Advanced Border Intrusion Ship Detection using Wireless Sensor Networks

Arivazhagan.B, Shyam Sundhar.B
Tech-IV year, Department of ECE,
Manakula Vinayagar Institute of Technology, Puducherry, India
a mail-id: areev16@gmail.com, sundharshyam619@yahoo.com

ABSTRACT - Wireless Sensor Network (WSN) has been emerging in the last decade as a powerful tool for connecting physical and digital world. WSN has been used in many applications such as habitat monitoring, building monitoring, smart grid and pipeline monitoring. In addition, few researchers have been experimenting with WSN in many mission-critical applications such as military applications. In this paper an innovative solution for intrusion detection system in sea is being presented. Intrusion detection on the sea is a critical surveillance problem for harbor protection, border security, and the protection of commercial facilities, such as oil platforms and fisheries. In this paper, we present an innovative solution for ship intrusion detection. Equipped with three axis accelerometer sensors, we deploy an experimental Wireless Sensor Network (WSN) on the sea’s surface to detect ships. Using signal processing techniques and cooperative signal processing, we can detect any passing ships by distinguishing the ship-generated waves from the ocean waves.

Index Terms – Intrusion detection; wireless sensor networks; border protection; target monitoring.

1. INTRODUCTION

The traditional methods of detecting ships entail the use of radars or satellites which are very expensive. Besides the high cost, satellite images are easily affected by cloud cover, and it is difficult to detect small boats or ships on the sea with marine radar due to the noise or clutter generated by the uneven sea surface. Hence we go for new system.

Terrestrial intrusion detection with Wireless Sensor Networks, deploy magnetometers, thermal sensors, and acoustic sensors in monitored areas to detect the presence of intruders. Though such networks may work well on the land, it is challenging to deploy these sensors on the sea surface for ship detection. The main challenge is that when sensors are deployed on the sea surface, they are not static and get tossed by ocean waves.

A v-shaped wake and its resulting waves is generated by a ship passing through the water. In this paper, we proposed a system of ship detection by taking advantage of the characteristics of ship-generated waves.
with WSNs. To detect ships three-axis accelerometer sensors is used with iMote2 on buoys on the sea surface. Using signal processing, we observed that ocean waves and ship-generated waves have different energy spectrums. We designed a three-tier intrusion detection system to detect intruding vessels. In the System, we propose to exploit spatial and temporal correlations of an intrusion to increase detection reliability. To the best of our knowledge, this is the first detailed, systematic experimental study of ship intrusion detection with WSNs.

![Fig 1: Wake waves generated by boat](image)

**II. MEASUREMENT OF WAVES**

When a ship moves across a surface of water, it generates waves which comprise divergent and transverse waves. The old method of measuring ship-generated waves is to measure the pressure fluctuations at some elevation points in the water column, then transform the pressure into wave height. However, this method requires expensive equipment. In addition, it is difficult to deploy the devices underwater. In this paper, we use accelerometers to measure the actual surface movement of ship-generated waves. When the accelerometer is used in an ocean environment, the buoy and the accelerometer undergo a generally oscillatory, sinusoidal-like vertical acceleration due to wave action.

![Fig 2: ship generated wave model](image)

In order to distinguish between ship-generated waves and ocean waves, we use Short Time Fourier Transform to process the measured signals. With 2,048 point sample STFT, we observe that ship-generated waves and normal ocean waves have a different energy spectrum. Its Spectrum has a high, single peak concentration around a characteristic period around 1 Hz. On the contrary, the spectrum of the ocean waves combined with the ship waves.
II. SHIP INTRUSION DETECTION SYSTEM DESIGN:

In this section, we first present the architecture of the distributed intrusion detection system, then discuss the three-tier intrusion system in detail.

3.1. The Architecture of the Intrusion Detection System:

A reliable intrusion detection system may involve node level detection, cluster-level classification, and sink-level classification.
The node-level detection involves sampling the event and extracting features. Once the node detects a target, it is better that only the extracted features are transmitted to the local head node or a sink for further signal processing and classification, due to the energy constraints of the sensor node and the limitations of the communication bandwidth.

Cluster-level classification deals with more complicated tasks, such as Collaborative Signal Processing or regional data fusion. The clusters are formed according to the geographical locations of nodes or the migration of the external “event” after the network deployment. In each cluster, local head node takes charge of the data fusion or other coordination tasks within the cluster.

Sink-level detection involves processing type data sent from local head nodes, and the final decision will be reported to the external used via satellite or other means.

To deploy a real long-term intrusion detection surveillance system, some power management should be used. To avoid the need for expensive periodic battery changes, the nodes may need expensive solar panel or other perpetual-powering solutions. Meanwhile some middleware services should be considered, such as the location of nodes, time synchronization, and routing infrastructure.

3.2. Node-Level Detection:
At node level detection, the task for a single node is to detect a ship waves generated by a nearby passing ship. In order to do that, the individual node periodically samples the event and processes the sampled data to extract features the event and processes the sampled data to extract features for node level detection.
3.3. Cluster-level Detection:
When a ship travels through the sensor networks, the waves generated by the passing ship disturb the sensor areas A1; A2; A3 in sequential manner. These areas have spatial and temporal correlations. By exploiting these correlations, we can improve the reliability of the detection system. In order to monitor the entire deployed area, the temporary clusters are combined with static clusters. The static clusters are formed according to the geographical location of the nodes, and temporary clusters are formed on demand when a node’s alarm is triggered. Since the nodes positions are fixed, they know where their neighbors are located. When a node discovers a ship intrusion, it initiates a temporary cluster, informs its neighboring nodes and automatically becomes the temporary cluster head. If more than one node detects a ship intrusion before it receives detection signals from other nodes, it sends out their average detection energy, thus the node with the higher detection energy becomes the cluster head. If the nodes within the cluster also find the intrusion, they report the findings to the temporary cluster head. If the cluster head has not received any report within a certain period of time, it will cancel the temporary cluster because its positive finding may be a false alarm.

3.4. Sink-level detection:
Processes the data sent from local head nodes and the final decision will be reported to the external user via satellite or other means. Multi target detection monitors several intrusion targets at the same time in different geographical areas over large distances. It increases the reliability of the intrusion detection with reduced false alarms with respect to spatial and temporal correlations of detection. The self-organizing localization algorithm which enhances the sensor nodes to be location-aware is deployed in our proposed system.

IV. PROPOSED SYSTEM
The process of finding accurate location of any sensor node is called as localization. The issue of energy efficiency and efficient data transmission is critical due to limited battery power and limited storage capacity of sensors. Spatial correlation is more doubtful due to higher distance among sensors and long propagation delays. Proposed algorithm Adaptive self-organizing localization algorithm is developed in proposed system. It can able to operate under modes of parameters such as: Temperature: Ranges 23 to 26 degrees centigrade within 33 meters. Distance: Node’s deployment distance D is within 40 meters. The proposed localization technique uses only the distance estimation between the reference Nodes (RN) and Ordinary Nodes (OrN). RNs are able to detect their position by means of GPS to find the accurate location of OrNs. OrNs are those nodes which execute without any centralized control to make randomly deployed WSN to be location-aware. In order to perform collaborative sensing tasks the sensor nodes must estimate
their position by means of a distributed positioning algorithm. Average Error (AE) is calculated to weigh the efficiency of proposed algorithm,

\[
AE = \frac{\sum_{i=1}^{500} \sqrt{(x_i-x^*_i)^2 + (y_i-y^*_i)^2}}{500}
\]  

\[(1)\]

where \((x_i, y_i)\) is a real sensor position and \((x^*_i, y^*_i)\) is estimated localization.

4.1. Network model and node level detection:

An undirected graph \(G (V, E)\) where the set of vertices \(V\) represent the mobile nodes in the network and \(E\) represents set of edges in the graph, which represents the physical or logical links between the mobile nodes. Sensor nodes are placed at a same level. Two nodes that can communicate directly with each other are connected by an edge in the graph. Let \(N\) denote a network of \(m\) mobile nodes, \(N_1, N_2... N_m\) and let \(D\) denote a collection of \(n\) data items \(d_1; d_2; . . . ; d_n\) distributed in the network. For each pair of mobile nodes \(N_i\) and \(N_j\), let \(t_{ij}\) denote the delay of transmitting a data item of unit-size between these two nodes. The experimental system is with 30 nodes deployed in such a way that five nodes in a row and a total of six rows is kept. The node’s deployment distance \(D\) is 25 m. The ship travels along one side of the deployed area with three different speed levels and with each speed the test runs some defined rounds. Node-level detection Sample the event and extract those features. Once the node detects a target the extracted features are transmitted to the local head node or a sink for further signal processing and classification due to the energy constraints of the sensor node and the limitations of the communication bandwidth. Sample the signal value at time \(t\) is \(a_t\), the total number \(r\) of sampling points in time period \(T\) is \(u\).

The average sample value of this period \(T\) and the standard deviation can be computed with threshold as

\[\ldots \ldots(2)\]

\[\ldots \ldots(3)\]

The threshold should reflect those changes. Thus design an environment adaptive threshold by moving the average value and the standard deviation with time. The moving average and the standard deviation is defined as

\[
m_{\Delta T} = \beta_1 \times m_T + m_{\Delta T} \times (1 - \beta_1), \quad \ldots \ldots(4)
\]

\[
d_{\Delta T} = \beta_2 \times d_T + d_{\Delta T} \times (1 - \beta_2), \quad \ldots \ldots(5)
\]
In other words the crossing of the threshold occurs several times within a short period of time. Thus anomaly frequency is defined as

\[ a_f = \frac{N_{dx}}{N_{2x}} \quad \text{Eq(6)} \]

4.2. Cluster-level detection and sink-level detection:

If more than one node detects a ship intrusion before it receives detection signals from other nodes, the nodes contend to become the temporary cluster head. To simplify the process, when the nodes try to set themselves up as cluster heads, they could also send out their average detection energy thus the node with the higher detection energy becomes the cluster head. If the nodes within the cluster also find the intrusion, they report the findings to the temporary cluster head. If the cluster head has not received any report within a certain period of time, it will cancel the temporary cluster because its positive finding may be a false alarm. However if it receives enough positive reports in a timely fashion it will process the received data using the spatial and temporal correlations of the ship waves. We define time correlations in row i. Because the cluster head knows the positions of each node, we arrange all reports according to their position and reporting time. If the number of ordered reports is N,

\[ C_{rt(i)} = \frac{N}{n_i} \quad \text{Eq(7)} \]

The group’s time correlations \( N_i \)

\[ C_{Ne} = \pi C_{rt(i)} \quad \text{Eq(8)} \]

\( C_{Ne} \) describes the cluster’s energy correlation coefficient C measures the spatial and temporal correlations in a cluster and is defined as

\[ C = C_{Ne} \times C_{CNe} \quad \text{Eq(9)} \]

Estimate the speed of the intruding ship using the equation,

\[ V = \frac{D \sin(\alpha - 70^\circ)}{(t_4 - t_2) \sin \theta} \quad \text{Eq(10)} \]

\[ \text{Eq(11)} \]
4.3. Sink-level estimation:
The intruding ship will keep moving it will eventually move away from the monitored area. So it raises false alarm when several clusters are affected and disappears. It process the data sent from local head nodes and the final decision will be reported to the external user via satellite or other means. To distinguish between friend and foe ships add ID to friendly ships. When such ships come, the system will not sound intrusion alarms. Thus it increases the reliability of the intrusion detection with reduced false alarms with respect to spatial and temporal correlations of detection.

4.4. Node Location Estimation:
The proposed localization technique uses only the distance estimation between the reference Nodes (RN) and Ordinary Nodes (OrN). RNs are able to detect their position by means of GPS to find the accurate location of OrNs. OrNs are those nodes which execute without any centralized control to make randomly deployed WSN to be location-aware. In order to perform collaborative sensing tasks the sensor nodes must estimate their position by means of a distributed positioning algorithm. Average Error (AE) is calculated to weigh the efficiency of proposed algorithm using the formula 1.

V. ANALYSIS OF PROPOSED SYSTEM
In order to improve energy consumption in efficient way, localization algorithm is proposed. It analyses inconsistency caused due to erroneous depth which is calculated using pressure sensors and find the average error in calculated node location. It autonomously performs the assigned task without human intervention.
The block diagram describes the overall methodology of the proposed system,
The block diagram shown in the above fig: 8 describe the working methodology of the proposed system. Using the three-tier accelerometer sensor to detect the intrusion ship. We introduced four detection algorithms namely node level, cluster level, sink level and node location detection to detect the intrusion ship more efficiently and accurately. The following graphs in fig:3 and fig:4 shows the ship speed estimation and success detection in accordance with the intruder ship. The fig:3 shows that minimum, maximum and the average speed that the ship could attain, any ship that exceeds the ratio calculated is considered to be an intruder ship.

VI. IMPLEMENTATION

NS-2 is an open-source simulation tool running on Unix-like operating systems. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired, wire less and satellite networks. It has many advantages that make it a useful tool, such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS-2 supports several algorithms in routing and queuing. LAN routing and broadcasts are part of routing algorithms. Queuing algorithm includes fair queuing, deficit round robin and FIFO. NS-2 started as a variant of the REAL network simulator. REAL is a network simulator originally intended for studying the dynamic behaviour of flow and congestion control schemes in packet-switched data networks.
In 1995 ns development was supported by Defence Advanced Research Projects Agency DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. The wireless code from UCB Daedelus and CMU Monarch projects and Sun Microsystems has added the wireless capabilities to ns-2. NS-2 is available on several platforms such as FreeBSD, Linux, SunOS and Solaris. NS-2 also builds and runs under Windows with Cygwin. Simple scenarios should run on any reasonable machine; however, very large scenarios benefit from large amounts of memory and fast CPU’s.

VII. CONCLUSION
The developed architecture enables the system to conduct efficient information processing including detection and classification in a large-scale WSN. This architecture naturally distributes sensing and computation tasks at different levels of the system so that the sensor network can support high-quality sensing and reliable classification without involving special high-power nodes. With evaluation data collected from field tests in physical environments, the evaluation demonstrates excellent performance on the detection rate, classification result, attribute (velocity) computation accuracy and timely information delivery. The developed approach is further extended in future in many ways. Propagation of ship waves over large distances is not concentrated in existing system. Real sensor network system drop buoys from a plane rather than grid environment have to be analysed.

The main limitation of our schemes is that it requires a relatively dense network, especially to detect a high detection ratio with small boats because of the high noise on the sea.

Power management in sink level detection is another methodology to improve the performance of the detection system in efficient way. On the other hand seek solution for supporting online intrusion detection system.

REFERENCES


