Identification of Intelligence Requirements of Military Surveillance for a WSN Framework and Design of a Situation Aware Selective Resource Use Algorithm

S. Deepak Raj¹,⁴*, H.S. Ramesh Babu³

¹SVIT, Rajanukunte, Bangalore, Affiliated to VTU, Belagavi 590018, India
²Department of CSE, Presidency University, Bangalore 560064, India
³Department of CSE, Sai Vidya Institute of Technology, Bangalore 560064, India

*Corresponding Author Email: sdrbangalore@gmail.com

https://doi.org/10.18280/ria.360209

Received: 17 February 2022
Accepted: 12 April 2022

Keywords:
WSN, intelligence surveillance, military ISR, sensor management

ABSTRACT

Protecting or safeguarding the place we live in is a basic activity of life. This is also observable in animals. Identifying a suitable place to build a nest or create a cozy home is a primary requirement of carefree living. Once such a place is identified and selected, a lot of effort and planning goes into making it comfortable. From then onwards begins the constant task of safeguarding the place of domicile. Protecting a place involves keeping a constant lookout for disruptive elements, invasion or attacks. The term corresponding to this activity is surveillance. Surveillance when extended to a city, a state, a nation and then to continents will perform the same functionality of enabling protection against attacks but at a larger scale. Unlike in case of a bird, animal or a family unit, such surveillance requires dedicated infrastructure. Usually such a large-scale surveillance infrastructure is designed, implemented and maintained by a dedicated military. Increase in organized crime and acts of terrorism have made military surveillance evermore important and an indispensable requirement of safety. In addition to attacks by men or manmade agents, natural calamities and disasters also require surveillance on an equally large scale. Surveillance which was historically centralized in deployment and investigative in essence needs to change. Existing surveillance and sensor infrastructure can be further used to gather intelligence. Aim of this work is to identify intelligence requirements of military surveillance for a WSN framework. We have designed and implemented an algorithm to compute the area under attack, communicated nearest neighbor nodes to carry out surveillance under attack. The proposed algorithm achieves situation aware selective use of sensor infrastructure.

1. INTRODUCTION

Military surveillance was limited to war time surveillance historically. In recent times, acts of terrorism have made military surveillance most necessary even in peace times. Due to the change in scales of such attacks, surveillance must also evolve to cover larger areas and transform into distributed deployments and be preventive in design of functionality. Formally, surveillance is the means of attaining situation awareness, the end. In order to construct the complete picture of a given situation, surveillance is used as a method to monitor and interpret the behavior of objects within a fixed space [1]. It follows that mere detection of activity is not sufficient. Surveillance must culminate in intelligence. Prevention of a disaster is the best case. If that fails, quick identification and immediate alarm generation with usable intelligence to contain or minimize loss is the next best case. If both are not possible, the system in place must help disaster management, salvage and provide inputs for process improvement. Military surveillance also involves enemy tracking, battle ground surveillance, intelligence, reconnaissance, attack strategy too [2, 3]. This process of intelligence gathering is analogous to understanding a situation while being physically away from the situation and analyzing with limited and local observations made from multiple independent observers.

Addition of intelligence in this context will allow us to deploy optimal networks, assign sensor tasks to necessary nodes and avoid energy loss on redundant data transfers. Need for such data reduction is a very important gap as identified. Irrespective of where intelligence is incorporated, such an effort only adds immense value to an otherwise passive surveillance and reporting framework. Ultimately, incorporation of intelligence in the WSN framework will reduce the extent of human involvement and automate decision making and network component management. Aim of this work is to recognize requirements of intelligence in a WSN framework designed for military surveillance and reconnaissance. Suitability of wireless sensor networks to military surveillance and reconnaissance applications to gather intelligence is clearly depicted in the data compiled in Table 1. In the present paper we propose a situation aware algorithm that identifies nearest neighbor nodes of area under attack and generates selective control commands. The algorithm brings down the total number of redundant use of sensor infrastructure. Thereby adds intelligence to the network. From the simulation experiments we have determined the number of sensor nodes actively sensing the environment with and without the incorporation of our situation aware selective resource use algorithm. Our results demonstrate a considerable reduction of redundant resource use.

In section 2 of this paper, we present an account of work
related to our problem at hand. We present a summary of prevalent problems and results of research. In section 3, open problems and gaps in research are identified while carrying out extensive literature survey. Section 4, deals with emerging research issues where challenges facing military intelligence and surveillance. Section 5 describes the mathematical model developed to exercise the algorithm designed as a simulation. Section 6 presents the implementation results and analysis of findings, followed by conclusion and scope of future work in section 7.

| Table 1. Network characteristics comparing WSN, fixed sensor networks and mobile networks (modelled on Table 1) |
|---------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|
| Deployment | Fixed coordinates as planned or Random, ad hoc | Fixed at planned coordinates | Fixed or Planned |
| Dynamics | Stationary or mobile | Stationary or mobile | Stationary |
| Spatial coverage | Dense coverage | Sparse coverage | Sparse coverage |
| Number | Large | Small | Large |
| Type | Passive as well as active | Passive as well as active | Active only |
| Heterogeneous or homogeneous | Heterogeneous or homogeneous | Heterogeneous or homogeneous | Heterogeneous only |
| Entities under surveillance | Cooperative or non-cooperative | Cooperative or non-cooperative | Always cooperative |
| Type | Dynamic only | Dynamic only | Dynamic only |
| Energy available | Constrained/Unconstrained | Unconstrained | Unconstrained |
| Extent | Distributed or localized | Distributed or localized | Distributed or localized |
| Data processing framework | Distributed or hybrid | Centralized | Hybrid |
| Operating environment | Small | Medium to large | Large |
| Area size | Low to High | Low to High | Low only |
| Threats in area under surveillance/coverage | | | |
| Communication | Bandwidth | Low | High |
| Networking | Wireless | Wired | Wired |

2. RELATED WORK

Singh et al. [4] have made a study of application of WSN to the problem of intrusion detection, classification of targets as well as tracking movements of intruders. They work with over ninety sensor nodes deployed on an experimental basis based on multiple designs. Their work assumes the network made of multimodal resource scarce sensors is unreliable. Sangaiah et al. [5] have also developed a similar application. A demonstration on similar lines is described in Ref. [6]. The application here deals with numerous vehicle tracking. The tracking is based on the framework of a pursuit evasion based game. The game basically has two teams contending to win: called the pursuers and the evaders. An additional element is a sensor network which aids pursuers track or trace their opponents. The sensor network keeps pursuers informed about the relative positions and movements of their enemies. In this way, sensors of the network amplifies the intelligence of pursuer elements and helps find their rivals. Yousefi et al. [7] have developed a vehicle tracking ‘vehicles of interest’. Approach used here is similar to basic immune based classification of own elements and intruder foreign bodies. We have implemented a similar algorithm to differentiate between self and non-self-presence in a military scenario and designed an algorithm. Yousefi et al. [7] have worked to keep track of a specifically identified vehicle using motes carrying audio or video sensors. The work deals with creating a coordinated effort among multiple sensors. Punriboobon et al. [8] have presented arguments in favor of feasibility of military intelligence, surveillance and reconnaissance applications of WSNs in their work. They have identified the following aspects of WSN infrastructure as contributing significantly to cutting surveillance costs: Rotomotion SR20 VTOL UAV helicopter system is identified as suitable for Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR), network extension, and sensor deployment. Crossbow wireless ad-hoc sensor networks are recognized to contribute Infrared (IR) and magnetic-anomaly sensor coverage. Suitable communication protocols identified are, Open-standard internet-protocol router; Cisco voiceover- internet protocol; and wireless, satellite, and land mobile-radio-over-internet Protocol. These are optimal with secure voice and data communication up to 60 MHz. Sensor nodes that are commonly deployed are identified as XACTA deployable wireless-mesh nodes. Other than on-ground deployment, there are definite requirements for aerial surveillance too. Sensor nodes deployed aerially may be performing sensor functions themselves or work as aggregators or cluster heads. Such nodes may be deployed using helium filled balloons. Additionally repeaters or relay antennae may also be deployed on such balloons. Balloons equipped with Mesh Dynamics antennas are selected as suitable to this end. In the matter of communication protocol, IEEE 802.11, 802.16, and 802.20 wireless protocols are identified. A military sensor network deployed for surveillance basically is a WSN. It follows that basic functions of the network must also be taken care of for the application at hand to work. Such functions are also recognized in the quoted work. Aggregation of sensor data from multiple layers of sensors and unmanned aerial vehicle UAVs is a fundamental
requirement. Sensors must sense individually but contribute data to the infrastructure as an aggregation. It is usual to deploy sensors of different energy levels in different physical or logical levels. Such a deployment aids in hierarchical management of data sensed in the bottom up movement of data and in top down movement of control communication. Physical requirement of such a deployment is the use of aerial nodes attached to quick-inflating balloons. Data integration also involves integration of sensor data from various types of sensors, like integration of IR and near-IR sensor data. Military surveillance is extended to monitoring of arms and ammunition. Weapons are also made to carry sensors. Such specialized weapons are called sensor fused weapons. They are made to serve the dual purpose of carrying out attack and sensing storage, use, and effectiveness of weapons. It is identified that ground sensors when deployed as clusters of sensor fused weapons will help data integration too. In summary, network assumes to be constructed out of multiple sensors interacting with each other. Such networks are implemented as physical models as well as simulation exercises in literature. Basic logic involved in surveillance and intrusion detection is similar to gaming implementations. Some intrusion detection implementations do apply immune related algorithms. Sensor data is used in limited scope to determine presence of detection only. Application of intelligence is limited to data fusion and aggregation.

3. OPEN PROBLEMS AND GAPS IN RESEARCH

Open problems and gaps in research are plenty in military ISR. Singh et al. [9] have recognized the determination of whether in addition to what degree, the communication network can contribute to situation awareness among other scope for further research. Though there are convincing arguments on both sides saying WSN was developed due to military surveillance requirements and that WSN was developed first and adopted later to military requirements. The Defense Advanced Research Projects Agency (DARPA) incorporated Sensor Information Technology in 1980. Specifically in terms of tracking capability of WSN, National Science Foundation’s programs have worked and contributed too. Mallick et al. [10] have explored tracking capabilities in their work. Initial frameworks were limited to detection of intruder activity only. Measurements gathered by the sensors deployed would then be relayed across the network. Special notifications would then be generated and communicated in case of detection of intruder movement. From there on, military surveillance has grown beyond mere intruder detection to detection and measurement of chemical, biological as well as nuclear substances. Ahmad Ali et al, in their study on real time applications of WSN have traced applications of WSN in military surveillance beginning with sound surveillance systems of the United States military in the 1960 to recent trends. They have submitted their findings in future internet 2017. It is noted that military surveillance has come to encompass detection and tracking of submarines, airborne vehicles, in addition to soldier or vehicular movement. Further target recognition, tracking and border surveillance [11]. Njoya et al. [12] have developed a dense deployment of WSN aimed specifically at border surveillance. This work focuses on ensuring intruders do not cross over the border under surveillance. Advantages of such a deployment are beyond military surveillance. The same infrastructure will also aid in detecting smugglers of wildlife and exotic plants and trees. Like terrestrial military surveillance, underwater surveillance has also gained substantial limelight in research. We have implemented intelligence incorporating algorithms into underwater surveillance. Alfouzan [13] have investigated underwater WSN too. Though they have focused on improvement of sensor lifetime while not compromising on the bandwidth, they have contributed to sensor surveillance of aquatic life, collision avoidance of submarine vehicles as well. Underwater WSN unlike terrestrial deployments aid in continuous monitoring of ecology. Passive surveillance is important and will always retain its value, however with evolving threats and increase in scale of attacks, surveillance systems must evolve too. Next step in surveillance is smart surveillance. The Ref. [14] reports work dealing with making military surveillance smart and informative. Smart surveillance is a suitable framework to incorporate preventive mechanisms with investigation of the aftermath of an attack. This specific evolution is geared towards integration of intelligence into WSN surveillance to attain situation awareness. Smart surveillance aims at automating the process of sensor data analysis [15]. Formally, this vital step was in the control and hands of human users of the network. Due to the inherent nature of the framework, a delay is expected in generating usable intelligence from the sensor data. By incorporating data analysis techniques within the sensor framework itself, observations are transformed into usable situation aware knowledge or intelligence. In spite of this technology, it will remain to be used in the capacity of a decision support system. Such intelligent situation aware surveillance networks are equally applicable to peacetime monitoring also. Public safety systems deployed in railway stations, airports, places of crowd congregations, and disaster management are candidate applications where such a framework will prove equally if not more valuable. Incorporation of intelligence requires addition of few desirable characteristics into the framework. Military surveillance in war and in peace keeping missions encompasses large areas. Safety, confidentiality and integrity are critical qualities of such applications. It is also an obvious requirement that human involvement, if any, will be from a geographically separated remote location. These requirements demand additional features from the framework. In addition to heterogeneous sensor capability, self-organization capabilities of WSN network, information fusion and collaborative sensor control must also be incorporated. Bunke et al. [16] have studied sensor application in robotics while dealing with details of how sensor data is transformed into spatial estimations of ground layout. The work describes creation of a topological map of a spatial region just using sensor data collected from sensors mounted on robotic devices. Saleh et al. [17] have introduced a sensor network architecture for an information gathering facility. Their work is two pronged, one aiming at querying information from sensor data, the other at performance of sensor tasks using programming scripts. The framework allows basic querying, monitoring and tasking of sensors by implementing a programmable intermediate substrate layer. The work shows how coordination and control of networks can create associations to achieve surveillance or intelligence gathering goals. The framework allows us to even keep a constant track of the sensors, their activities and enforce coordination rules on their activities. Enabling sensor nodes with computational capabilities or inclusion of intelligence in WSN sensors, requires computational capability at the node
level itself. Emerging technologies and advances in sensor hardware have made this quite possible. One such model is studied and reported. They have created and evaluated a directed diffusion paradigm. Computation capability of the sensor is employed to sense and use the data within the network itself. Approach here is data centric, where every node is enlightened about the application it is part of. Nodes are not dumb observers with passive tasks assigned to them, but intelligent and active appendages of the networking infrastructure. Next issue with WSN is the loss of sensors. Sensor loss is a persistent issue irrespective of the size of deployment. Some sensors are lost due to drainage of the onboard battery. Some sensors are physically partially damaged or completely destroyed due to physical factors of the terrain. Especially in military surveillance, sensors are damaged and destroyed more than in civilian deployments. Graceful management of sensor loss while continuing the monitoring activity is a very essential attribute of the WSN framework. Ullah [18], and Singh et al. [19] have come up with an algorithm to add fault tolerance. They have brought in a bottom up approach to detect loss of a node at the lowest level of deployment possible. When lost nodes are detected and accounted for, in sensor management, robustness of observation is enhanced. The graph summarizing global expenditure on military shown in Figure 1 is a clear indication of increase in expenses despite the regional classification recognized by the study. This data is from the Stockholm peace research institute, which has recognized Africa, America and surrounding regions, Asia and the neighbors, Europe and Middle East as the regions and accommodated all nations within the classification. According to the report published on 26th April 2021, the global expenditure stands at $1981 billion by the end of 2020. Military expenses have also been observed to have grown in the first twelve months of the COVID-19 pandemic. What actually shows the focus on military expenditure is the fact that a 2.6% increase in expenditure is recorded in spite of a 4.4% decrease in the global gross domestic product. Gaps identified can be summarized as under:

- use of ground intelligence to manage sensor infrastructure.
- use of situation awareness to selectively enable sensor and communication functions.
- use network infrastructure topology in making situation aware decisions.
- design and apply situation aware, topology aware intelligence algorithms to aid military surveillance and reconnaissance.

According to a technical report cited from the study [21], military expenditure is also focused on emerging smart surveillance systems. Reason attributed to such an increase is the affordability of pervasive system technology. Recognizable domains like consumer, corporate, government, homeland security, and homeland defense have also emerged around the technology. These have also gained research momentum. Military pervasive surveillance is aptly suited to border security, territorial control and crisis management. Especially after recent terrorist acts, defense and security expenditure have increased globally in surveillance, intelligence and pervasiveness [22]. Nature and modus operandi of a terrorist act are almost always random, unpredictable and non-repetitive. Detecting such acts and nipping them in the bud requires an alert framework that is pervasive, ubiquitous and quick to respond or agile. There are studies that have worked with pervasive surveillance in order to add intelligence. Such studies have also extended to civilian environments and commercial hubs of dense human activity [23]. The inferences arrived at by many studies in the domain lead to the effective and efficient management of infrastructure rather than on other means. The gap recognized is to use the infrastructure to generate intelligence, while incorporating intelligence within the framework.

Additionally, well known intelligence approaches are also applicable to problem solving in surveillance applications. Table 3 presents a survey of such approaches. Genetic based algorithms are found to be applicable in surveillance of three dimensional spaces as well as in determination of nearest base station. Analysis of sensor data also finds use of select genetic algorithms. Estimation of cost of sensor deployment and effective coverage evaluation are also implemented using genetic algorithms. Algorithms developed based on greedy and fuzzy logic are also found to be applicable to similar areas of research. Substantial literature as evidenced in the table support this fact. To military specific applications of intrusion detection and target tracking, algorithms based on artificial neural networks and un categorized ground breaking approaches are used [24-30]. Table 4 summarizes and compares intelligence techniques based on problem solving approaches. Techniques implemented, features of the algorithms put in place, study references and their findings are also tabulated. Drawbacks or challenges of each strategy is also identified and presented in the last column of the table.

4. EMERGING RESEARCH ISSUES

Incorporation of intelligence in military surveillance using WSN is a critical area of research. Its importance can never be understated. There is ample scope for intelligent sensor data analysis, intelligent sensor management, design and application of propositional, predicate logic rules and frugal or judicious use of sensor capabilities. Cooperative sensor management, energy aware sensor framework operations and extended surveillance are recent domains gaining attention. As the area under surveillance increases, the framework will be suitable for applications like military ISR, wildlife preservation efforts, forest security against poachers and wildfires [31-45]. Large area surveillance is also applicable to natural disaster management and border surveillance. A common feature of all such applications are huge number of sensor nodes deployed in an unattended environment, distributed operation and huge volumes of sensed data.

Figure 1. Global expenditure in billion us dollars, since 1990 [20]
Challenges in such environments are distributed operation and control, selective perception, management of huge volumes of sensor data, deriving intelligence from data, collaborative decision making and related difficulties. Energy is a great and perpetual concern of WSN frameworks. As the sensor nodes are battery operated, they are prone to power drain related node loss. Minimizing unnecessary sensor activity directly contributes to battery lifetime and thereby improves framework efficacy. Gathering intelligence, obtaining world view or global perspective from sensor data is also a new and emerging challenge faced by WSN framework when applied to a military surveillance scenario [46-53]. Cooperative multi sensor management improves decision making, efficiency and intelligence gathering. Cooperative sensing when fed with intelligence feedback will improve framework performance. Such applications will be most valuable in dynamic environmental conditions. Cooperative multi sensor framework in the form of cue or handoff or both allows the detected information to flow through the network intelligently rather than redundantly. Sensor information is used to refine the operation of sensors in the future [53-55].

Table 2 summarizes literature surveyed in Ref. [56-100].

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom contractors</td>
<td>Dust Inc and others</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large shoebox and above</td>
<td>Pack of cards to small shoebox</td>
<td>Dust particles</td>
<td></td>
</tr>
<tr>
<td>Kilograms</td>
<td>Grams</td>
<td>Negligible</td>
<td></td>
</tr>
<tr>
<td>Vehicle placed or air dropped</td>
<td>Hand placed</td>
<td>Embedded or sprinkled/left behind in case of tactical missions</td>
<td></td>
</tr>
<tr>
<td>Large batteries, hours, days or longer</td>
<td>AA batteries, days to weeks</td>
<td>Solar, perpetual</td>
<td></td>
</tr>
<tr>
<td>Point to point, star</td>
<td>Client-server, peer to peer</td>
<td>peer to peer</td>
<td></td>
</tr>
<tr>
<td>Sensor, processor and communication</td>
<td>Sensor, processor and communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capabilities separated</td>
<td>Capabilities are integrated</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3. Survey and analysis of logical approach to problem solving in surveillance and related applications

<table>
<thead>
<tr>
<th>Logical approach to problem solving</th>
<th>Genetic algorithm</th>
<th>Greedy based approach</th>
<th>Fuzzy logic</th>
<th>Virtual forces</th>
<th>Linear programming</th>
<th>Artificial neural networks</th>
<th>Swarm intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited or fixed area surveillance</td>
<td>Limited or fixed area surveillance</td>
<td>[69]</td>
<td>[70]</td>
<td>[71]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Surveillance in 3D space</td>
<td>Surveillance in 3D space</td>
<td>[57-60]</td>
<td>[61]</td>
<td>[62-64]</td>
<td>[65]</td>
<td>[77]</td>
<td>[78]</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>Intrusion detection</td>
<td>[62-64]</td>
<td>[65]</td>
<td>[77]</td>
<td>[78]</td>
<td>[79, 92-94]</td>
<td></td>
</tr>
<tr>
<td>Target detection and tracking moving targets</td>
<td>Target detection and tracking moving targets</td>
<td>[72]</td>
<td>[73]</td>
<td>[65, 74-76, 80-82]</td>
<td>[91]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification of Base station location</td>
<td>Identification of Base station location</td>
<td>[89, 90]</td>
<td>[89]</td>
<td>[91]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aggregation of sensor data</td>
<td>Aggregation of sensor data</td>
<td>[89]</td>
<td>[89]</td>
<td>[91]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics</td>
<td>Analytics</td>
<td>[83]</td>
<td>[84-86]</td>
<td>[99, 100]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other applications</td>
<td>Other applications</td>
<td>[96, 97]</td>
<td>[98]</td>
<td>[99, 100]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage of area under surveillance / number of manager nodes served</td>
<td>Coverage of area under surveillance / number of manager nodes served</td>
<td>[57-60, 90]</td>
<td>[61, 69, 89, 96]</td>
<td>[62-64, 65, 70]</td>
<td>[66, 68]</td>
<td>[65, 74-76, 80-82]</td>
<td>[78]</td>
</tr>
<tr>
<td>Cost of deployment</td>
<td>Cost of deployment</td>
<td>[58, 59, 90]</td>
<td>[61, 89]</td>
<td>[65, 70]</td>
<td>[77]</td>
<td>[78]</td>
<td>[91]</td>
</tr>
</tbody>
</table>

Table 4. Intelligence techniques categorised based on problem solving approaches

<table>
<thead>
<tr>
<th>Technique</th>
<th>Features</th>
<th>Findings</th>
<th>Drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random probability decision making</td>
<td>Markov decision process, decision outcomes are partly random and to limited extent under decision maker's control</td>
<td>Modelling is in terms of decision making. Provides a Mathematical model to represent decision processes.</td>
<td>Effective when applied in combination with dynamic programming or reinforcement learning.</td>
</tr>
<tr>
<td>Heuristic decision making</td>
<td>Evolutionary algorithms</td>
<td>Learning and discovery</td>
<td>Experience based, attempts to arrive at optimal solutions at optimal times. Based on search heuristics that apply.</td>
</tr>
</tbody>
</table>
5. MODELING

U={(ID,x,y)|ID is unique, min=<x=<max, min=<y=<max }, where min and max are the least and greatest coordinate value within the deployment respectively. It is the universal set of all nodes.

A={(ID,x,y)|ID is unique, min=<x=<max, min=<y=<max }, where min and max are the least and greatest coordinate value within the deployment respectively. It is the set of all nodes that have recorded an attack.

B={(ID,x,y)|ID is unique, min=<x=<max, min=<y=<max }, where min and max are the least and greatest coordinate value within the deployment respectively. It is the set of nodes neighboring elements from the set A. These are selected such that they are enclosing the region occupied by elements of set A.

Graphical representation of the problem’s model is as in Figure 2. Red colored circles are the nodes that have sensed and reported attacks. Region shaded pink is therefore the area under attack. Nodes on the periphery shown as blue circles are the nodes on the boundary. Blue colored lines connecting blue circles form the outer boundary of the area under intrusion or attack. Immediate neighboring nodes on the outside of this blue colored region shown in the figure as green colored circles are the destination nodes identified. Green lines connecting these nodes form the region intended for counter attack action to be initiated. Aim of the algorithm is to determine shortest routes to nodes in this selection. Additionally, computation of area under attack contributes to managing the magnitude of counter action required.

![Figure 2. Layout of military surveillance and reconnaissance deployment showing attack, boundary and shortest paths to points of strategic attack](image)

Input to the algorithm is a connected graph with positive edge costs. Let G be the graph input which is a triplet (V, E, W) where V is the set of vertices, E is the set of pairs of vertices representing directed edges, |V|=n, the number of nodes in the deployment. |E|=m, the number of edges. Wi is an edge cost of an edge belonging to the set E such that Wi=(u,v) where u and v are vertices in the set V. S, a vertex belonging to V is the source and a set T is a set of points Ti on the boundary of the area under attack, the set of destinations. T is a proper subset of V. Weight or cost of a feasible path is the sum of individual weights of edges selected to form the path. Wpath(s,ti) is the weight of the path from source s to a certain destination ti. Wpath(s,ti) = j=1|path(s,ti)|Wj.

Minimum path however is the minimum of all feasible paths from S to Ti. The algorithm we have designed, the shortest route is determined from a source node to the nodes on the boundary of the area under attack. Source is a point of strategic advantage. Instead of treating the problem as a single source multiple destination shortest path problem directly, we identify the nearest destination node out of the set of destinations first. This identified node is assigned as the new source and the rest of the nodes on the boundary are made multiple destinations. Before the algorithm iterates, for every destination node its adjacent nodes are identified and corresponding edge costs are reduced by the minimum of all edge costs. This procedure makes the cost of reaching the destination 0 from the nearest neighbor.

Algorithm: selectivesourceuse (A, U, B, E)

Inputs: U the universal set of all sensor nodes, their location coordinates, A is the set of nodes on the boundary of area under attack, B is the source, E is the set of edges

Output: an array of node IDs selected to continue monitoring

1. Create L1[],L2[],L3[]
2. while(|A|>0)
3. a,d<-0
4. For all v in (A-a) do
5. min<-+∞
6. For all (x,Ai) in E do
7. If w(x,Ai)<min then
8. min<-w(x,Ai)
9. End if
10. End for
11. For all (x,Ai) in E do
12. w(x,Ai)<-w(x,Ai)-min
13. Ak<-Ak union x
14. End for
15. For i<0;i<|A|;i++
16. path[i]<-singlesourcesingledestination(U,B,A)
17. a<-min(path[i])
18. For all v in (A-a)
19. v.d<-+∞
20. v.tag<-0
21. v.pre<-NULL
22. End for
23. area<-0
24. For all v(x,y) in A
25. area<-area+(y1+y2)/2)*(x2-x1)
26. If Ak==a return 0 else
27. Repeat finding shortest route using (Ak, U, a, E)

6. IMPLEMENTATION AND RESULTS

Simulation experiments are performed on Matlab R2021a running on Intel® Core™ i3-6006 CPU @ 2.00GHz 1.99GHz with 4.00 GB RAM. Test bed layout is a grid as shown in Figure 1. Area of the grid is 100X100 units. Each square unit is of 20X20 units and they are identified as unit cells. Each unit cell is under the surveillance of one high power node identified also as the grid head. High power nodes are represented as the red colored circle in Figure 2. The sky blue colored nodes are also high power nodes but not grid heads. The dark blue colored nodes are low power nodes whose responsibility is limited to monitor physical parameters. The screenshot in the figure is showing an output of one of the many simulations. Green colored circles represent the boundary nodes enclosing every node that has detected attack. Figure 3 is showing the nodes on the periphery of the area under attack in green. Shortest path is discovered to reach nodes along this outer boundary connected to a chosen point of strategic advantage. The graph in Figure 4 is showing the marked reduction in the number of nodes employed in monitoring the area under attack. Number of nodes involved in intelligent monitoring is constantly less than the number of nodes employed to monitor the same area without the application of deployment and situation aware intelligence. Figure 5 presents the results of comparison experiments showing the number of active nodes involved in surveillance with and without intelligent node management.

7. CONCLUSION

WSN when applied to large area surveillance evolves into an intelligent pervasive surveillance framework. They are self-organizing, expansive and ever active. Constant surveillance implies huge volume of data, redundant transmissions and unnecessary use of infrastructure in gaining the same data. With increased pervasiveness comes lower efficiency. Challenge is to maintain pervasive surveillance while maintaining efficiency. This dual purpose can be achieved by adding intelligence to the framework. Sensor information must aid in sensor management. Coordination of sensors, optimal use of sensors are possible if logical rules are incorporated in node management. Earlier studies in this domain do not use the sensor data to make framework management decisions. Intelligence gathered is not utilized in selective sensor use. These two are the contributions of the proposed algorithm. Due to the inherent quality of the intelligence added by the proposed algorithm, redundant use of every sensor node in the deployment is avoided. Strategic use of required subset of nodes improve the overall life of the sensor infrastructure. Limitation of our study is that we have not made a study of direct impact of the proposed algorithm on control message communication. Logically reduction of such messages is also an indirect impact of situation aware algorithms. We wish to study that impact in the future.
REFERENCES


Yadav, S.S., Chitra, A., Deepika, C.L. (2015). Reviewing...


Cao, N., Brahma, S., Geng, B., Varshney, P.K. (2019)....


Yadav, S.S., Chitra, A., Deepika, C.L. (2015). Reviewing...


Cao, N., Brahma, S., Geng, B., Varshney, P.K. (2019)....


Yadav, S.S., Chitra, A., Deepika, C.L. (2015). Reviewing...


