Target Tracking in Marine Wireless Sensor Networks

Ahmed M. Mahdy and Jonathan M. Groenke
Department of Computing Sciences
Texas A&M University-Corpus Christi
Corpus Christi, TX USA
ahmed.mahdy@tamucc.edu and jgroenke@islander.tamucc.edu

Abstract— **It is evident that wireless sensor networking has a secure place in the future of communication systems. The potential and promise of such networks cannot be underestimated. A major advantage is the wide array of configurations and working environments that allow a wealth of applications. In the last few years, research on marine wireless sensor networks has been growing steadily. Nonetheless, there is an immediate need for further investigation into basic and applied research. In this paper, major challenges and applications are discussed. A perspective on target tracking in marine wireless sensor networks is thoroughly presented. In addition, the basic concept for underwater tracking algorithms is presented. From inhabitant monitoring to homeland security, the underwater environment is a major user of target tracking. The military field has greatly benefited from terrestrial wireless sensor networks. We strongly believe that the case with marine wireless sensor networks is no different. This paper discusses how underwater target tracking may enhance digital battlefields of the future. We also present a two-layer broadband wireless infrastructure for marine/terrestrial sensor networks with military and homeland security applications. The development of such infrastructure enhances the survivability of ad hoc networks, widens the domain of applicability, and emphasizes the role of marine wireless sensor networks in future battlefields.**

Keywords-marine wireless sensor networks; underwater communication; target tracking; digital battlefields

I. INTRODUCTION

Modern communication systems have been enjoying the unique capabilities of the wireless technology for the last few decades. Wireless systems have introduced new possibilities and opened the door for novel technologies that made wireless communications a first choice to a wide range of applications in a variety of domains. The versatility and flexibility of the wireless technology have enabled the design of revolutionary systems including satellite, cellular, and ad hoc networks through the years.

The communications discipline has substantially progressed over the last century. From the early telegraphs and telephony, to mobile systems, and to recent optical wireless systems, the field has witnessed numerous advances on all levels. Nonetheless, wireless communications represent a major factor in the way communications have evolved. The use of wireless transmission added new dimensions to the human perception of communications especially with the evolution of cellular and satellite systems. Cellular systems are infrastructure based networks divided into a group of contagious cells. Every cell is serviced by an access point (i.e. base station) that controls data traffic. Ideally, a cell is circular with a radius equal to the transmission range of a centered base station. However, hexagonal cells make the actual case. The ability to communicate on the move has enabled tremendous applications and fuelled related research especially within the areas of network protocols and data multiplexing. Satellite systems with their line of sight communications have triggered extensive research leading to novel transceiver designs. The application of satellite systems affects our daily life whether it is a TV broadcast, weather forecast, or a Global Positioning System (GPS) satellite. The impact of wireless systems on all aspects of our modern life is clear.

Among the many flavors of wireless systems, ad hoc and sensor networks represent a remarkable and unique kind of wireless communications. An ad hoc network is a multihop wireless system; an autonomous system that is composed of wireless nodes communicating in a peer to peer fashion where every node serves as a host and router at the same time [2][3]. A node may be mobile or stationary. Nodes exchange information packets that usually travel in a store and forward manner. A wireless sensor network is a collection of tiny sensor devices with wireless capabilities. A sensor device includes sensing, processing, communication, and battery modules. A sensor node can locally process data and communicate with other nodes to form a network of tiny sensors. The placement of such nodes usually follow a random approach, which eases the setup process and facilitates the deployment of sensor networks in temporary locations such as disaster relief areas. Nevertheless, this complicates the design process of sensor networks' algorithms and protocols, which have to be self-organized.

Despite the fact that wireless sensor networks have a wide range of applications that have ensured a secure place in the future for this technology, research and development of underwater wireless sensor networks have been minimal [4]. Basic and applied research on the development of this unique kind of wireless sensor networks is greatly needed. In this paper, we present major challenges and applications focusing on the role of marine wireless sensor networks in future digital battlefields. The rest of this paper is organized as follows. In Section II, major research challenges are presented. In Section III, a discussion on target tracking in marine wireless sensor networks is presented. Sections IV and V emphasize the use of these networks in military applications. The paper is concluded in Section VI.

II. MARINE WIRELESS SENSOR NETWORKS

The current protocols and design specifications of terrestrial wireless sensor networks cannot accommodate the requirements of the marine environment [5]. This makes the deployment of current wireless sensor networks in a marine environment challenging [6]. New techniques and algorithms are needed to achieve this goal. The following presents major design issues that need immediate attention.

A. *Types of Sensors*

Sensor nodes are the building components of wireless sensor networks. A sensor node is a tiny device that has the ability to sense, process, and communicate data. These nodes are usually deployed in harsh environments such as battlefields and disaster relief areas. Therefore, the manufacturing of sensor nodes handles this problem by providing reliable sensors that can stand unfriendly conditions. Nonetheless, most of these sensors cannot survive marine environments. Water can have severe impact on the operation of sensors. The effect of water on sensor devices and the different characteristics of waterproof sensors need to be closely studied. In addition, we believe that the marine environment opens the door for the introduction of new capabilities of the sensor devices.

Many applications of marine sensor networks will require sensors to monitor the underwater conditions. This necessitates the need for sensor nodes that can either reside under the water surface permanently or temporarily. Accordingly, new features of sensor devices will be introduced, which may lead to a redesign of existing sensor nodes. A typical marine sensor network will be composed of floating and diving sensor nodes. The former will be nodes that can float on the water surface and collect relevant data such as surface temperature, wave frequency…etc. On the other hand, diving sensors are those nodes residing under the surface of the water collecting data like pressure, depth, visual imaging…etc. It is imperative to understand the different factors that affect the operation of such nodes. Each type has its own and unique characteristics that should be reflected on the design of these sensors. A careful study on these factors should be conducted and a comparative analysis of the different characteristics should be carried out.

B. *Network Architecture*

Ad hoc networks can be classified according to the existence of an infrastructure support. In fact, ad hoc networks do not necessarily require an infrastructure, which leads to two major classes; infrastructureless and infrastructured ad hoc networks. Infrastructureless ad hoc networks are pure decentralized systems where all participating nodes equally share network management responsibilities. This organization has been known for its simplicity and has dominated the design of ad hoc networks. Yet, its performance has never been to the expectations due to the inefficiency of such decentralized systems [7][8][9][10]. This triggered the development of more efficient infrastructured organizations, centralizing some functionalities of the network, has been inspired by the classic base station cellular scheme. The hierarchical clusterhead model has proved to be the best practical solution for infrastructured ad hoc networks. The network is virtually divided into clusters managed by designated nodes called clusterheads. Despite the fact that many clustering techniques have been proposed for the clusterhead based scheme, the selection of clusterheads has been mostly based on a single quality measure. This severely limits the efficiency of the selection process and can degrade the network performance. For example, consider a connectivity based selection that assigns the node with the highest connectivity degree to be the clusterhead. In this case, a highly connected node with low energy level can be selected as a clusterhead. Such a node, with the extra load a clusterhead is exposed to, may become out of energy in a short period of time triggering a new selection round, which increases the overhead and affects the stability of the network. We believe that clusterhead selection should not be based on only one measure but rather a set of quality measures. Moreover, the selection criterion should be scalable in order to accommodate new measures and/or disable existing measures. The effect of the clustering techniques on the network performance is commonly evaluated in terms of network stability and fairness (i.e. load balance). Network stability is adversely proportional to the number of clusterhead replacement; the less the number of selected clusterheads is, the more stable the network is. On the other hand, an ideally fair clustering technique uniformly distributes the management load over the network nodes. The more the number of nodes involved in the management of the network is, the fairer the technique is. Clearly, there is a tradeoff between network stability and fairness. One of the two merits is sacrificed on the account of the other in many cases for the sake of simpler designs. This can significantly deteriorate the network performance. Therefore, the clustering technique should be able to strike a tradeoff between stability and fairness in order to achieve better overall performance. We believe that clustering techniques should be adaptable and can be easily configured to seek specific network merits. To illustrate, the same technique can be configured for maximum stability, maximum fairness, or optimized overall performance.

C. *Network Protocols*

The impact of the marine environment on the operation of sensor networks cannot be underestimated. Basic communication protocols and techniques will need to be redesigned to reflect the new requirements of such an environment [11][12]. For example, existing routing algorithms cannot serve marine sensor networks in their current format [13][14]. A distinction between the floating part of the network and its diving counterpart will be essential for a proper operation of the network. Therefore, the algorithm should reflect the associated cost with every communication link by providing a relative weighing factor distinguishing all-surface, surface-underwater, and all-underwater links' costs.

It may be necessary for a wireless sensor network to update its topology to alleviate the effect of recent changes to the environment that degrade or even halt the operation of the system. In such cases, the network seeks the best possible topology that can furnish an optimized performance given the current conditions. A best possible topology for conventional sensor networks may not be the same for a marine sensor network due to the heterogeneity of communication links and the impact of water on signal transmission. This raises the need for new algorithms that can handle the topology reconfigurability in the water. The network efficiency highly depends on the performance of clusterheads. A clusterhead failure might result in a cluster failure triggering the isolation of its nodes. Accordingly, clusterheads must be qualified enough and adequately selected to claim such responsibility. Ideally, the outcome of the selection process should improve the performance of the cluster as well as the whole network. Currently available selection algorithms need to be revisited to reflect the changes in the environment and the characteristics of the sensor devices. The selection of a diving sensor as a clusterhead may not be appropriate in a network dominated by floating nodes.

A vital aspect of sensor networks is the energy consumption due to the size and working lifetime of sensing nodes. Therefore, low-energy protocols are essential for the operation of marine sensor networks. New internetworking schemes are also needed to allow better communication between sensor networks and other non sensor networks. In addition, error control protocols for mobile sensor networks are highly appreciated. Dedicated coding schemes to improve communication quality between nodes are needed.

Another major issue is network security. The rapid growth rate of communication networks and the open nature of nowadays information resources have turned network security into a mandatory requirement for communication systems. Military, business, and personal information are major types of data exchange across networks. Such information is mostly intended to designated recipients. Vulnerability of such networks imposes a major design challenge for secure data transmission. With this concern in mind, security is on the top of design priorities in current networks especially wireless sensor networks. Several security measures are required including authorization and authentication. Relevant research has shown that secure protocols for the recently developed communication technologies, especially those involving mobility, are easily recognizable. Routing algorithms with security guarantee are needed. Related research focuses on the different types of attacks to help measure the vulnerability of a network. In this context, detection of anomaly in communication behaviors can help prevent possible attacks. More attention to this issue should be given. All of these areas are widely open for research especially for the unique marine environment. Further discussion can be found in [15]. In this paper, we focus on target tracking algorithms due to the wide range of applications that may benefit from such capabilities.

III. A PERSPECTIVE ON TARGET TRACKING USING MARINE WIRELESS SENSOR NETWORKS

Target tracking is a skill currently used by individuals in occupations such as wildlife management to locate and track various animals, and military organization to detect and track the enemy on a battlefield. For example, in wildlife management, there are many cases where a specific animal needs to be located or tracked for various studies. Depending on the environment it may be very difficult for any person or group to deploy in order to locate a specific animal and gather required information. This is especially true if the animal's habit is not well suited for humans. For example, if marine biologists are trying to track and record what specific species of fish eat in a certain area of the ocean, it might be more prudent to deploy relatively low cost sensor nodes to record data in the area of interest instead of deploying a team of scientists to collect the same data. Deploying sensor nodes can be less dangerous and more cost effective than having a group of people live on a boat in the middle of the ocean for some indeterminate amount of time. This also holds true for other inhospitable environments such as a desert or tropical jungle. Military applications of WSN for target tracking may be more apparent. On the battlefield there are numerous scenarios where sensor nodes would be preferred over human deployment. For instance, if some military leader needs to know when or if the enemy is transiting some specific area of interest then it is much safer to deploy a network of sensors instead of sending a team of soldiers.

Issues to be considered with mobile target tracking include types of nodes, node distribution, initial target detection, target localization, target classification, and sustained target tracking. Node type discusses basic types of sensor nodes and how they can be configured. Node distribution covers how nodes are to be distributed given specific target characteristics. Target detection discusses how the network detects a target. Localization deals with the transition from target detection to sustained target tracking. Classification and sustained tracking cover how the network classifies the target and tracks its movement.

One of the first items to consider prior to determining the type of sensor node to use is the target's characteristics. Knowing the characteristics is essential to identify what target traits can be exploited. In order to better illustrate this point, consider an example of a marine biologist who needs to locate a specific species of whale off the coast of Alaska. The biologist wants to locate as many of the whales as possible so it can tag and track them for further study. The biologist knows the general area where the whale lives but the area covers hundreds of square miles and he does not have the manpower to effectively cover the territory. The biologist wishes to utilize sensor networks that will be deployed in strategic areas and notify him when a whale is located.

There must be some classifying trait that emanates from the whale such as sound. If the biologist heard this particular noise he could immediately identify the sound as a characteristic of the target whale and classify the target as the whale of interest. We can now use this identifying characteristic to choose or configure a specific sensor. In this example, the sensor must be able to detect sound in a particular frequency range with the use of a hydrophone. Sensors can be configured to sense one or many frequencies in the spectrum and they are not limited to sound.

Sensors can be categorized as passive or active. Passive sensors are more suitable for target tracking since they do not disrupt the environment in which they are placed and they do not alert the target to anything unnatural. These passive sensors can be a) omnidirectional which simply detects a signal within a particular range from any three dimensional directions, or b) directional which means they can provide a relative bearing to the signal of interest. Active sensors do not rely on the target to emit light, sound, or electromagnetic energy. Instead the active sensor transmits some form of energy and detects any alteration of that energy caused by the target. For example, an underwater sensor can produce sound and sense any echo that bounces off an object in the water. The advantage of using this type of sensors over a passive sensor is the higher probability of accurate tracking data. In some cases, this active signal will illuminate the target more than the targets natural emissions. However, the disadvantage is the target will be alerted to the tracking devices and it may alter its course away from the sensor field. Also, the energy needed to produce an active signal will deplete the battery life much faster than that of a passive sensor.

Sensors can detect many different phenomena and it is paramount the right sensor is used when trying to locate a target. Using the correct type of sensor is the foundation for the rest of the network. The sensor must be able to detect the exploitable characteristics of the target or the entire system may fail.

Prior to searching, the sensor's storage device will have to be preloaded with the relevant target information. In order for the sensor to detect the target, each sensor will have to discern between the target of interest and any other frequency it may detect. When a node is first deployed one of the first tasks the node must execute is an ambient noise reading. Ambient noise is background noise which is always present and the sensor will use this reading as a baseline for all other signals received. Having the ability to compare a received signal with ambient levels and prerecorded target data is an important feature. The end user is only interested in target information and he/she is not concerned with all received signals. Therefore, we do not want every sensor node to pass everything it detects to the base station or end user. This will expend much of the network's power by transmitting data that could be of no use. If each node can determine if the frequency received matches that of the desired target then each node will only pass relevant data. This will allow for efficient message passing which helps maximize quality of service and increase energy efficiency.

The sensor node distribution is important because sensors must be placed in such a manner that the network will have the highest probability of target detection. One factor to consider when designing a distribution pattern is the detection range of the sensor. This will require some prior research of the target to determine a source level for each detectable characteristic. If the user wishes to exploit a specific frequency then he will need to know the average distance from the source that the frequency will be detectable. For example, if the sensor uses a hydrophone to detect a target then the source of the sound must be close enough to the sensor for the sensor to detect the sound. Using our whale scenario, an average range of the emanated sound from the whale must be predetermined in order to know how far apart we want to place our sensors. For example, if we want to use the song of the whale as a target identifier. We will assume the biologist has done some research and knows the average distance from which a whale's song can be heard is 5 kilometers direct path. Therefore, for a high probability of detection the sensor must be within 5 kilometers of the whale to detect the song. This means the distance between any two nodes should be no greater than 10 kilometers to ensure no holes exist inside the network. Nodes can be positioned closer together to increase probability of detection but then area covered will be reduced. Conversely, the nodes can be positioned farther apart to cover more area but then probability of detection will decrease. Node placement all depends on probability of detection and the desired area coverage.

Once the detection range is resolved it must be compared to the effective communication range between sensor nodes. If the sensor nodes are too far apart to communicate then spacing will have to shrink. A cost analysis will have to determine the best course of action. One solution would be

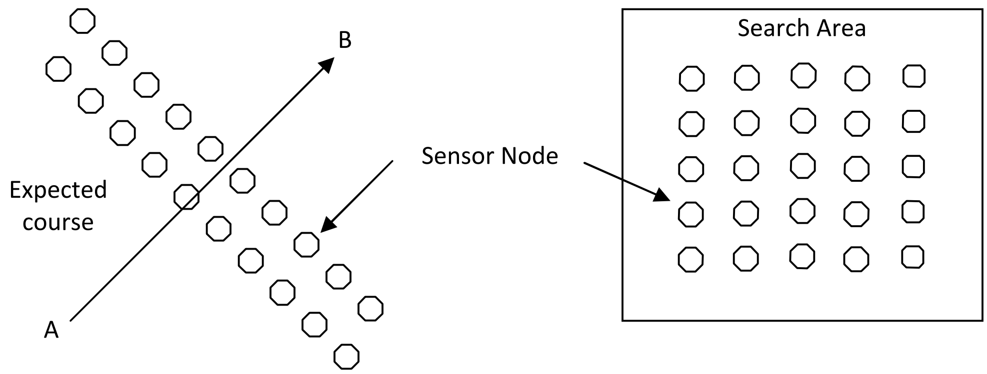

Figure 1. An Example of a Network Distribution Pattern; 2x10 and 5x5 patterns

to use sensor nodes with larger batteries and powerful transmitters but this raises the price of each node. If the nodes are placed closer together then the target may be alerted and it may alter its natural course or speed of advance. This is a case where an Autonomous Underwater Vehicle (AUV) [16] would be a good option to cover the voids within the network grid.

After the node spacing is decided, it is necessary to determine the overall physical shape of the distributed sensor node network. This shape, of course, depends on the target. If the target is going to transit from some point ‘A’ direct to another point ‘B’ then an elongated pattern configured perpendicular to the line from ‘A’ to ‘B’ would be favored; shown in Figure 1.a. A good example would be a 2 by 10 pattern with 10 kilometer spacing between nodes and the center node positioned on the expected route of travel. A top down view of the nodes would look like a 100 kilometer long pattern. This will provide a good probability of detecting our transiting whale. If we determine that our target is not transiting and is, instead, feeding or mating in a certain area then our pattern will have to adapt. The shape of the distribution pattern should match the search area while maintaining our predetermine node spacing as shown in Figure 1.b. A typical example would be n nodes laid out in a √n by √n pattern.

Since the sensor nodes are placed in specific locations relative to each other it is easier to manage the topology of the network. Topology control is an important issue that determines which nodes are allowed to, or able to, communicate with surrounding nodes. When there is a predetermined plan where each node will be placed then it is easier to control and maintain the topology. Depending on the network structure and the nodes task designation the node will become self aware of its relative position when the node is alive. If we are using a flat network structure were all nodes play the same role then each node will find its location in the network by finding its neighbors and the topology control protocol will establish links. If it is a hierarchical network structure then, after each node discovers it relative position within the network, the topology protocol will establish master nodes or clusterheads. These superior nodes are either chosen through some election protocol or they are preselected because they possess some characteristics the surrounding nodes do not. The nodes will self organize in their respective clusters and communicate with the clusterhead/master node. Homogeneous nodes may alternate roles between slave and master status depending on the network protocol [17].

When the search area is large, the nodes will most likely be deployed from a moving airplane, boat, or truck so node placement is estimated and not exact. This differs from random node distribution where nodes are deployed in some arbitrary pattern leading to unpredictable node density. This type of deployment is faster but the topology control is more difficult to establish and maintain. The nodes will still form a predetermined flat or hierarchical network but the initial establishment of communication links will take more processing power. When nodes are distributed randomly, there is no way to determine if every node will be connected to the network. The possibility of multiple networks within the entire set of nodes is possible. On the other hand, if nodes are placed in a prearranged manner then this possibility is greatly reduced.

Routing techniques are vital for such systems because the information must go from the sensor to some clusterhead or base station when the target is detected. In the case of the clusterhead, it must receive all relevant information from the sensor nodes in order to locate, track, and classify the target. The information must transfer from node to node with minimal latency. The routing technique mentioned in [17] discusses virtual grid architecture routing.

The network is constructed in "clusters that are fixed, equal, adjacent, and no overlapping with symmetrical shapes." Each cluster has a clusterhead that performs data aggregation at a local level (i.e. within the cluster) while a subset of clusterheads perform data aggregation at a global level. The clusterheads are responsible for tracking targets moving throughout their respective clusters. The data is routed from the sensors to the clusterhead. In [18], a different approach with location-aware routing and processing is discussed. In this case, the nodes are self organized in cells upon the occurrence of an event of interest. The event in this case is target detection. When a target is detected, the nodes detecting the target are organized in a cell and elect a manager node which creates new cells. As the target moves through the sensor field, the nodes route data to the current manager node which processes the data to track the target. There are numerous routing techniques that can be used. The application takes a toll on determining which technique to use.

Once the network is configured, deployed, and activated the network works autonomously to detect the target. Target detection begins when one or more of the sensor nodes detect a frequency that matches a target frequency in its database. If the target is moving, which is likely the case; the detected frequency may not be the exact frequency in the data base due to the Doppler effect. The node will have to process this information in order to determine a probability or confidence level that the frequency is the target of interest. If the node determines that the frequency does belong to the target then it will pass this information to the manager node (or clusterhead). The manager node will process this information and match it with any other event data received. If the manager node has not received any messages from other nodes it might send a request message or alert message to other nodes in the vicinity of the sensor which received the target frequency. Once other nodes detect the target and pass the respective information to the manager node, the manager node will attempt to localize the target and determine an estimated course and speed of the target. The manager node will send a message to other manager nodes in the direction of the target. These other manager nodes can put their respective clusters on alert if they have been asleep to conserve energy. One of the manager nodes will have to eventually collect enough data points to positively classify the target as the target of interest and then send a message to the base station which will alert the end user.

A. Target Tracking Algorithms

Following the aforementioned discussion, developing a tracking algorithm for such underwater applications is greatly based on the classical Doppler equation:

$$f_o = \frac{(c + v_o)}{(c + v_s)} f_s \qquad (1)$$

Where: f_o= the frequency observed by the listener. f_S = the frequency emitted by the source. c = the speed of the wave through the medium. v_o = the velocity of the listener through the medium. v_S = the velocity of the source through the medium

The basic algorithm concept is for a given sensor to detect an acoustic frequency f_o of a target source f_S and calculate the velocity of the target v_s. If the observed frequency is higher than that of the source frequency then the target is moving toward the sensor. Conversely, if the observed frequency is less than that of the source frequency then the target is moving away from the sensor. The location of the target is automatically known to be in the vicinity of the sensor due to the fact that the sensor detected the target. The direction of the target can be approximated if other sensor nodes detect the same target. It should be noted that this Doppler equation is only accurate when the source is moving directly to or from the listener. However, the level of inaccuracy for targets that do not move directly to or from a sensor is acceptable considering the large coverage areas in an ocean environment. It is also assumed that the acoustical path from the source to the sensor is a direct path.

For this concept to work properly, the node placement and the acoustical characteristics of the target must be predetermined. Sensor nodes must be spaced at a distance so that only one or two sensors can detect the target at any one point in time. As previously discussed, in order to ensure appropriate sensor spacing, we must take into account the predicted range or our target. Assuming the target is in the vicinity of our sensor network, if the detection range of our target is smaller than expected then, at most, only one sensor will detect the target at a given point in time. If the detection range is larger than expected then no fewer than two sensor nodes will detect the target at any given point in time. The tracking algorithm can still work in these two cases but it will require more processing and more intra-network communication which will result in more power consumption. For the purpose of this research, the assumption is made that the predicted detection ranges of the target are accurate and spacing between any two sensors is twice that of the predicted range. Once the sensor spacing has been determined the next step is to construct a sensor pattern. We believe that a honeycomb pattern, illustrated in Figure 2, fits the majority of underwater tracking applications.

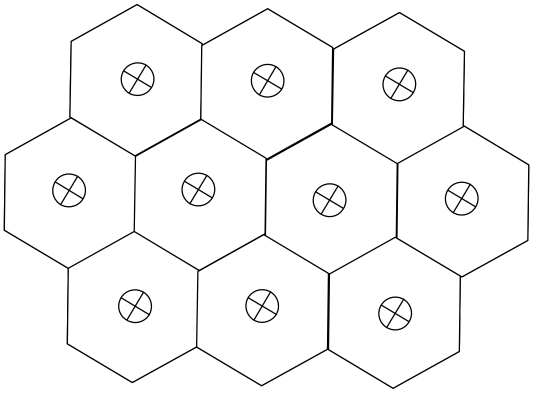

Figure 2. A Honeycomb Pattern

This orientation will provide minimal overlap in sensor coverage and negate any coverage gaps. Each hexagon is divided into six sections with the sensor node positioned at the center and each of the six sections is given a number and relative bearing as shown in Figure 3. Neighboring nodes are predetermined and programmed into each sensor. Furthermore, each sensor node is aware of its neighbors' relative location. This configuration will aid in allowing the sensor nodes to pass relative positions of the target. When a sensor detects a target the only immediate conclusion that can be made is that the target is within the detection radius of a sphere surrounding the sensor. Using the Doppler equation and the stored source frequency the sensor can determine an approximate velocity.

The stored source frequency is loaded into the sensor and based on historical target observations. Multiple source frequencies can be loaded in the sensor for the same target. Using a threshold for acceptable velocities, the sensor can ignore observed frequencies if they do not match target characteristics. For example, suppose a sensor observes a frequency of 80 Hz and has two stored frequencies of 30 Hz and 150Hz.

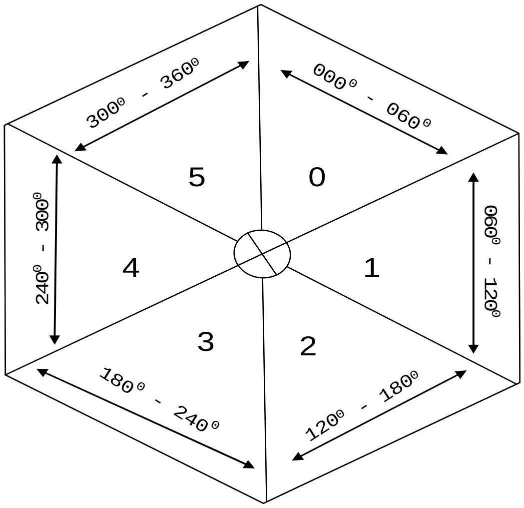

Figure 3. A Honeycomb Cell

The stored frequencies are used as frequency emitted by the source in the Doppler equation. The stored historical target data gives an acceptable velocity of two to seven knots. Computing the velocity of the observed frequency would yield 1820 knots and 2548 knots respectively. This observed frequency would be discarded by the sensor. If the sensor observed a frequency of 149.8Hz then the computed velocity would be 2329 knots and 4 knots respectively. This observed frequency would be accepted and the sensor would continue to monitor this frequency.

In the following, we present a tracking algorithm that can be used in marine wireless sensor networks (i.e. Figure 4 and Figure 5):

1) Sensor receives frequency and compares it with preset frequencies in its tiny database through the use of the Doppler equation.
2) If velocity is out of predetermined tolerance then discard. Otherwise, send 'contact' message to neighboring nodes.
3) Receive 'contact' replies from neighbors. If no positive contact replies from neighbors then send contact report with time stamp to clusterhead. Wait for another signal and/or continue monitoring frequency
4) If positive contact from a neighbor is received, then match neighbor's ID with sector and determine approximate relative direction. Send contact report with time stamp to clusterhead.
5) If a contact message is received by neighbor and no received frequencies match target data, reply to neighbors with 'no contact' message. If monitoring a frequency that matches target data then reply to neighbor with 'contact' message and then calculate approximate direction of target.

With respect to communication between nodes, all stationary nodes will be connected in a 2-D mesh with no wrap around. That is, each node will only be able to communicate with its immediate neighbor north, south, east, and west. When the sensor nodes are given their respective grid coordinates, they are also given the coordinates and identification of their immediate neighbors. The AUV will be able to communicate only with its closest neighbor. To find its closest neighbor, the AUV will have to broadcast its position and wait for a return message from the closest stationary sensor node. Different algorithms may be developed based on the concepts discussed in this Section.

IV. APPLICATIONS OF MARINE WIRELESS SENSOR NETWORKS WITH TARGET TRACKING

Marine wireless sensor networks offer an unmatched option to a wide range of different domains. The significance of the aforementioned research lies in the fact that it opens the door for a variety of applications as well as new areas of relevant research in wireless networks. In the following, we present candidate areas that highly benefit from a marine wireless network with target tracking capabilities.

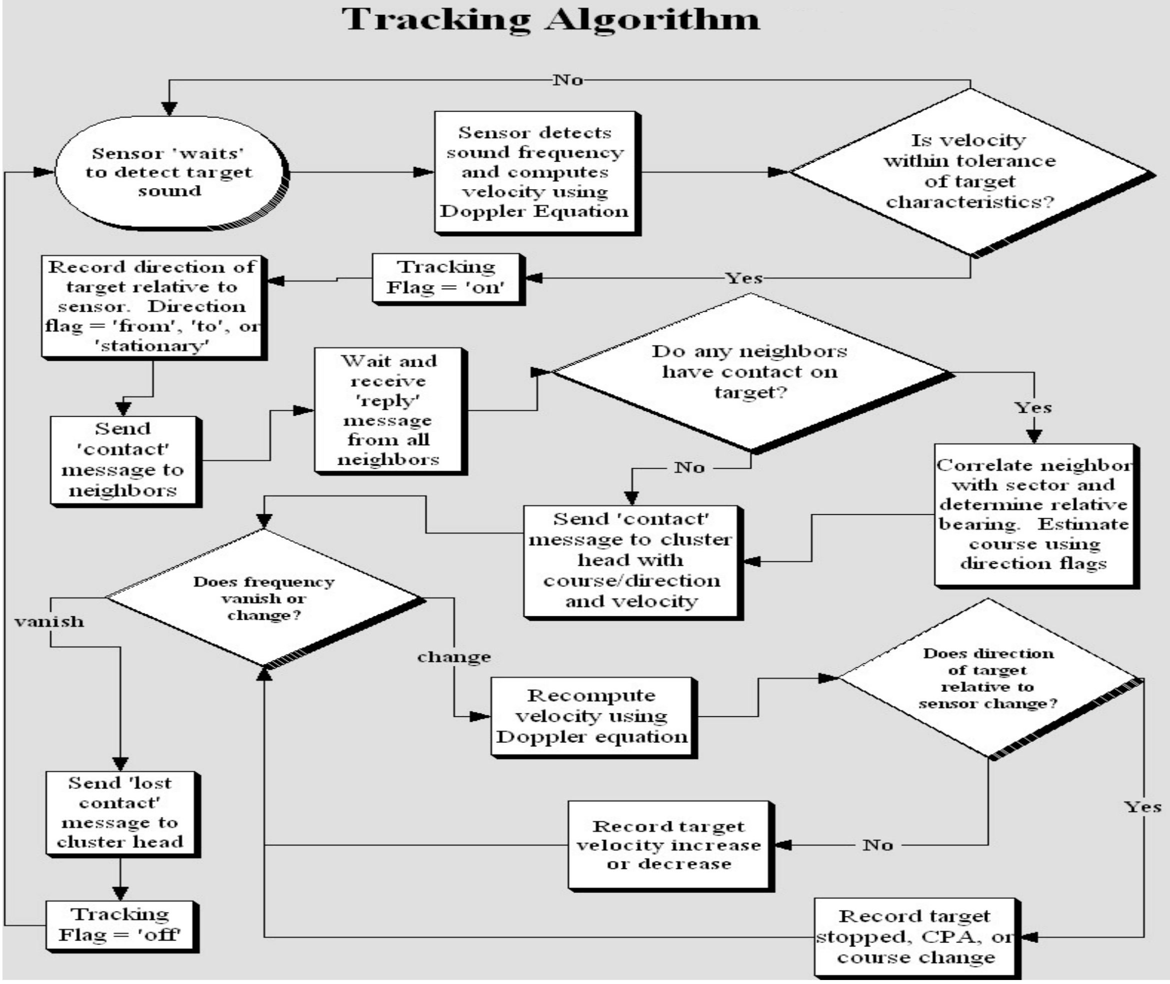

Figure 4. Flow Chart for the Tracking Algorithm

Military and Homeland Security: The land-based applications of sensor networks in the military and homeland security domains show how significant wireless sensor networks can be. Smart uniforms equipped with sensor nodes can automatically report data on the status of troops and their locations. Tanks and military vehicles can also be equipped with sensor nodes forming a wireless network connecting the different units of the army. Real-time border sensor networks represent a great asset in policing the borders and reporting any suspicious movements. All of these applications can be mapped to their corresponding marine applications only if a wireless sensor network can be deployed in the water.

Ocean Inhabitant Research: The possibility of having sensor nodes diving in the ocean collecting data about the different inhabitants offers a unique opportunity for ocean life can play a major role in bringing ocean research to new levels.

V. MARINE WIRELESS SENSOR NETWORKS IN FUTURE DIGITAL BATTLEFIELDS

According to the “Army Research Office In Review document” [1], the need for *on-the-move mobile wireless networks* that can be deployed in the battlefields of the future cannot be underestimated. Sensor networking presents an essential component of future digital battlefields. The main idea is to develop a secure two-layer broadband wireless infrastructure for mobile ad hoc and sensor networks with military and homeland security applications that take advantage of underwater sensors that can track targets of interest. The development of such infrastructure enhances the survivability of ad hoc networks and widens the domain of applicability by ensuring secure communications with broadband capabilities that can meet

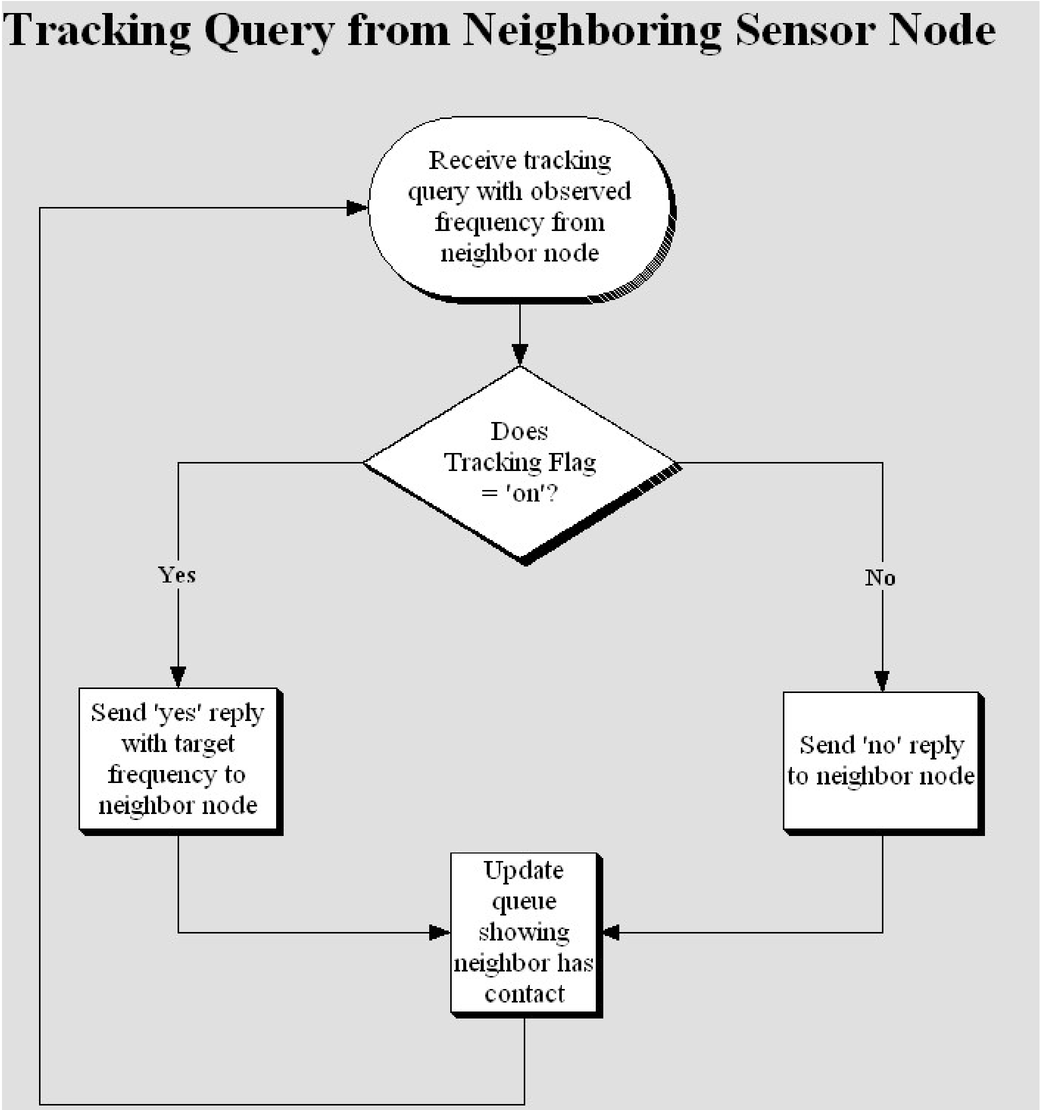

Figure 5. Flow Chart for the Tracking Query

the requirements of expected future digital battlefield applications. More specifically, improving the efficiency of the virtual organization of ad hoc networks through scalable clustering techniques and the support of a secure wireless broadband backbone are the scope of this work. We present a two layer networking infrastructure with virtual as well as physical support. The bottom layer is a virtual layer that addresses the efficiency issues of infrastructureless ad hoc networks by providing a hierarchical organization. The network is divided into clusters where every cluster is supervised by a clusterhead. Clustering methods are designed to seek specific network merits such as security, stability, and load balance. The proposed infrastructure includes further support through a second layer of broadband backbone. This top layer furnishes the network with broadband-enabled nodes with communication capacity that meets the growing demands on high transmission rates unlike existing ad hoc networks. This layer provides an alternate communication path for isolated nodes ensuring a connected network and robust military operations. This will alleviate the problem of poor reliability of existing ad hoc networks leading to better scalability. In addition, these nodes will function as gateways allowing broadband communications with other networking platforms independent of the underlying technology, thus conferring to a major requirement of future wireless systems. Figure 6 depicts a hypothetical battlefield sensor network based on the proposed architecture. This network can be rapidly deployed allowing a wide range of entities to securely communicate for fast information sharing and better decision making. The bottom layer forms a mobile ad hoc network of army robots, underwater sensor nodes, troopers, tanks, vehicles, sensors…etc. The top layer is a backbone that provides a broadband wireless cloud using high-speed wireless technologies such as optical wireless, ultra-wideband, WiMAX and/or WiFi. Helicopters, robots, and ships can be equipped to operate as backbone communication nodes. The following explains how this research satisfies the Army Future Force operational goals and how it is highly relevant to the army research and needs.

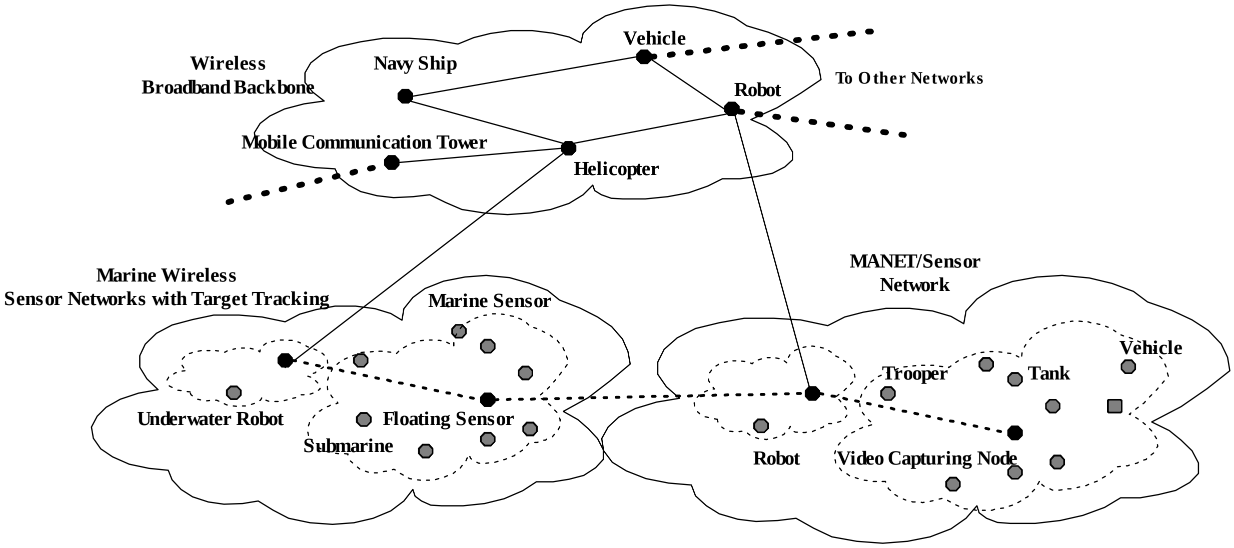

Figure 6. An Example of How Marine Wireless Sensor Networks can be used in Future Digital Battlefields

Communications and Networks Needs:

The Army Research Office In Review explicitly states its major communications and networks needs as follows [19]

- *“Mobile wireless communications networks will be required that are both adaptive and can operate on-the-move.”*
- *“New sensor, communication, and weapon systems based on unmanned robotic and teleoperated aerial and ground vehicles must be developed.”*
- *“The concepts of light, agile forces and the digital battlefields require a seamless…and highly mobile wireless communication system with a highly dynamic topology.”*

The proposed architecture directly addresses the above army research goals by providing a self-organizing mobile ad hoc network that can be rapidly deployed. The bottom layer of the proposed architecture furnishes the network with a flexible topology that can timely respond to environment changes. Moreover, the nature of mobile ad hoc networks allows the use of marine sensor networks, robots, and vehicles to serve as communication nodes (see Figure 1). The ad hoc layer of the proposed infrastructure will address the performance and efficiency issues. This layer is organized in the form of clusters and is dynamically established in two steps. Clusters are, first, formed following a cluster formation technique, and then clusterheads are selected. The top layer of the proposed architecture provides a backbone through the use of broadband wireless technologies that mostly operate in a point-to-point fashion (ex, optical wireless or ultra-wideband) achieving highly secure communication links with high immunity to jamming and interference.

VI. CONCLUSIONS

Current research on wireless sensor networks is based on the assumption that these networks are deployed in a terrestrial environment. Relevant protocols and design specifications are developed under this condition. This makes the deployment of currently existing wireless sensor networks in marine environments extremely challenging. In this paper, we present major challenges and applications of underwater wireless sensor networks. Target tracking in such environments is emphasized. A basic target tracking algorithm for cluster-based marine wireless sensor networks is presented. We discuss application areas that highly benefit from a marine network with target tracking such as military and inhabitant monitoring. We highlight the army’s immediate needs for secure agile broadband communications for future digital battlefields emphasizing the role of marine sensors with target tracking capabilities. A two-layer architecture for broadband terrestrial/marine ad hoc and sensor networks that can provide warfighters with a secure on-the-move means for high-capacity communications is discussed.

ACKNOWLEDGMENT

This work was supported, in part, by an NSF CRI grant and a Texas Research Development Fund grant.

REFERENCES

[1] A.M. Mahdy, “Marine Wireless Sensor Networks: Challenges and Applications," Proceedings of the 7th International Conference on Networking (ICN), 2008, pp 530-535.
[2] D.P. Agrawal and Q-A. Zeng, “Introduction to Wireless and Mobile Systems,” Thomson Brooks Cole, USA, 2003.
[3] D.B. Johnson and D.A. Maltz, “The Dynamic Source Routing Protocol in Ad Hoc Networks,” Mobile Computing, T. Imielinski and H. Korth eds., Culwer, 1996, pp. 152-181.
[4] I.F. Akyildiz, D. Pompili, and T. Melodia, “Underwater Acoustic Sensor Networks: Research Challenges”, Ad Hoc Networks, Volume 3, Issue 3, 2005, pp. 257-279.
[5] J.H. Cui, J. Kong, M. Gerla, and S. Zhou, “The Challenges of Building Scalable Mobile Underwater Wireless Sensor Networks for Aquatic Applications”, IEEE Network, 2006, pp.12-17.
[6] I. Vasilescu, K. Kotay, and D. Rus, “Krill: An Exploration in Underwater Sensor Networks”, Proceedings of the 2nd IEEE Workshop on Embedded Networked Sensors, 2005.
[7] J.N. Al-Karaki, A. Kamal, and R. Ul-Mostafa, “On the Optimal Clustering in Mobile Ad Hoc Networks,” Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC), 2004, pp. 71-76.
[8] W. Lou and J. Wu, “A Cluster-Based Backbone Infrastructure for Broadcasting in MANETs,” Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS), 2003.
[9] J. Waldo, “Constructing Ad Hoc Networks,” Proceedings of the IEEE International Symposium on Network Computing and Applications (NCA), 2001, pp. 9-20.
[10] Y. Song and D. Park, “Infrastructure Support for Ad Hoc Network: When and Where?,” Proceedings of the 2004 International Conference on Parallel Processing Workshops (ICPPW), 2004, pp. 141-147.
[11] P.C. Etter, “Underwater Acoustic Modeling, Principles, Techniques and Applications,” 2nd edition, E&FN Spon, 1996.
[12] D.B. Kifoyle, and A.B. Baggeroer, “The State of the Art in Underwater Acoustic Telemetry”, IEEE Journal of Oceanic Engineering, (OE-25, no. 5), 2000, pp. 4-27.
[13] D. Makhija, P. Kumaraswamy, and R. Roy, “Challenges And Design of Mac Protocol For Underwater Acoustic Sensor Networks”, 4th IEEE International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2006, pp.1-6.
[14] J. Proakis, J. Rice, E. Sozer, and M. Stojanovic, “Shallow water acoustic networks,” Encyclopedia of Telecommunications, John Wiley and Sons, 2003.
[15] J. Partan, J. Kurose, and B.N. Levine. “A Survey of Practical Issues in Underwater Networks,” Proceedings of the 1st ACM International Workshop on Underwater Networks, 2006, pp 17-24.
[16] S. Pai, P. Guerrini, and J. Potter, “Autonomous initial capture systems for AUV recovery,” Proceedings of the 3rd International Conference and Exibition for Underwater Acoustic Measurements: Technologies and Results, 2009.
[17] J.N. Al-Karaki, and A.E. Kamal, “Routing techniques in wireless sensor networks,” IEEE Wireless Communications, Volume 11, Issue 6, 2004, pp 6-28.
[18] R.R. Brooks, P. Ramanathan, and A.M. Sayeed, “Distributed target classification and tracking in sensor networks.” Proceedings of the IEEE. Volume 91, Issue 8, 2003, pp. 116 –1171.
[19] Army Research Office In Review, http://www.arl.army.mil/main/main/default.cfm?Action=29&Page=172, (last visited June 2010).