International Journal of Computer Science and Business Informatics

IJCSBI.ORG

Cluster Integrated Self Forming Wireless Sensor Based System for Intrusion Detection and Perimeter Defense Applications

A. Inigo Mathew and M. Raj Kumar
UG Student, Department of Electronics and Communication Engineering
SVS College of Engineering, Coimbatore, India.

S. R. Boselin Prabhu
Assistant Professor, Department of Electronics and Communication Engineering
SVS College of Engineering, Coimbatore, India.

Dr. S. Sophia
Professor, Department of Electronics and Communication Engineering
Sri Krishna College of Engineering and Technology, Coimbatore, India.

ABSTRACT
Intrusion detection and perimeter defense was a major concern for military and civil applications. In military the purpose is mostly for monitoring remote high altitude areas, areas with less access and extreme weather conditions and for force protection. Provided suitable sensors the system can detect identify and classify threads based on the count, number, type weather it is armored vehicles or men in foot, type and amount of weapons they carry, etc., can be detected in advance. This system provides reliable real time war picture and better situational awareness. This will further help to improve the troop readiness and decrease the reaction time. Added using the data collected tactical planning for deploying troops effectively can be done. In case of civil applications economic zones like oil fields, gold mines, can be protected from intruders and attackers. Industrial complex and production facility can be protected with minimized man power and improved efficiency. Basic criteria are which had to be taken into account while deploying wireless sensors for such applications has been discussed. Particularly locating the intruder with respect to the distance from the sensor node to the target in terms of latitude and longitudinal coordinates are discussed here.

Keywords
Radar signals, quantization error, friend identification, power management, perimeter defense

I. INTRODUCTION

Recent trends and advancement of technologies in the area of micro-electronics has lead to the creation of the Micro-Electro-Mechanical Systems, commonly referred to as MEMS [3]. MEMS had overcome the limitations of system on chip technology by providing sensing capabilities of physical parameters and control of the real world through actuators instead of just performing logical operations. Not only MEMS which took advancement in silicon valley, RF technology and digital circuits has also evolved for long distance low power applications and digital circuits have shrinked the circuitry into a single chip and minimized the fabrication cost and time, the sequence of process like sensing, processing, communication and integration lead towards advancement in WSN. Device which used to perform such sensing operations in its range is called as motes which come as a prototype or a commercial product. In this paper wireless mote is used for border surveillance, detection and tracking of enemies in hostile environment to secure our main land. Surveillance needs capabilities to detect, track, identify and classify enemies and priorities them according to the thread. Normally surveillance needs high degree of stealth in order to avoid detection. Placing our soldiers along the border directly leads to their life thread and the solution is to place wireless sensor motes along the borders to listen to the ground. The problem with wireless sensor network is power backup. Energy efficient algorithms have to be deployed to tackle this problem which improves their endurance capability. The main objective of this paper is to discuss how to detect, classify, and track intruders in border to protect our perimeter. A field deployed wireless sensor must have the ability to detect the presence, count, location, track, and identify the intruders.

II. CHALLENGES IN DEPLOYMENT

a) Field noise:

Sensors mainly convert one form of energy signal into other, mostly an analog signal to digital for error free transmission. On the other hand digital systems also have their own problems to tackle. But the worst enemy for any electronic system is its noise. It may be from outside environment of natural noise or an internal noise of system noise. Since our high precision sensor system works on small rate of sample mostly small amount of photons in case of optical sensors and electrons in case of low power circuits [4]. Other than this, in the process of conversion of signals to digital, quantization, aliasing, and bit error rate (BER) after analog to digital conversion (ADC) will also affect the system performance.

b) Field variation

Field of environment taken for study will not remain so for a long period. The nature of the environment may change in course due to climatic conditions which will affect the vision of the system. For example, infrared sensors may get affected due to heat source emitted from vehicles, flame, explosion in its area, activities of our soldiers and it can't be reliable. Radar signals get affected by moisture and mist [4]. Computer vision may get affected due to improper illumination and shadow formation.

c) Background signals

Separating target from background environment is a major issue. The same issue is faced by computer vision in separating target from background in off-laboratory condition. In Some sensing methods like within range systems like RADAR, LIDAR, SONAR can easily be fooled by noise and multipath interference.

Sensing human presence can be put together under a single roof as follow.

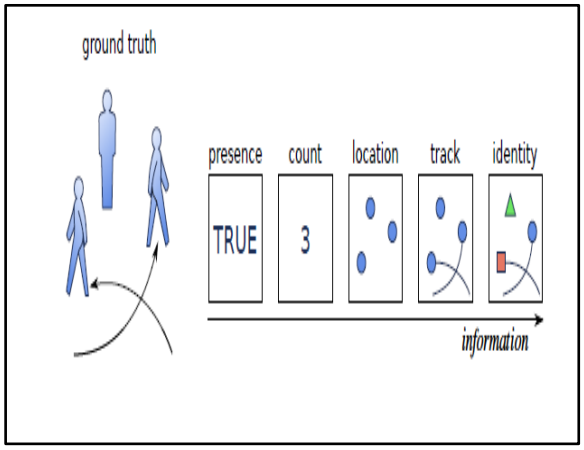

Figure 1: Sensing humans in an environment

III. DECISIONS TO BE TAKEN WHILE SENSING HUMAN PRESENCE

a) Presence

Decision has to be taken "Is there any human beings are present". During this process of detecting the presence the system must not miss took outside environmental components as a human being. In a scenario, if enemy soldiers are airdropped into our territory and if the use dummies

among those (i.e., some dead bodies are airdropped system will mistook them as soldiers) which is a serious issue. Presence has to be justified with no chance if error so that the system can be made system proof.

b) Count

Number of enemy soldiers are intruders present into our territory has to be identified accurately so as precise and valuable intelligence can be provided to our soldiers regarding the hostile environment. Counter measures can be taken accordingly are our tactics can be planned accordingly.

c) Location

Locating targets is very much important to provide surprise attacks on enemy so as we can get him in situation, no idea what is happening. In some scenario locating target is very much important so that we can eliminate thread situation with indirect fire support elements like mortar, artillery shells, and even unguided are guided rockets like Pinnak and Hellfire.

d) Tracking

Course of the enemy or intruder may change in time and it has to be checked continuously so called a task known as tracking. It is same as locating. But it is repeated continuously over time for a long duration. Tracked data has to be continuously updated with our soldier to improve the reliability of the intelligence.

e) Identification

In some situations our soldiers also has to be placed in front of the line and the system must not miss took our solders as intruders and take any counter actions. In some within sensing range sensors this situation is handled by using Friend or Foe (FOF) check. This will be handled by system itself to make it a fool proof.

IV. REQUIREMENT FOR THE SYSTEM TO BE MILITARY COMPATIBLE

a) Physical attributions

In most scenarios the sensor nodes are hand deployed and transported to the field via vehicles or by the soldier in his back pack which means the sensor must be small in size and weight [5]. In some occasions the sensors may be air dropped using transport aircrafts or UAV's in the sense the sensor node has to be ruggedized.

b) Self formation

Deployed sensor nodes must identify its friend with in its range and network itself to transfer data using hopping techniques as like ad-hoc, because of power constrain. It is needed the sensor to be static because some nodes can get displaced due to physical influential factors and the node has to reconfigure with the network. If any sensor node fails reconfiguration has to be done without human intervention.

c) Data flow

During the early stages of the concept of WSN technology particularly during the period of first generation sensor network one way communication is much more enough. But advancement of technology lead us into a new phase of second generation sensor network where in some scenarios the commander has to take control of the sensor node where we need duplexed communication techniques say to steer electro optical sensors like CC TV.

d) Coverage and network size

Coverage in the sense the sensing area of the node. Military standard sensor must require an appreciable sensing area and the network size says about the number of nodes which can be connected with the network. The network must have the property of robustness, self-healing and configurable.

e) Life of the sensor

Some operations last for weeks and some for month's even years. In such case the sensor must last long to provide intelligence of the war picture particularly one placed in hostile environment. If the sensors are deployed for protection of home land and strategic locations it is possible to change the power source which further improves the life of

the sensor. In some modes the sensor need not to function to its full effect and there some power saving algorithms are deployed to save more power thus to improve life.

f) Stealthy characteristics

Now-a-days stealthy is not only for human eyes. Stealth is to cover from every illuminative characteristic. Means also from electronic and electromagnetic signature. Deployed node must emit very tiny electronic signature.

g) Reliability

Data gathered must be reliable for the commander to take split seconds decision. The network must provide necessary security to avoid eaves dropping, tampering and interception.

h) Denial of service

In any instant of physical attack on the sensor nodes it must be capable of reporting it back to the command center by using some switch mechanism.

i) Tamper proof

Any single data present in the sensor may leads to compensate national security if it gets in the hands of third party. So that the node must be tamper proof to secure the data within it.

j) Cost

One of the deciding factors for implementation of any project in real time is the overall cost of the system in terms of implementation and maintenance. So this factor has to be taken into account during pre and post development of the product by implementing latest technology.

V. MILITARY APPLICATION

One of the main applications of wireless sensor network for security purpose like base protection and perimeter defense. In base protection wireless sensor motes will be placed around the base to provide real time data. All the data gathered will be relayed back to the command and control center located in the base. Our sensor mote will look for intruders in any

form. Our sensors will take care of seismic and acoustic signature of the intruder. If necessary thermal imagers can also be placed to identify targets. In a practical scenario it is necessary to provide surveillance capability upto10 kilometer from the base. But target identification is enough up to four kilometers. Since the area of 10 kilometer radius is covered for surveillance [1], it provides necessary time for our force to get ready for combat.

In case of perimeter defense, we may need to cover a large area like remote villages, roads connecting key locations for hostile activities. In such cases we may also need real time war picture of the battle space where it is necessary to place electro optical sensors like CCTV with day and night optics and thermal imagers.

a) Operational issues

The sensors have to be connected in a configuration which provides dynamic target conformation details if one mote fails. If a mote senses a target and it got failed due to some external or internal tamper before it reports to base station, anther mote must be able to identify and track the same target. Collecting more samples from many motes regarding the same event will improve the accuracy of data, but improves the band width [2]. In case of any mote failure system has to reconfigure dynamically on its own. To locate the exact latitude and longitudinal coordinates of the enemy, the mote first must be able to know its own location. Let us consider the stationary mote as 'A', whose latitude and longitudinal attributes are known to it. Now one of the sensors in the mote detects the presence of an enemy, but it doesn't know the latitudinal and longitudinal coordinates. Instead the mode just finds the distance of the target from its sensor, which is 'B'. Using this value one can get the coordinates of the target.

Normally the distance can be calculated using the following methods.

Let 'R' be the radius of the earth which is approximately 6,371 km.

$$\Delta lat = lat_2 - lat_1$$

$$\Delta long = long_2 - long_1$$

Another method was to use Haversine formula.

$$A = \sin^2(\Delta lat/2) + \cos(lat_1) x \cos(lat_2) x \sin^2(\Delta long/2)$$

$$C = 2.a \tan2(\sqrt{a}, \sqrt{(1-a)})$$

$$D = R*C$$

According to Spherical law of cosines,

$$D=\text{acos}(\sin(lat_1)\sin(lat_2)+\cos(lat_1)\cos(lat_2).\cos(long_2 - long_1)) * 6371$$

But all these method is used to find the distance between two known longitudinal and longitudinal parameters. But in our case the reverse in required. We need to calculate the longitudinal and longitudinal parameters using the known distance. In this method the directional factor affects the measured value. Direction of the target can be found by the sensor which faces in that direction. But this method of finding the direction will not be that much accurate. But the distance to that target in that direction can be found accurately.

Let as consider as ultrasonic range finder which is used here. The distance to the target is found using the bounced energy from the target. But because of the environmental objects the noise will be more. This can be eliminated using adaptive filter technology. Here the cut-off frequency of the software defined filter can be changed dynamically. Thus the noise can be eliminated.

Next factor will be the position of the sensor mote. This data can be found using the GPS chip inbuilt in the mote.

Consider ‘X’ which is the position of the mote and ‘Y’ which is the distance to the target which gives the coordinates of the target. This is related by

Unknown coordinates = known coordinates + distance

Note: here the distance is related to the angle and also the direction. The directional angle can be related with the coordinates by the following method.

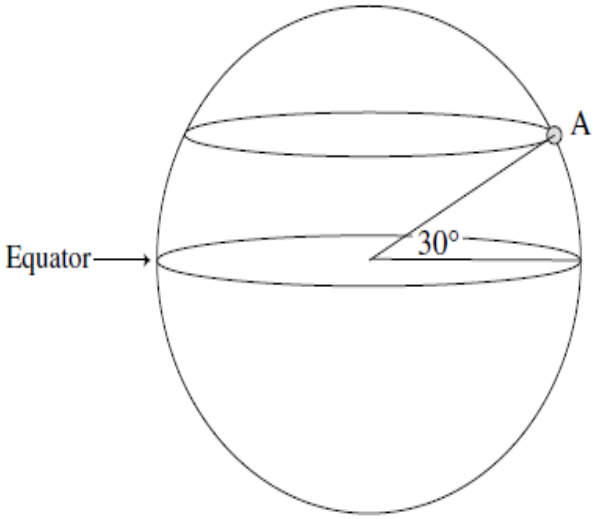

Figure 2: Determining latitude with respect to equator

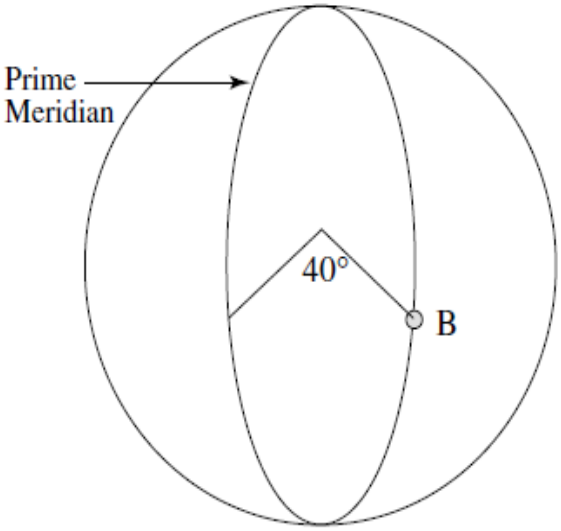

Figure 3: Determining longitude with respect to the prime meridian (green which meridian)

Equator is an imaginary line which decides the earth into two, northern and southern hemisphere. The latitude of the equator is 0 degree. Point 'A' forms some angle with equator which is 30 degree north. Latitude is the degree to north or south of the equator. Prime meridian is a line of reference which divides the earth into two, eastern and western hemisphere [14-19].The longitude of the prime meridian is 0 degree. Meridian to longitude is the degree to which the point is east or west. Here the point is forty

degree east.Thus using directional angle procedure we can say the unknown point here is 30 degree north and forty degree east. Thus the position of unknown target can be found.

But the real problem arises when four sensors each for each direction work simultaneously. The reference points for 0^o, 90^o,180^o, 270^o has to be well defined. This is similar to working on a graph. Assume that each sensor can cover 90^o which represents one quadrant. Four sensors represents four quadrants. Each mote contains four sensors and thus a single mote can cover up to 360^o.

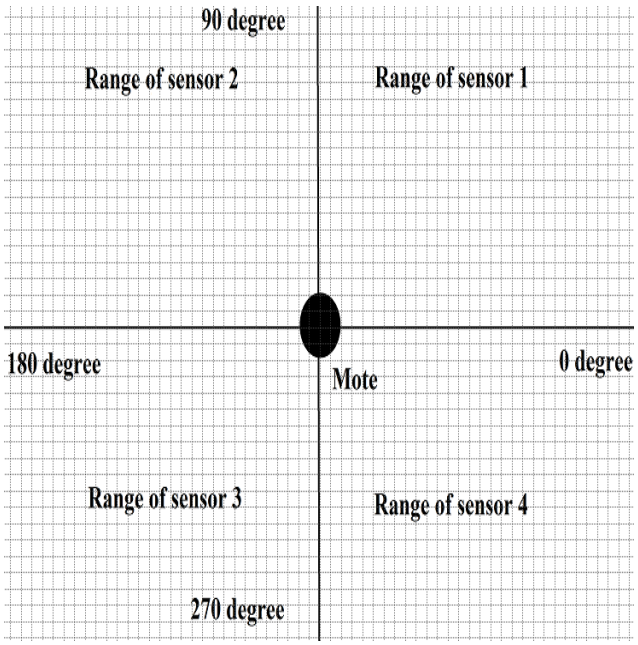

Figure 4: Sensor arrangement in a single mote

Now the next issue will be the integrity of the data collected by the mote. For better accuracy and conformity one of the basic principles of digital communication is adopted. More the sample more accurate the data. So up to three motes can be placed in a close range so that the range of one mote can form triangulation pattern with other mote. Combination of data from these clusters of motes can be used to define the exact coordinates of the enemy. Also the blind spot of one sensor in a particular direction can also be eliminated with this group of sensors.

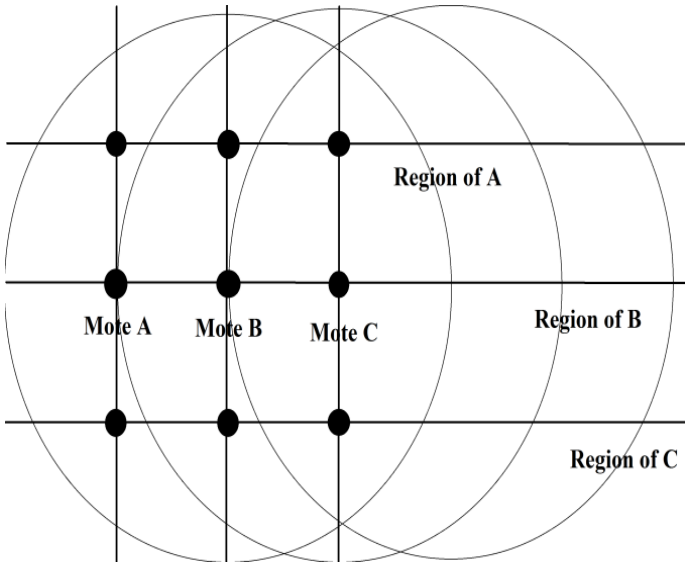

Figure 5: Deployment model of multiple motes

This above figure clearly indicates that each sensory motes are covered by other adjacent motes. This approach will reduce the blind spot and improves integrity of data but increase bandwidth usage to its peak. This approach will also be helpful if any one of the motes fails.

b) Operational flow

The below mentioned flow chart clearly explains the operational method of the system. In the system if the distance to the target was found as infinity, the targert was ignored. Because no target can be infinite and infinity cannot be measured. The range to be measured can also be pre-defined, i.e., the threshold value can be set, which is based on the level of noise. Say if a signal with output voltage is found as 8V and it can be ignored if output above the range of 6V is found as noise.

VI. CONCLUSION

Implementing such self forming sensors will reduce the deployment and maintenance cost which also helps us to provide better situational awareness and troop readiness in case of military scenarios. In civil application perimeter can be managed effectively using such wireless sensors. In future the same will be done in hardware and real time operational issues will be discussed.

Flow Chart:

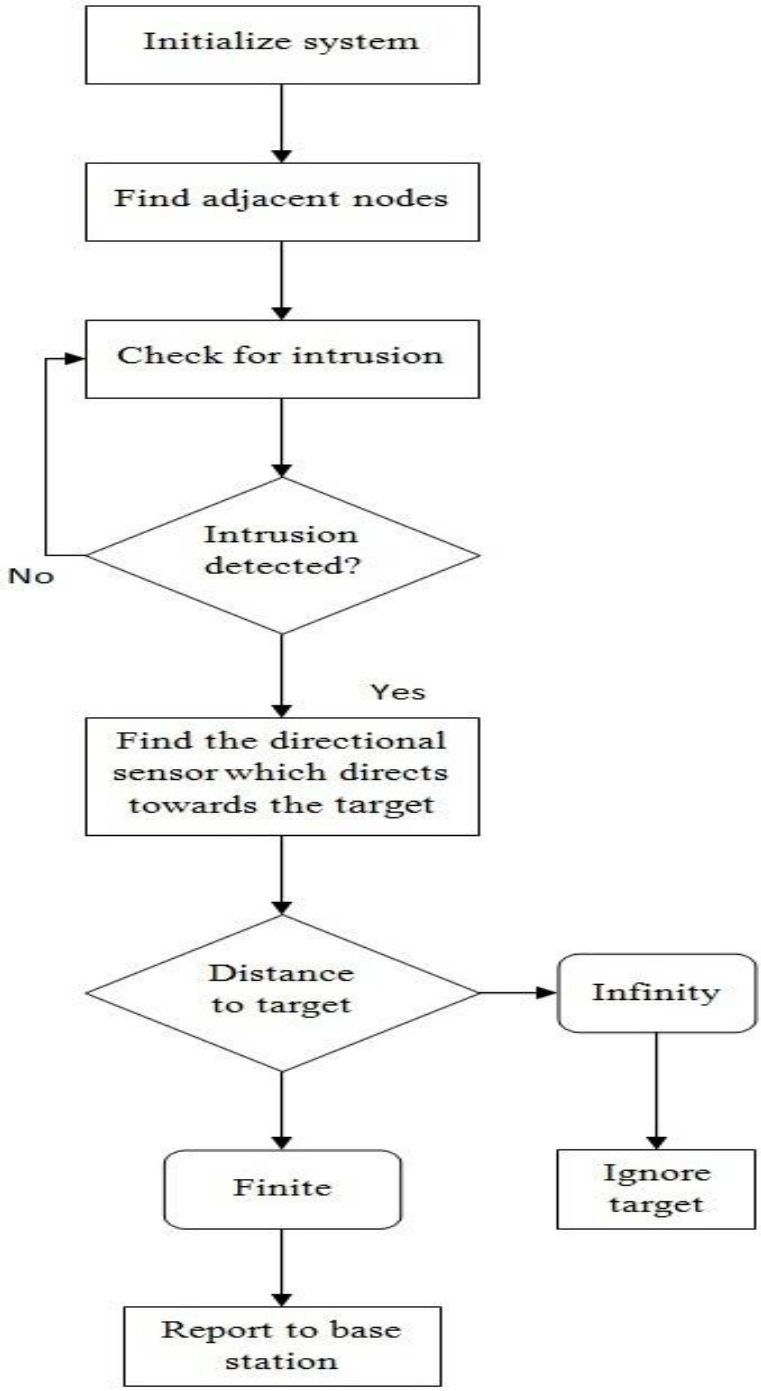

Figure 6: Flow chart of the methodology

References

[1] http://www.memsnet.org/mems/what-is.html.

[2] Thiago Teixeir, Gershon Dublon, "A survey of human-sensing: methods for detecting presence, count, location, track, and identity", ACM Computing Surveys, Vol. V, No. N, 20YY, Pages 1-77.

[3] Michael Winkler, Klaus-Dieter Tuchs, Kester Hughes, and Graeme Barclay. "Theoretical and practical aspects of military wireless sensor networks", Journal of Telecommunications and Information Technology, pp. 37-45.

[4] K. Akkaya and M. Younis, "A survey on routing protocols for wire-less sensor networks", Ad-hoc Netw., no. 3, pp. 325–249, 2005.

[5] Al-Karaki and Kamal, "Routing techniques in wireless sensor networks: a survey", IEEE Wirel. Commun., vol. 11, iss.6, pp. 6–28, 2004.

[6] Niculescu, "Communication paradigms for sensor networks",IEEE Commun. Mag., vol. 43, iss. 3, pp. 116–122.

[7] Bhattacharya, Kim, Prabh, and Abdelzaher, "Energy conserving data placement and asynchronous multicast in wireless sensor networks", Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys), May 2003.

[8] Blum, Nagaraddi, Wood, Abdelzaher, Son, and Stankovic, "An entity maintenance and connection service for sensor networks", First Intl. Conference on Mobile Systems, Applications, and Services (MobiSys), May 2003.

[9] Boselin Prabhu, SR & Sophia, S, 2012, 'A research on decentralized clustering algorithms for dense wireless sensor networks', International Journal of Computer Applications, vol. 57, no. 20, pp. 35-40.

[10] Boselin Prabhu, SR & Sophia, S, 2013, 'Mobility assisted dynamic routing for mobile wireless sensor networks', International Journal of Advanced Information Technology, vol. 3, no. 3, pp. 9-19.

[11] Boselin Prabhu, SR & Sophia, S, 2013, 'A review of energy efficient clustering algorithm for connecting wireless sensor network fields', International Journal of Engineering Research and Technology, vol. 2, no. 4, pp. 477-481.

[12] Boselin Prabhu, SR & Sophia, S, 2013, 'Variable power energy efficient clustering for wireless sensor networks', Australian Journal of Basic and Applied Sciences, vol. 7, no. 7, pp. 423-434.

[13] Boselin Prabhu, SR & Sophia, S, 2013, 'Capacity based clustering model for dense wireless sensor networks', International Journal of Computer Science and Business Informatics, vol. 5, no. 1, pp. 1-10.

[14] Boselin Prabhu, SR & Sophia, S, 2013, 'Hierarchical distributed clustering algorithm for energy efficient wireless sensor networks', International Journal of Research in Information Technology, vol. 1, no. 12, pp. 45-55.

[15] Boselin Prabhu, SR & Sophia, S, 2013, 'Real-world applications of distributed clustering mechanism in dense wireless sensor networks', International Journal of Computing Communications and Networking, vol. 2, no. 4, pp. 99-105.

[16] Boselin Prabhu, SR & Sophia, S, 2013, 'An integrated distributed clustering algorithm for dense WSNs', International Journal of Computer Science and Business Informatics, vol. 8, no. 1, pp. 1-12.

[17] Boselin Prabhu ,Inigo Mathew,A, SR & Sophia, S, 2014, 'Modern cluster integration of advanced weapon system and wireless sensor based combat system', Scholars Journal of Engineering and Technology, vol. 2, no. 6A, pp. 786-794.

[18] Chen, Jamieson, Balakrishnan, and R Morris, "Span: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks", 6th ACM MOBICOM Conference, 2001

[19] Arras, Mozos, and Burgard. "Using boosted features for the detection of people in 2d range data", In Proc. of the int. conf. on robotics & automation, 2002.

This paper may be cited as:

Mathew, A. I., Kumar, M. R., Boselin, S. R. P. and Sophia, S. 2015. Cluster Integrated Self Forming Wireless Sensor Based System for Intrusion Detection and Perimeter Defense Applications. *International Journal of Computer Science and Business Informatics, Vol. 15, No. 3, pp. 70-83.*