N+1)] \tag{22}$$

8 Handling of intrusion detection in proposed methodology

See Fig. 3

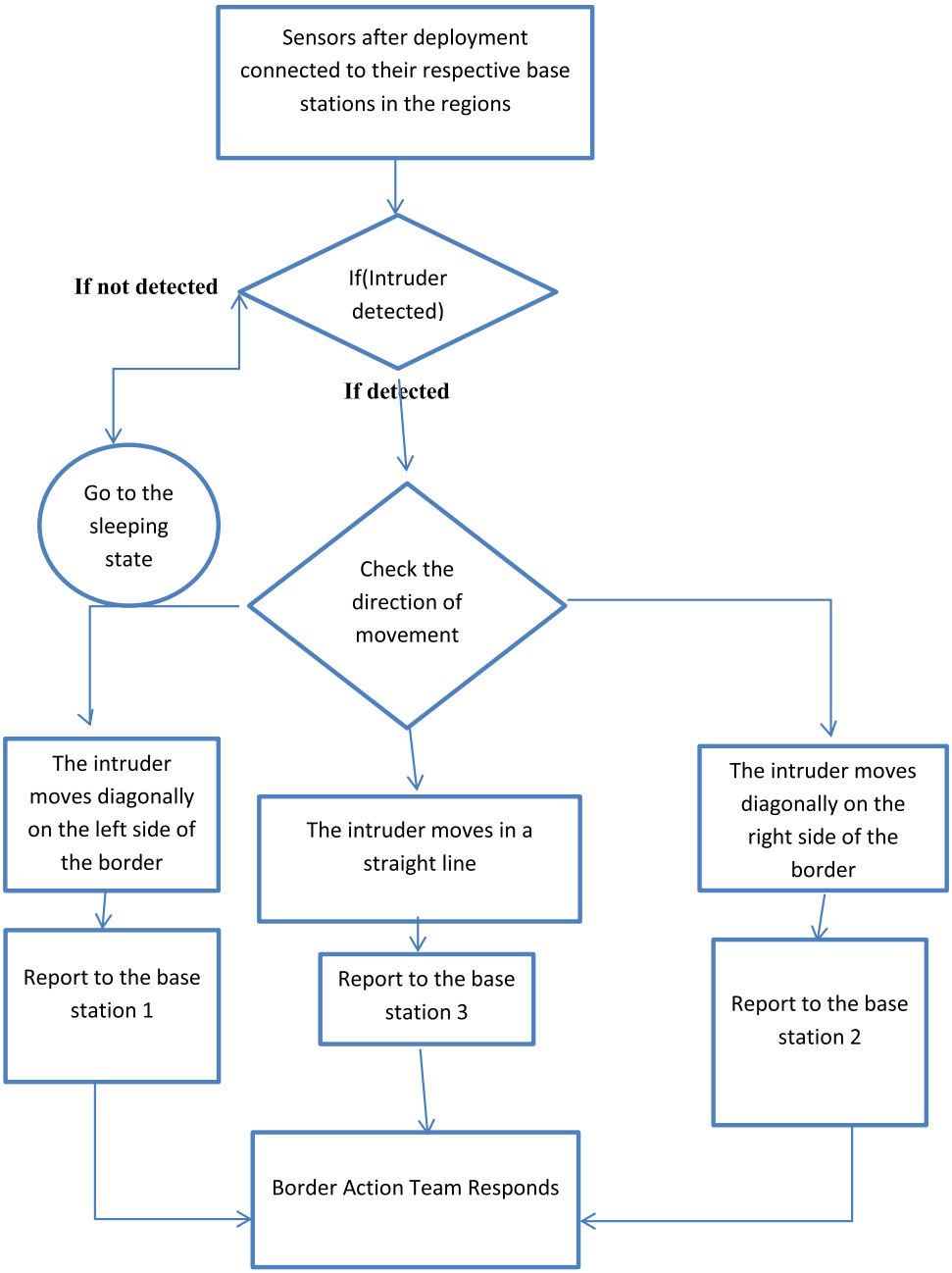

Fig. 3 Flowchart to represent intrusion detection in our work

9 Homogeneous zone routing protocol

This routing protocol is used in order to distribute the load equally among the network depending upon the direction of the intruder and also with the respective zone.

In the homogeneous zone routing protocol, all the nodes share among themselves their details and also, this protocol operates in order to minimize the overall burden taking place in only one part of the network. The algorithm used in the work is given in Table 1:-

(1) We have categorized all the deployed sensors into three groups. Each of these groups, we have classified them as Zone A, Zone B and Zone C. Let S_a^b denotes the bth sensor of the ath layer, $a = 1,2,\ldots,c$; $1 \leq b \leq 3a$. The sensors S_a^b belong to the group M ($M = 1,2,3$), while a $(M\text{-}1) + 1 \leq b \leq Ma$

(2) After the step1, next-hop transmission of the deployed sensors is set. Hence, for these three stages, we develop a probability equation as:-

Table 1 The pseudo-code HZR

Algorithm HZR

for M from 1 to 3 // Maximum No of spiral regions

for every sensor S_a^b // b^{th} sensor of the a^{th} layer .

if a(M-1)+1≤b≤Ma //This is transmission of detected communication from one spiral to other spiral .

$G(S_a^b) = \leftarrow M$ // The Detected information is sent to the base station in next successive node

end if

end for

for every sensor S_a^b // b^{th} sensor of the a^{th} layer. This is the place where the detection takes place

if b=a[$G(S_a^b) - 1$] + 1 // Detection if intruder enters in region 1

$N1(S_a^b) = S_{a-1}^{b-M}$, $r1(S_a^b) \leftarrow 1$ // Sensor node in region 1 responsible for detection.

end if

if a(M-1)+1<b<$G(S_a^b)$a // Transmission in case of detection from one spiral to another.

$N2(S_a^b) \leftarrow S_{a-1}^b$,$r2(S_a^b) \leftarrow$ 1-(a/a-1)+$r2(S_i^{b-1})$ // Sensor node in region 2 responsible for detection

end if

end for

for every available sensor from c^{th} layer to the first layer

Create and receive detected information

Create next hop of sensors

end for

$$N\left(S_a^b\right) = S_{a-1}^{b-M+1};\ b = a(M-1) + 1$$

$$S_{a-1}^{b-M};\ b = aM$$

$$S_{a-1}^{b-M},\ S_{a-1}^{M+1};\ a(M-1) + 1 < b < \text{Ma}$$

(3) Amount of information transmitted to the next hop is determined. Initially, the ratio is set as 1 for S_a^b that contains next-hop sensor. Then, according to the same information received, the ratio of the information of S_a^b which has remaining two hops is determined. For example,- S_a^1 has one next-hop sensor $S_{a\text{-}1}$; S_a^2 has remaining two-hop sensors, S_1^{a-1} and S_{a-1}^2 is determined. We have set the ratio as 1 for S_a^1. For S_a^2, the ratio's are $(a/a - 1) - 1 = 1/a - 1$

and $2-(a/a-1) = a-2/a-1$, which signify that all the detected information of S_a^2 is transmitted to S_{a-1}^1, then $(a-2/a-1)$ to S_{a-1}^2

(4) From the cth layer to the ath layer (i.e. the three directions to the base station), each sensor involved in the process of detection sends it to the base station and generated.

10 Performance evaluation

Here, in this section, we have mainly focussed on how to defend the borders if there are more than one intruder(s). We have tried to understand the situation in the following way:-

(1) If there is a single intruder, what if he uses three ways as shown in the above diagram (which is the chess queen strategy).
(2) If there are one than one intruder (say three), what if they use three different paths to handle that situation. In other words, how to safely route their information effectively and efficiently.
(3) If there are one than one intruder (say four), what if two people run towards left, one towards straight and the other towards right. So, in this way, if the nodes involved in the detection are routed properly, then the power consumption depending upon the intruders' path shall be less.

Chess queen strategy is the name derived from the game of chess the path followed by the piece of queen, viz. one towards right, one straight line and one towards left. But in our work, we have taken the case of three intruders. Using this work, we want to show that if the system is efficient in terms of detection and routing, then we can minimize the power consumption of sensors.

11 Simulation result of the work

Here, the number of sensors used for deployment in this scenario is 100. We have here taken a scenario where the intruder is about to enter the border. This is the simulation result when we are considering the case when more than one intruder. Here, we have taken number of rounds into consideration as at the end of every round, the sensor nodes dissipate some amount of power when they have to transmit the detected information to the nearby base station. Here, in Fig. 4, we have taken a scenario about the status of the sensor nodes before the intruders are about to enter the monitored region.

After the intruder enters the monitored region, we have tried to highlight that the power consumption of the sensor

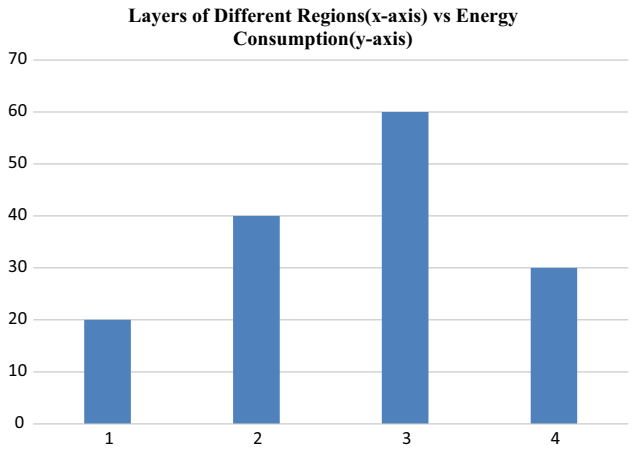

Fig. 4 Energy consumption when the intruder enters different regions

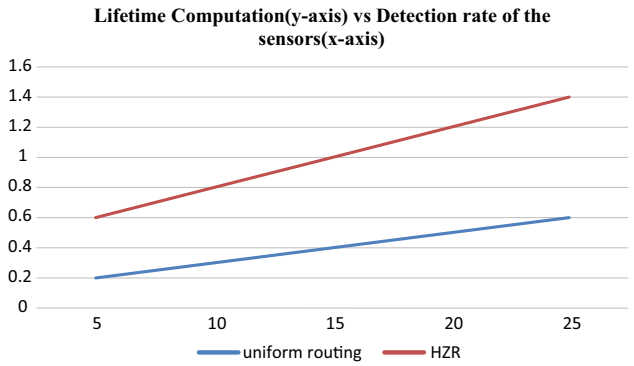

Fig. 5 Lifetime calculation using HZR

node here is handled distributedly depending upon the path that is followed by the intruders. Hence, in this scenario, we have taken the path of the three intruders into consideration and what happens when they adopt any specific path and also how the information that has to be sent has to be decided by the activated sensors. So, in Fig. 5, we have tried to highlight how the sensors detect different intrusion activities, how they monitor their activity and how the power consumption is distributed in this scenario.

Finally, depending upon the intruders' path, we have applied horizontal zone routing and have calculated the intrusion detection rate *Vs* sensor range, using which we can determine how the lifetime of the sensor networks is maximized.

12 Conclusion

In this paper, we proposed a solution for the border surveillance using wireless sensor networks. The major contribution of this paper is the efficient utilization of the sensors deployed along the border such that the problem of energy consumption of the sensors during multiple

intruders tracking can be overcome. We presented the general aspects of a scenario where we focussed on the movement of intruders first apart from node deployment. We also provided the milky-way deployment technique used in this paper to ensure better probability of detection in order to detect the movement of the intruder completely and to reduce the energy consumption of all the nodes in the network by taking into account some of the sensor nodes and which is further minimized by use of multiple zonal base stations. Our work here is focussed on only maximizing the lifetime of the sensor networks only, and this we have done using HZR and using three base stations in turn can reduce the extra burden on the networks if more and more intruders cross the monitored area, especially in nights. We have found using our simulation scenario that our HZR is better in terms of network lifetime than the uniform routing that is done using a single base station. Future work can be done using different deployment strategies.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Akyilidz IF, Stuntebeck EP (2006) Wireless Underground sensor networks: research challenges. Ad hoc Netw 4(2006):669–686

Alkhathami MH (2015) Overview of border control using wireless sensor network. Int J Sci Eng Res 6(3):768–771

Alkhathami M, Alazzawi L, Elkateeb A (2015) Border surveillance and intrusion detection using wireless sensor networks. Int J Adv Eng Technol 8(2):17–29

Bellazreg R, Boudriga N (2013) Border surveillance using sensor based thick-lines. In: IEEE explorer (ICOIN). University of Carthage Tunisia

Cayirpunar O, Tavli B, Kadioglu-Urtis E, Uludag S (2017) Optimal mobility patterns of multiple base stations for wireless sensor network lifetime maximization. IEEE Sens J 17(21):7177–7188

Chakraborty S, Chakraborty S, Nandi S, Karmakar S (2015) Fault resilience in sensor networks: distributed node-disjoint multi-path multi-sink forwarding. J Netw Comput Appl 57:85–101

Cheng C-F, Wang C-W (2018) The target-barrier coverage problem in wireless sensor networks, ieee transactions on mobile computing. IEEE Trans Mob Comput 17(5):1216–1232

Ghosha A, Das SK (2008) Coverage and connectivity issues in wireless sensor networks: a survey. Pervasive Mob Comput 4:303–334

Guerriero F, Violi A, Natalizio E, Loscri V, Costanzo C (2011) Modelling and solving optimal placement problems in wireless sensor networks. Appl Math Model 35(1):230–241

He J, Ji S, Pan Y, Li Y (2011) Reliable and energy efficient target coverage for wireless sensor networks. Tsinghua Sci Technol 16(5):464–474

Hochbaum DS, Mass W (1985) Approximation schemes for covering and packing problems in image processing and VLSI. ACM J 32(1):130–136

Hung KS, Lui KS (2010) On perimeter coverage in wireless sensor networks. IEEE Trans Wirel Commun 9(7):2156–2164

Jin Y, Wang L, Jo J-Y, Kim Y, Yang M, Jiang Y (2009) EECCR: an energy-efficient *m*-coverage and *n*-connectivity routing algorithm under border effects in heterogeneous sensor networks. IEEE Trans Veh Technol 58(3):1429–1442

Kershner R (1939) The number of circles covering a set. Am J Math 61(3):665–671

Lazos L, Poovendran R (2006) Stochastic coverage in heterogeneous sensor networks. ACM Trans Sens Netw 2(3):325–358

Lin J-W, Chen Y-T (2008) Improving the coverage of randomized scheduling in wireless sensor networks. IEEE Trans Wirel Commun 7(12):4807–4812

Melissen JBM, Schuur PC (1996) Improved coverings of a square with six and eight equal circles. Electron J Comb 3(1):32

Mostafaei H (2018) Border surveillance with WSN systems in a distributed manner. IEEE Sens J 99:1–10

Mostafaei H, Meybodi MR (2013) Maximizing lifetime of target coverage in wireless sensor networks using learning automata. Wirel Pers Commun 71(2):1461–1477

Nurmela KJ, Ostergard PRJ (2006) Covering a square with up to 30 equal circles. Laboratory for Theoretical Computer science, Helsinki University of technology, Res Rep. A62, 2000

Said O, Elnashar A (2015) Scaling of wireless sensor network intrusion detection probability: 3D intruders, 3D environments. EURASIP J Wirel Commun Netw 2015:46

Subir H, Amrita G, Sanjib S, Avishek D, Sipra D (2009) A lifetime enhancing node deployment strategy in WSN. Springer, Berlin, pp 295–397

Tiegang F, Guifa T, Limin H (2014) Deployment strategy of WSN based on minimizing cost per unit area. Comput Commun 38(1):26–35

Wang Y, Wang X, Xie B, Wang D, Agrawal DP (2008) Intrusion detection in homogeneous and heterogeneous wireless sensor networks. IEEE Trans Mob Comput 7(6):698–711

Wang Y, Fu W, Agrawal DP (2013) Gaussian versus uniform distribution for intrusion detection in wireless sensor networks. IEEE Trans Parallel Distrib Syst 24(2):342–355