

IFAA: An Intelligent Framework Aware Algorithm to Determine the Boundary of Area under Attack in Military Surveillance and Reconnaissance WSN



Deepak S. Raj^{1,2,3*}, Ramesh H.S. Babu¹

¹ Department of CSE, Sai Vidya Institute of Technology, Bangalore, Karnataka 560064, India

² Visvesvaraya Technological University, Belagavi, Karnataka 590018, India

³ Department of CSE, Presidency University, Bangalore, Karnataka 560064, India

Corresponding Author Email: sdrbangalore@gmail.com

<https://doi.org/10.18280/ria.360417>

ABSTRACT

Received: 17 February 2022

Accepted: 25 May 2022

Keywords:

WSN, intelligence surveillance, military ISR, sensor management, boundary detection, situation awareness

Wireless sensor networks (WSNs) have proven effective in military applications of surveillance and reconnaissance. Sensors capable of detecting pressure, temperature, movement and presence of specific chemicals are deployed in such applications. Traditionally, sensor data is collected and transferred to a centralized high-capacity node or control station. Analysis of data is carried out at such centralized facilities. Information or intelligence gathered from sensor data after analysis is used to generate control and management commands that are relayed back to sensor nodes. The situation is analogous to an actual wartime scenario where soldiers who are on the field are equivalent to the sensors. Soldiers observe and sense the situation and communicate their observations to the decision maker who is stationed in the control tent. On gathering field information, the decision maker analyses the data and arrives at his decision which is again communicated to the soldiers on the field. Soldiers as well as sensors are not placed illogically or randomly but intentionally and strategically. Observations made on the field ultimately affect how the soldiers or sensors continue to function. Intelligence gained on the field ultimately gets used on the field itself. Our attempt is to observe, analyze and apply intelligence on the field itself. This work proposes an intelligent algorithm that is aware of the sensor network topology, analyses sensor data within the network and uses the network framework to arrive at usable intelligence. Locally generated intelligence avoids communication to and from the command/control and adds value to military surveillance and reconnaissance applications of WSN. Intelligent sensor management allows us to use just the necessary number of sensors while saving resources on otherwise redundant expenditure. In the present work we have designed and applied a dynamic boundary computation algorithm to determine the boundary of the area under attack. We have compared the results of simulation experiments incorporating the proposed algorithm against a control experiment without the algorithm.

1. INTRODUCTION

Wireless sensor networks (WSNs) are described as a collection of specialized transducers equipped with an appropriate communication infrastructure developed for the aim of either monitoring or recording different designed circumstances in various places. Temperature, pressure, humidity, wind direction and speed, light, vibration, and sound intensity, power-line voltage, physiological functions, and pollution levels are some of the most regularly monitored characteristics utilizing a sensor network. Because a sensor network can connect the physical and logical worlds, it is one of its most important advantages. It can do this by gathering information from the physical world and transmitting it to sophisticated logical devices that can process it. Because of this, it is possible that the collection of data for military and civilian purposes will need less human interaction or interference if we use technology to its full potential. Figure 1 depicts a military surveillance situation in visual form.

Military personnel must keep an eye on the nation's borders,

where adversaries may infiltrate, and an assault could be launched. It might be either a vast land mass or a vast body of water. As a result, a comprehensive examination of the monitoring area's geography is required. A wireless client is an individual who uses a wireless network's services. At the location, there are armored, and patrolling vehicles equipped with radar (both terrestrial and aerial). If the national boundary is an ocean, ships, boats, and water vehicles are required to monitor the oceanic zones, which are under the command and control of naval troops. Advanced technologies including SATCOM Radio, Backhaul Radio, Wireless Access Point, and UAV Link Radio allow them to communicate with the local and central control units. Sensors such as acoustic, vibration, seismic, and motion sensors are used. Among the duties of military surveillance systems are monitoring the borders, monitoring friendly troops, monitoring the reconnaissance of opposing forces, equipment, and ammunition, target tracking, and the evaluation of combat damage caused by nuclear, biological, and chemical attacks.

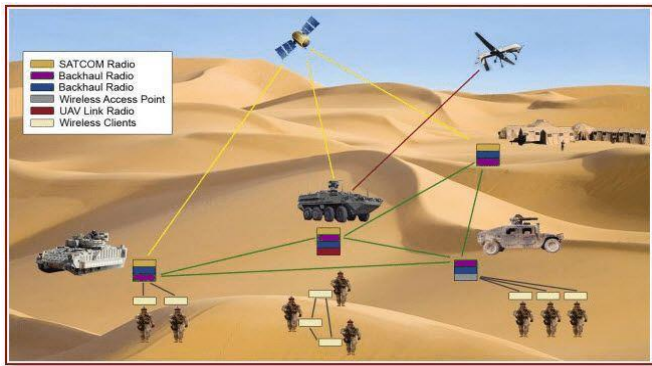


Figure 1. Military surveillance scenario

Surveillance is defined as the continuous act of monitoring behavior of a system with its constituent entities in order to validate compliance with set norms of behavior [1]. The set norms of behavior are location dependent and are set to vary based on societal rules and regulations. For instance restrictions on smoking in hospitals, schools or fuel stations. Ban on bringing weapons in to theatres, public areas like parks and schools. Surveillance usually involves monitoring activities occurring in a fixed area or region. Deviations, if any, from the present normal behaviour needs to flag off an alarm to initiate combating mechanism. Basic purpose of surveillance is to keep an eye on a volume of space for an extended period of time. As long as the space is unaffected or operations and changes happening there are in line with expectations, nothing is done. In case of abnormal or unexpected changes surveillance must trigger off a series of counter measures. Historically surveillance has been a human intensive activity, digital surveillance systems have replaced round the clock human guards. However digital surveillance is limited to data collection. Analysis of sensor data and further analysis still continue to be invested in the hands of humans [2]. Human involvement brings in an element of error prone analysis and marginal reduction in efficiency with increase in time duration of analysis. Smart surveillance or intelligent surveillance overcomes these drawbacks by incorporating much needed intelligence within the surveillance framework itself. Recent increases in acts of terrorism have added immense value to surveillance and reconnaissance. Types of attacks have advanced, attackers have adapted technology, in most cases cutting edge technology to perpetrate terror. Such changes call for real-time and immediate counter measures to be initiated. A moment's delay in detection, analysis and application of intelligence in combating the threat makes the entire exercise futile. Therefore, the surveillance needs to be an intelligent or smart as well as proactive and independent framework [3].

Typical military surveillance and reconnaissance systems are built out of heterogeneous sensors, they are typically deployed to organize themselves into a network without human intervention. Due to the variety of parameters sensed, they are almost always in multimodal data and information fusion state. Collaboration in resource control and utilization are also challenges of WSN deployments. Additionally, sensor networks for military surveillance require intelligent sensor management unlike in civilian applications where need and scope of management is minimum and not critical. As against the centralized surveillance framework, which is rigid and less appropriate for military deployments, a distributed framework with computational capability spread across network

components is more suitable. Such a framework is composed of smart sensor networks spread over large geographical areas. Greater the area under surveillance, greater the number of nodes deployed. Increase in number of nodes mandated an element of management. Management of node resources must not be fixed but proactive and dynamic. There is another facet of smart distributed surveillance, data volumes. Like how sensor nodes are managed, the huge volume of data they gather as a network must also be managed to gather intelligence. Sensor management process involves planning, controlling and decisive use of sensor nodes of the surveillance framework to optimize the efficiency [4].

An intelligent framework involving sensor management is a system of organization aimed at generating situation awareness by management of sensor nodes [5]. In building such a process, sensor node cooperation and coordination are also achieved. Such a scheme allows us to use optimal combinations of strategically selected sensor nodes instead of redundantly using every node within deployment. This work proposes an intelligent framework aware algorithm Dynamic CH (IFAA- dynamic convex hull) to determine the boundary around intruders in a military surveillance and reconnaissance WSN. Convex hull algorithm determines the boundary of the least area encompassing random points in a two-dimensional space.

The remainder of the sections of the paper's structure are section II, which discusses the related works; the proposed model is discussed in the III section. Design and implementation are discussed in the IV section. Section V, the conclusion of the work.

2. RELATED WORK

Studies related to high level sensor management are reported in [6, 7], where a situation aware as well as business aware framework is proposed with improvements reported in homeland security and surveillance. They propose a high-level management approach to sensor control. With different types of sensors, an additional unit is incorporated to combine data. Additionally, an inference mechanism is also implemented to make informed decisions. Error in sensor data is also accounted for. Sensor node energy levels or general health is also an additional parameter in management decision making. Sensors deployed are not custom made and thereby bring down the cost of deployment and makes the framework affordable. Due to the inherent centralized approach, the work carried out is unscalable and involves risk of bottleneck in exchange of control and command exchange. Similar to work in the same domain, performance analysis or testing are ignored.

The research presented in Teixeira et al. [6] proposes an abstraction approach to situation awareness in a business environment. The architecture proposed is flexible and enables scaling. Deployment of seemingly unconnected devices is achieved there by implementing service-oriented design. The work goes on to prove that higher level usable intelligence gathering need not depend upon low level knowledge.

The work Flammini et al. [7] in particular analyses methods for optimized resource allocation in an environment having video and multimedia surveillance. The communications examined are over the internet and a wireless ad hoc network and WSN. A control-based sensor management scheme is studied in Paggi et al. [8]. The paradigm behind the

infrastructure is called holonic. Triad of sensor networks, the communication platform and the intelligence gathering group is the basis of the architecture. Sensor nodes are at the bottom of the triad. Every platform is associated with a set of sensors and controls them. Larger sensor management task is divided into functional subtasks and assigned to each one of the many platforms. This framework necessitates the increase in the number of holons as the size of network deployment also increases. Such an increase contributes to the increase in complexity also. Despite drawbacks of the work like limitations in simulation experiments where a single threat is only considered and comparison between open and closed approach of implementations, the work successfully proves the efficacy of holonic architecture in sensor management.

Multi object optimization is the focus if work in Iqbal et al. [9]. The chance of overlooking occurrence of an event and the chance of recognizing a false positive are the key parameters considered in the work. These are the two key parameters considered in the sensor management model designed. Bird's eye view or the larger scale intelligence gathered from ground observations made by individual sensors is an NP complete problem. In this work, particle swarm optimization is applied to combat this issue of intelligence optimization. Results published in this work shows reduction in the chance of false alarm at the cost of heavy weight computation. Such large computation loads are manageable in networks with greater computational capability but unsuitable in WSNs.

Preece [10] have worked with assignment of sensors to missions by following a natural language based approach. They base their work on a market architecture for sensor management built around a computational economy. Framework is under the control of dual managers, namely mission manager and sensor manager. Mission level decisions and intelligence gathering activities are managed by the mission manager which also assigns priority to various contending tasks. Prioritized tasks are further assigned to sensor managers which are responsible for carrying out tasks from sensor data collection, aggregation and analysis. Sensor managers in turn assign and schedule tasks to sensor nodes. Network resource management is also under their jurisdiction. In case of deadlocks or faults in communication flow, they take up the additional responsibility of troubleshooting too. Among sensor nodes under one's control, sensing tasks are universally allocated. Data aggregation tasks are however assigned to a select few sensors only based on their current physical parameters. Free slots of sensor nodes and bandwidth available with them for use in communication channels are published by all entities. This data is used to calculate consumer bid prices.

A service chart-based database along with bid formulators are used to convert sensor infrastructure into a service database. Service database is the basis of allocating resources to advanced applications like targeting, identification of intruders, environmental monitoring, and such where intelligence gathering is involved. Service chart allows us to compare all possibilities of allocations, which can further be mapped to a list of costs and thus a decision can be made on optimized allocation. After bids are placed, an auction finalizes the most profitable bid as the winner allocation. Ultimate winner of the auction is aimed at maximizing gain while restricting the number of allottees of each resource to one only. The bidding scheme requires a centralized sensor management and control. Centralized control rules out scalability and flexible deployments. Exchange of bids add

communication overhead too. Further, the decision regarding the winner of bids is an NP-hard problem. Overall the scheme adds considerable complexity instead of reducing it in terms of computation and exchange of control communication.

Singh et al have presented a thorough analysis of trajectory schemes for data collection using mobile elements in WSNs in Singh and Kumar [11] among which an integrated mobile surveillance system is one. This system consists of a fixed subset of sensor deployment in addition to another subset of mobile sensors [12-15]. The framework proposed is for real time applications. Its working principle is based on reactive activity. Sensor management is centralized and event driven. Management is implemented within an external server that is the focus of sensor data collection and single point of control command dissemination. System users must communicate with the sensor network via the server and receive data in usable format at the server itself. On receiving command from the server, fixed location sensors start their sensor activity and continue to transfer back sensor data. Sensor data is continuously monitored and if and when abnormalities are observed, command is sent to mobile sensors. Mobile sensor nodes respond to commands on cue. Mobile nodes have the freedom to move to locations that require attention and perform additional surveillance or reconnaissance activities. Drawback of the architecture is the bottleneck in data gathering and huge overhead in analysis on the external server.

The problem of computing the convex hull is studied in [16-20]. Graham's scan is reported as having an efficiency of $O(n \log n)$ [21]. An alternate three-dimensional implementation of Graham's scan reporting the same efficiency is available [22]. Guo et al. [23] reports Jarvis march approach having an efficiency of $O(nh)$, its implementation is reported to have an efficiency of $O(n \log h)$ in Hernández-Landa et al. [24]. All these algorithms which have h are output sensitive. In the military surveillance scenario, nodes detect intrusion dynamically. Due to the inherent dynamism in data collection itself, a dynamic algorithm serves the application better.

3. PROPOSED MODEL

We have designed the model for experimentation and simulation consisting of the following components.

$U = \{(x_i, y_i) | L \leq x_i \leq H \ \&\& \ L \leq y_i \leq H\}$ is the universal set of node coordinates where i and j assume all values in the range $(1, N)$ and N is the number of sensors deployed, L is the minimum index and H is the maximum index.

$C_1 = \{(x_i, y_i) | L \leq x_i \leq H \ \&\& \ L \leq y_i \leq H \ \&\& \ (x_i, y_i) \text{ is an element of } U \text{ that has returned TRUE from negative selection}\}$ is the set of candidate points for the first iteration.

$C_i = \{(x_i, y_i) | L \leq x_i \leq H \ \&\& \ L \leq y_i \leq H \ \&\& \ (x_i, y_i) \text{ is an element of } C_{i-1} \text{ that has returned TRUE from negative selection and belongs to the boundary set identified in the } i\text{-1th iteration of boundary detection}\}$ is the set of candidate points for the i th iteration.

$C_{i+1} = \{C_i - C \cup C_{i+1}\}$ is the set of candidate points considered as candidates for the $i+1$ th iteration of the boundary detection algorithm.

$HF = \{(x_i, y_i) | L \leq x_i \leq H \ \&\& \ L \leq y_i \leq H \ \&\& \ (x_i, y_i) \text{ is on the determined boundary}\}$ is the set of all points on the boundary encompassing the minimum area polygon enclosing every node that has sensed and reported intrusion.

$H_1 = \{(x_i, y_i) | L \leq x_i \leq H \ \&\& \ L \leq y_i \leq H \ \&\& \ (x_i, y_i) \text{ is identified as a boundary node}\}$ is the set of nodes belonging to

the set U and identified as a node on the boundary encompassing the area under intrusion, that are identified after first iteration. $H_{Fi+1}=i=n,m$ Is the function defined $i=0$ $\sum_{j=0}^m$ for Dynamic CH computation (C_j , of H_{Fi} the) dynamic boundary.

Here n nodes identified in the $i-1$ th iteration are retained along with m nodes from the candidate nodes of the i th iteration. The algorithm computes incremental output of the

$i+1$ th iteration. Therefore, the algorithm output of i th iteration depends on the number of nodes identified as boundary nodes in the previous iteration. The asymptotic algorithmic efficiency is therefore $O(n \log h_i)$ where h_i is the number of nodes identified on the i th iteration and n is the cardinality $|C_j|$.

The algorithm is exercised in a simulation environment as described in the next section. Design is based on an attempt to overcome challenges of studies summarised in Table 1.

Table 1. References summarized based on methodology

Ref.no	Published year	Methodology	Advantages	Disadvantages
[5]	2019	The most efficient auction process for the tracking of a target.	Better performance, in terms of MSE	Need to focus on more accuracy for auction-based crowdsensing.
[6]	2020	LAURA - Lean Automatic code generation for situation-aware and business-aware Applications. To minimize the impact of vagueness and uncertainty in message exchanges based on an interconnected set of fully intercommunicating elements (peers), this paper examines holonic structures or formations that are generated when there are constraints on resources (energy, available messages, time, etc.).	Provide better results for situation-aware or business-aware final IoT applications	Need to focus on Quality of Context parameters.
[8]	2020		Provides shortage of resources prevents communications	Produce the low-quality results
[9]	2016	Different sensor network optimization problem-solving techniques were described in the research.	Different sensor network design, operation, deployment, location, planning, and management issues may be addressed using the suggested multi-objective optimization approaches.	Need to focus on optimisation.
[17]	2019	In order to recover the original dataset, we proposed three unbalanced data processing algorithms and retrieved protein attributes from the evolutionary conservation of amino acids to develop a predictor for the identification of protein interaction locations	Improving protein-protein interaction site prediction	Need to focus on accuracy

Algorithm: DynamicCH(C_j, H_{Fi}, R) $R \geq 1$

1. $I \leftarrow \text{Union}(C_j, H_{Fi})$
2. Identify partitions of I , $I_1, I_2, I_3, \dots, I_{n/m}$ each of maximum cardinality m
3. For $i \leftarrow 1$ to m do
4. Compute $\text{conv}(I)$ by applying Graham's scan, store in counter clockwise order
5. $I_0 \leftarrow (0, -\infty)$
6. $I_1 \leftarrow$ point of I with maximum positive x coordinate value
7. For $k \leftarrow 1$ to R do
8. For $l \leftarrow 1$ to n/m do
9. Compute point C_i belonging to candidate set such that C_i does not belong to C_{i-1} by performing binary search of vertices from step 4
10. If $C_{i+1} = C_i$ return list
11. Return error

4. IMPLEMENTATION AND RESULTS

The problem identified for implementation in the present work is divided into two stages of incorporation of intelligence. First stage is to determine the boundary of the area under attack or intrusion. The second is to compute the area under attack. Once an area is under intrusion, further countermeasures entirely depend upon the location and extent

of intrusion. These two intelligence parameters are critical in mission control and management. Simulation experiments are carried out on Matlab R2021a running on Intel® Core™ i3-6006 CPU @ 2.00GHz 1.99GHz with 4.00 GB RAM. Test bed design is grid based. Extent of the grid is 800X800 mts. Each square unit is of measure 20X20 mts identified as a unit cell. Every unit cell is under the surveillance of one high power node identified as the grid head. Simulation results are repeated for larger areas in multiples of the initial dimensions. Results are found to be consistent.

This high-power node is represented as the red coloured circle in the Figure 2. The sky-blue coloured node is also a high-power node but not a grid head. The dark blue coloured nodes are low power nodes whose responsibility is limited to sensing of physical parameters. The screenshot in the figure is showing a sample of the outcome of one of the many simulation experiments. Additional nodes are deployed as per the framework design and need. Green coloured circles represent the boundary nodes of the minimum area identified, enclosing every node that has detected an intrusion.

As coordinates of nodes are fixed and available in data structures, distances are computed as Euclidean distances. Algorithm applied to determine attack locations is an artificial immune algorithm of negative selection [14, 15]. Algorithm designed and applied for determination of the boundary is a dynamic convex hull algorithm that accepts coordinates of points identified from negative selection as input. The algorithm determines the boundary and returns the coordinates

of nodes along the computed boundary. The opportunity identified here is detection of intrusion is not a synchronous event. As individual nodes detect intrusion using negative selection sequentially at different times, we have an opportunity to compute the boundary in increments as well. Additionally, in subsequent iterations of the algorithm every point within a previously computed hull need not be considered as possible candidate boundary nodes. For example in instance 1, if H1 is the set of points identified as the boundary encompassing I1 out of C1 candidate points, in the next iteration when C2 is the set of candidate points we drop I1 and consider C2 along with points from H1 only.

Figure 3 Result graph showing time taken to find the boundary of the area under intrusion.

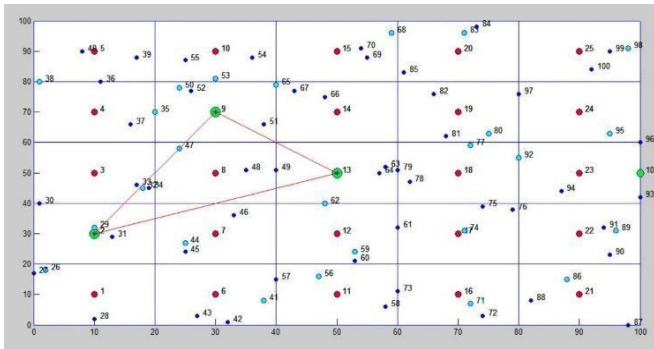


Figure 2. Test bed deployment

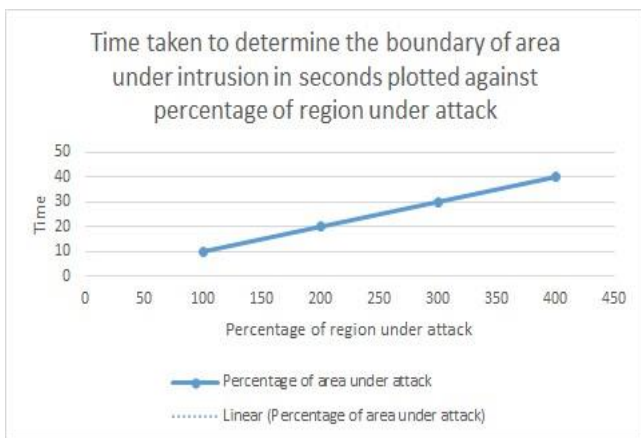


Figure 3. Result graph showing time taken to find the boundary of the area under intrusion

We observe that up to 66% of totally deployed nodes, the time taken for boundary computation is almost negligible. Beyond the 66% mark the time taken increases marginally. In terms of Time taken to compute boundary of area under attack when analysed in terms of percentage of area under attack, we observe that the time taken to compute the boundary is directly proportional to the extent of region under attack.

Figure 4 shows the asymptotic performance comparison of the two algorithms. The blue line on the graph shows the efficiency of the existing work at $N \log H$ and the orange line shows the performance of the proposed algorithm at $h+k \log H$ where h is the number of points identified on the boundary of previous iteration of algorithm and H is the number of points identified after the current iteration. It is well evident that the runtime efficiency of the proposed algorithm is better than the existing algorithm.

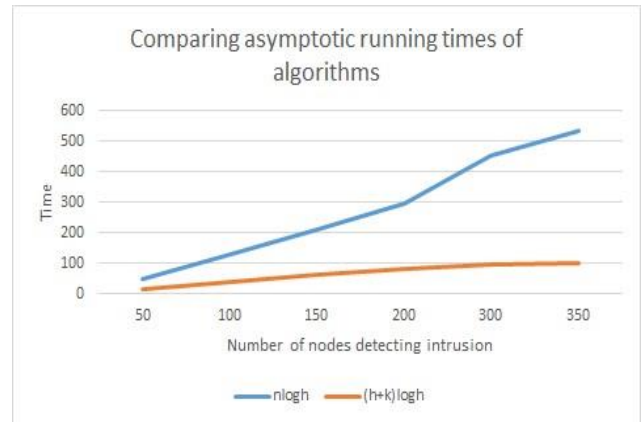


Figure 4. Result graph showing time taken to determine boundary of area under intrusion

5. CONCLUSIONS

In the present work, we have considered incorporation of intelligence within the network to detect attack and intrusion in an area under military surveillance. We have designed a dynamic algorithm to determine the boundary by incrementally reducing the number of candidate points in input as subsequent nodes sense and report intrusion. We have compared the asymptotic running time of the proposed algorithm with the existing algorithm. We have also presented results of the simulation experiments carried out. We plan to incorporate computation of area in the future work.

REFERENCES

- [1] Carrabine, E., Cox, A., Cox, P., Crowhurst, I., Di Ronco, A., Fussey, P., Sergi, A., South, N., Thiel, D., Turton, J. (2020). *Criminology: A Sociological Introduction*. Routledge. 15-30.
- [2] Wickens, C.D., McCarley, J.S. (2019). *Applied Attention Theory*. CRC press. Ch2, pp 12-19.
- [3] Hell, P.M., Varga, P.J. (2019). *Drone systems for factory security and surveillance. Interdisciplinary Description of Complex Systems: INDECS*, 17(3-A): 458-467. <https://doi.org/10.7906/indecs.17.3.4>
- [4] Nazari, E., Biviji, R., Farzin, A.H., Asgari, P., Tabesh, H. (2021). *Advantages and challenges of information fusion technique for big data analysis: Proposed framework. Journal of Biostatistics and Epidemiology*, 7(2): 189-216. <https://doi.org/10.18502/jbe.v7i2.6737>
- [5] Cao, N., Brahma, S., Geng, B., Varshney, P.K. (2019). *Optimal auction design with quantized bids for target tracking via crowdsensing. IEEE Transactions on Computational Social Systems*, 6(5): 847-857. <https://doi.org/10.1109/TCSS.2019.2931476>
- [6] Teixeira, S., Agrizzi, B.A., Pereira Filho, J.G., Rossetto, S., Pereira, I.S.A., Costa, P.D., Branco, A.F., Martinelli, R.R. (2020). *LAURA architecture: Towards a simpler way of building situation-aware and business-aware IoT applications. Journal of Systems and Software*, 161: 110494. <https://doi.org/10.1016/j.jss.2019.110494>
- [7] Flammini, F., Setola, R., Franceschetti, G. (2013). *Effective Surveillance for Homeland Security*. Taylor & Francis Group, New York, pp 5-9.

- [8] Paggi, H., Lara, J.A., Soriano, J. (2020). Structures generated in a multiagent system performing information fusion in peer-to-peer resource-constrained networks. *Neural Computing and Applications*, 32(21): 16367-16385. <https://doi.org/10.1007/s00521-018-3818-1>
- [9] Iqbal, M., Naeem, M., Anpalagan, A., Qadri, N.N., Imran, M. (2016). Multi-objective optimization in sensor networks: Optimization classification, applications and solution approaches. *Computer Networks*, 99: 134-161. <https://doi.org/10.1016/j.comnet.2016.01.015>
- [10] Preece, A. (2019). Sensor assignment to missions: A natural language knowledge-based approach. In *Mission-Oriented Sensor Networks and Systems: Art and Science*, pp. 227-263. https://doi.org/10.1007/978-3-319-91146-5_7
- [11] Singh, S.K., Kumar, P. (2020). A comprehensive survey on trajectory schemes for data collection using mobile elements in WSNs. *Journal of Ambient Intelligence and Humanized Computing*, 11(1): 291-312. <https://doi.org/10.1007/s12652-019-01268-4>
- [12] Raj, S.D., HV, A., HS, D., Babu, R. (2020). Intelligent determination of shortest route for troop movement in military operations by applying ISR in wireless sensor networks. *Institute of Scholars (InSc)*.
- [13] Abhijith, H.V., Rameshbabu, H.S. (2021). Secure data transmission framework for internet of things based on oil spill detection application. *International Journal of Advanced Computer Science and Applications*, 12(5): 189-195. <https://doi.org/10.14569/IJACSA.2021.0120523>
- [14] Abhijith, H.V., Raj, S.D., Babu, H.S. (2018). Intelligent boundary determination of oil spill detection using IOT. In *Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT)*, pp. 26-27. <https://dx.doi.org/10.2139/ssrn.3167315>
- [15] Abhijith, H.V., Raj, S.D., Babu, H.S. (2019). Intelligent method using IOT to determine oil spill spread rate while avoiding data looping. *National Conference on Cognitive Computing (NCCC)*, 2019, Presidency University, Bangalore.
- [16] Asudeh, A., Jagadish, H.V., Stoyanovich, J., Das, G. (2019). Designing fair ranking schemes. In *Proceedings of the 2019 International Conference on Management of Data*, pp. 1259-1276. <https://doi.org/10.1145/3299869.3300079>
- [17] Wang, B., Mei, C., Wang, Y., Zhou, Y., Cheng, M.T., Zheng, C.H., Wang, L., Zhang, J., Chen, P., Xiong, Y. (2019). Imbalance data processing strategy for protein interaction sites prediction. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, 18(3): 985-994. <https://doi.org/10.1109/TCBB.2019.2953908>
- [18] Lynch, C., Devaney, N., Dainty, C. (2019). Locally adaptive super-resolution through spatially variant interpolation. *Applied Optics*, 58(11): 2920-2928.
- [19] Wang, Z., Zhou, X., Xu, C., Gao, F. (2022). Geometrically constrained trajectory optimization for multicopters. *IEEE Transactions on Robotics*. <https://doi.org/10.1109/TRO.2022.3160022>
- [20] Nitesh, K., Azharuddin, M., Jana, P.K. (2018). A novel approach for designing delay efficient path for mobile sink in wireless sensor networks. *Wireless Networks*, 24(7): 2337-2356. <https://doi.org/10.1007/s11276-017-1477-2>
- [21] Deng, B., Genova, K., Yazdani, S., Bouaziz, S., Hinton, G., Tagliasacchi, A. (2020). Cvxnet: Learnable convex decomposition. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 31-44.
- [22] Ferrada, H., Navarro, C.A., Hirschfeld, N. (2020). A filtering technique for fast Convex Hull construction in R2. *Journal of Computational and Applied Mathematics*, 364: 112298. <https://doi.org/10.1016/j.cam.2019.06.014>
- [23] Guo, Z., Liu, C., Zhang, X., Jiao, J., Ji, X., Ye, Q. (2021). Beyond bounding-box: Convex-hull feature adaptation for oriented and densely packed object detection. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 8792-8801.
- [24] Hernández-Landa, R.C., Barrera-Falcon, E., Rioja-Nieto, R. (2020). Size-frequency distribution of coral assemblages in insular shallow reefs of the Mexican Caribbean using underwater photogrammetry. *PeerJ*, 8: e8957.