PARAMETER ASSIGNMENT FOR IMPROVED CONNECTIVITY AND SECURITY IN RANDOMLY DEPLOYED WIRELESS SENSOR NETWORKS VIA HYBRID OMNI/UNI-DIRECTIONAL ANTENNAS

A Thesis

by

SONU SHANKAR

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

August 2008

Major Subject: Computer Engineering

PARAMETER ASSIGNMENT FOR IMPROVED CONNECTIVITY AND SECURITY IN RANDOMLY DEPLOYED WIRELESS SENSOR NETWORKS VIA HYBRID OMNI/UNI-DIRECTIONAL ANTENNAS

A Thesis

by

SONU SHANKAR

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Approved by:

Co-Chairs of Committee,	Deepa Kundur
	Alexander Sprintson
Committee Members,	Eun Jung Kim
	Jiang Hu
Head of Department,	Costas Georghiades

August 2008

Major Subject: Computer Engineering

ABSTRACT

Parameter Assignment for Improved Connectivity and Security in Randomly Deployed Wireless Sensor Networks via Hybrid Omni/Uni-Directional Antennas. (August 2008)

Sonu Shankar, B.E., Anna University, India

Co–Chairs of Advisory Committee: Dr. Deepa Kundur
Dr. Alexander Sprintson

Configuring a network system to operate at optimal levels of performance requires a comprehensive understanding of the effects of a variety of system parameters on crucial metrics like connectivity and resilience to network attacks. Traditionally, omni-directional antennas have been used for communication in wireless sensor networks. In this thesis, a hybrid communication model is presented where-in, nodes in a network are capable of both omni-directional and uni-directional communication. The effect of such a model on performance in randomly deployed wireless sensor networks is studied, specifically looking at the effect of a variety of network parameters on network performance.

The work in this thesis demonstrates that, when the hybrid communication model is employed, the probability of 100% connectivity improves by almost 90% and that of k-connectivity improves by almost 80% even at low node densities when compared to the traditional omni-directional model. In terms of network security, it was found that the hybrid approach improves network resilience to the collision attack by almost 85% and the cost of launching a successful network partition attack was increased by as high as 600%. The gains in connectivity and resilience were found to improve with increasing node densities and decreasing antenna beamwidths.

To My Mother

ACKNOWLEDGMENTS

I would like to thank Dr. Deepa Kundur for being the most inspirational person I have met during my time at Texas A&M. I owe her a lot for driving my interest in sensor networks and specifically for building my skill set when looking at security related problems. I would like to thank Dr. Alex Sprintson for the many fruitful discussions we have had and also for the tremendous support he has provided. I am deeply grateful for his support.

I would also like to thank the members of my committee Dr. Eun Jung Kim and Dr. Jiang Hu for their time and input towards the betterment of my thesis. Dr. Takis Zourntos is someone who would always reinvigorate the motivation and trust I have in the wonderful art of engineering and I thank him for the same.

I would like to give my thanks to Unoma Okorafor for her suggestions with my thesis and to Ji Heon Kwon for his work towards realizing many parts of my plan. I give my thanks to Julien Jainsky for being an amazing friend, helping me whenever the need existed and my group mates Alexandra Czarlinska and William Luh for all their help and encouragement.

Last, but not the least, I thank my family for seeing me through my best and worst and being my continuous source of motivation.

TABLE OF CONTENTS

CHAPTER Page

CHAPTER Page

LIST OF TABLES

LIST OF FIGURES

FIGURE Page

CHAPTER I

INTRODUCTION

A. Wireless Sensor Networks, Connectivity and Security

The need for constant surveillance, especially of physical areas that are remotely located, dangerous or just not economically feasible for the active presence of human observers strongly motivates the use of wireless sensor networks (WSNs) that consist of a network of tiny nodes capable of sensing, collecting and organizing data along with communicating significant information to a central base. Sensor networks are expected to cooperatively monitor physical and environmental parameters in a broad set of applications that include battlefield surveillance and reconnaissance, environment and habitat surveying, healthcare, home automation, border security and many more [1] [2]. A defining characteristic that usually separates WSNs from other ad-hoc networks is that of self-organization and unattended operation. Sensor networks are expected to organize, sense and communicate on their own once they are deployed in a target environment.

The most fundamental sensor network architecture consists of randomly distributed nodes in a target area. Each node is typically equipped with multiple sensors, depending on the physical quantity that needs to be measured along with a radio frequency (RF) or optical transmitter/receiver arrangement and a small microprocessor. The power source for each node is usually a battery that has a limited life time. The nodes sense physical activity and report significant information to a data collection center called the *sink*. The sink may be in an area that is also occupied by human beings and is in any case considered to be of higher capabilities than a member node

The journal model is *IEEE Transactions on Automatic Control.*

in the network in terms of energy, memory, computational power and bandwidth. It is a trusted entity in the network. The sink is also envisioned as a mobile entity or a mobile base station [3] that is useful in cases when nodes collect data and transmit readings to a base station when available.

Although the areas in which sensor networks may be applied can vary sharply, a common requirement of all applications is a high level of connectivity and inherent procedures to secure the functioning of the network deployment [4–6]. These issues drastically affect the performance of a sensor network deployment. To be able to extract the most out of any investment in a network deployment, connectivity and security must be priortized.

Connectivity is a fundamental requirement in wireless sensor and ad-hoc networks, representing the capability of a member node to communicate with other nodes in the network either by direct transmission or via multi-hop relays. It impacts every aspect of network performance including comprehensive monitoring, the capability of self-organization, energy consumption, network longevity and network capacity.

Security in the context of WSNs deals with protecting a network deployment from common network attacks that work against the normal, expected functioning of a network drastically affecting performance and harming the capability of a network to collect and report data in a timely manner. A secure network has an inherent set of procedures that provides a reasonable level of resilience against network attacks, such that even in the presence of adversaries the network can be expected to function without any hindrance or possibility of sending distorted information to a data collection center.

B. Background and Motivation

1. Connectivity, Security and Deployment Costs in Today's WSNs

A major factor that is considered while installing sensor nodes in a target environment is the number of nodes to be deployed in order to guarantee the surveillance of the area considered. According to the necessity of an application, it may be necessary to have a high degree of precision for sensing physical quantities. Along with accuracy of sensed data, the capability of a network deployment to monitor the entire target environment is crucial in many sensor network applications.

Traditionally, each node in a sensor network is equipped with an omni-directional antenna such that it can directly communicate with any other member node that is within a particular radius around it. This radius is called the *transmission radius* of the node. It defines the maximum transmission reach any node has and the circle of a radius equal to the transmission radius around each node defines the *transmission range*. Another member node that is within the transmission range of a particular node is termed its *neighbor*. Equivalently, any node can send information to a neighbor via direct transmissions. If transmission of information between two nodes require relays where-in other member nodes forward the senders packet, passing it on to other member nodes to eventually reach the destination, then the path followed is called a *multi-hop* path as it does not reach the intended destination with a single direct transmission.

Sensor network nodes are usually deployed randomly and hence there is a non-zero probability that one or more nodes in a deployment may be *isolated.* This means that certain nodes will not have any other node within its transmission range or equivalently, there exists no neighbors for this node. This also means that there is no way for the node to send information to the data collection center or the sink.

As nodes are usually randomly deployed in a target field, there is substantial motivation to be able to provide higher probabilities of connectivity for the nodes dropped. Again, depending on the application, *connectivity* may be defined in multiple ways. A very strict requirement is that of *100% connectivity* which means that every node in the deployment is capable of communicating with every other node in the network via direct or multi-hop paths.

Connectivity and capability of comprehensive monitoring can be improved quite simply by increasing the number of nodes deployed. This isn't always the best approach as certain applications also have limitations on network cost. Increasing node density equates to increased cost of deployment. Hence, there exists a need to increase the level of connectivity without really increasing the number of nodes deployed, with a reasonably minimal increase in per-node cost.

Another perspective is that of applications that have a fixed cost. It would be interesting to look at ways in which assuming a fixed cost of deployment and operation, high levels of connectivity could be guaranteed with higher probabilities, possibly even by using a smaller number of nodes in the network.

There is a close relationship between connectivity and security of the network. Secure protocols [7], at all layers of the networking stack, of course, help the cause of improved resilience to network attacks. Improved connectivity, being a fundamental physical issue works towards member nodes in a network deployment possessing multiple paths, independent and otherwise, between each other. This directly affects the resilience of a network to denial of service (DoS) attacks [8] as when more paths exist between nodes in a network, the cost of launching a successful attack would be expected to increase. Consequently, there is also the need to study ways in which the security of a deployment can be improved such that similar levels of resilience can be provided at lower node densities, again with reasonable increase in per-node cost if modification is at the mote level.

Beyond the motivation of an improved cost-to-benefit ratio, being able to extract better performance from smaller node densities also have strong implications in deployments that require a high level of covertness. Military applications like reconnaissance procedures [9] and other security applications may require that only a certain number of nodes may be deployed as a larger number might tend to compromise the covertness of the intelligence mission. It is interesting to note that in such applications there is a significant need to limit the number of nodes deployed although there is no limitation on costs. This requirement may also exists in applications that involve monitoring very delicate biological environments [10] where the least number of foreign hardware and entities need to be employed for observation.

2. Omni-Directional and Uni-Directional Antennas in WSNs

An omni-direcitonal antenna radiates or receives equally well in all directions. It is an antenna system that radiates power uniformly in one plane (say, the horizontal plane) and has a directive pattern in a plane perpendicular to the first one. Traditionally sensor networks are modeled using motes that use omni-directional antennas for communication.

The radiation pattern of an omni-directional antenna is shown in Fig. 1. It is to be noted that in reality, radios produce three dimensional radiation patterns (Specific details on antennas in [11]) but in this section only the azimuthal patterns are presented. The radiation patterns are three-dimensional quantities involving the variations of field or power (which is proportional to the square of the field) as a function of the spherical coordinates [12].

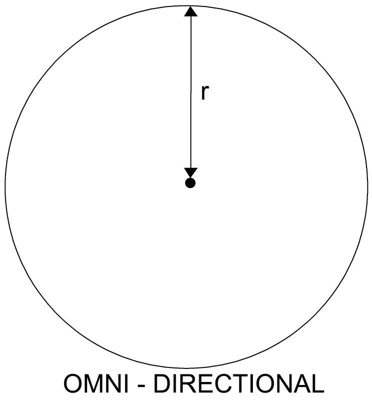


Fig. 1. Omni-Directional Antenna - Radiation Pattern

Antenna *gain* is the ratio of the power density of an antenna's radiation pattern in the direction of strongest radiation to that of a reference antenna. An isotropic radiator, a theoretical point source of waves which exhibits the same magnitude or properties when measured in all directions, is usually the reference antenna. *Directive Gain* is a related term that is the measure of the intensity of an antenna's electromagnetic radiation in a particular direction.

In Fig. 2 a uni-directional antenna's radiation pattern is shown. The energy in a uni-directional antenna is focused in one direction and hence these types of antennas are typically characterized by transmissions that reach much farther than omni-directional antennas. The *main lobe* in the uni-directional antenna's pattern is the direction of maximum radiation (or reception, if reception is also modeled using directional antennas). As seen in the figure there are also extra *minor lobes* (*side* and *back* lobes). These lobes represent lost energy, that is energy spent on directions away from the direction of interest, where the antenna intends to transmit. Uni-directional antenna designers always attempt to minimize these lobes. If a field pattern is described in the three-dimensional spherical coordinate system, then the

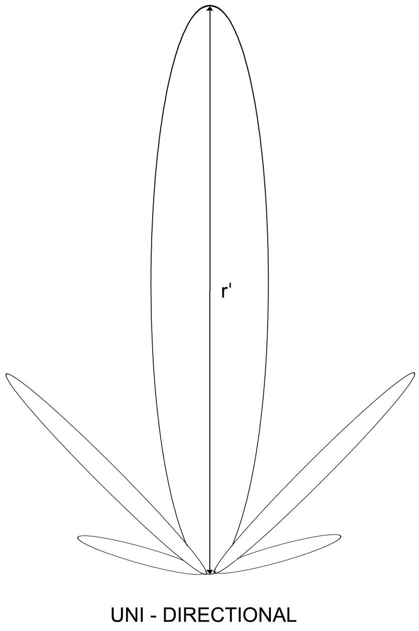


Fig. 2. Uni-Directional Antenna - Radiation Pattern

pattern will have its main lobe or direction of maximum radiation in the z direction, where $\theta = 0$. The minor lobes, will be in other directions.

Any field pattern that is represented in the three-dimensional spherical coordinate system can also be presented by plane cuts through the main lobe axis [12]. Two cuts at right angles, the *principal plane patterns* are possible in the xz and the yz planes. For uni-directional antenna patterns, as the pattern is symmetrical around the z axis, one cut is sufficient to describe the pattern. Such a pattern is shown in Fig. 2.

The *beamwidth* of a uni-directional antenna is a measure of its directivity which is the width of the main lobe measured in degrees. Beamwidth is usually measured between the -3 dB points, the points on the main lobe where the signal strength drops

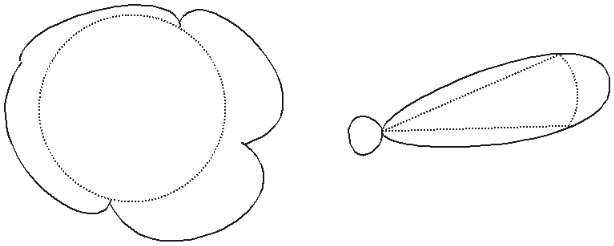


Fig. 3. Radiation Pattern Approximations

by -3 dB (one-half) from the point of maximum signal intensity. This is also called the *half-power beamwidth*.

It may also be noted that the omni-directional and uni-directional radiation patterns are approximated as circles and sectors corresponding to the largest regular shape that the actual radiation pattern of such antennas can enclose. This can be seen in Fig. 3 where the dotted lines represent the approximated pattern, which is a circle in the case of an omni-directional antenna and a sector in the case of a uni-directional antenna.

$$P = C.\pi r^2 \tag{1.1}$$

$$P = C'.\frac{\alpha r'^2}{2} \tag{1.2}$$

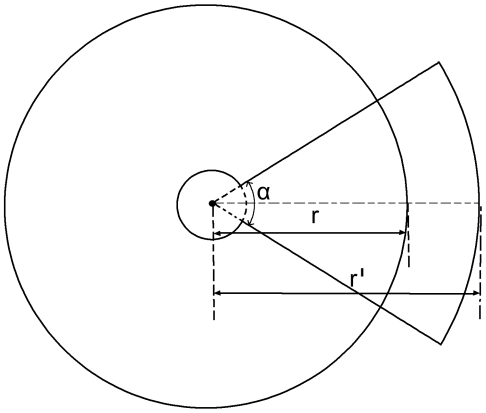
From [13], the energy required by a sensor node to reach all neighboring nodes within its transmission range is proportional to the area covered by it's radiation pattern and is given in Eqs. (1.1) and (1.2) where r is the omni-directional antenna transmission radius, r' is the uni-directional range in the direction of peak gain, α is the antenna beamwidth, P is the transmission power drawn at each antenna and C and C' are appropriate constants. In Eq. (1.2) the sidelobes and backlobes are considered to be negligible and the power is radiated entirely through the primary main lobe.

To compare the capabilities of uni-directional and omni-directional antennas, the case where the area covered by the respective antenna's radiation pattern is the same for each type of antenna is considered. The assumption of using a constant area in both antenna modes is justified from the knowledge of the drawn power being proportional to the area covered by the radiation patterns. Then, the ratio $k = r'/r$ quantifies the additional reach possible by a uni-directional antenna over its omni-directional counterpart and this improvement depends on the uni-directional antenna beamwidth.

$$k = r'/r = \sqrt{\frac{2\pi}{\alpha}} \geq 1 \tag{1.3}$$

Eq. (1.3) shows that a uni-directional antenna with a narrower beamwidth will be able to transmit signals that reach a longer distance, i.e. the narrower the beamwidth, the higher the antenna gain. The above equations also assume that the antennas involved have 100% efficiency, meaning that all the power delivered to the antenna circuit is radiated during transmission, the power fed being effectively converted into radiated power.

Fig. 4 compares the perfect radiation patterns of uni-directional and omni-directional antennas. It is to be noted that although it may appear that a very narrow antenna beam would have phenomenal effects on increasing antenna gain there are practical limitations in extending transmission range using this approach. Sensor networks have very strict requirements on form factor and size of motes. The antenna size needs to be equivalent to the wavelength λ of operation [14] for power efficient operation. Antenna systems that need arrays of elements also require that they be placed at set distances apart, for example $\frac{\lambda}{2}$. The unlicensed bands that are usually used for the operation of sensor networks works at 2.4 Ghz [15]. This brings



UNI OVER OMNI

Fig. 4. Uni-Directional Antennas vs. Omni-Directional Antennas

up limitations on the number of antenna elements that may be used in an array if there are constraints in the size of a sensor mote. Thus, antenna beamwidths of $\frac{\pi}{3}$ through $\frac{\pi}{6}$ are common although achieving even narrower beams is expensive and usually avoided in sensor mote design.

3. Graph Theory Basics

As the analysis on connectivity and security presented in this work will strongly use concepts from graph theory, some basics are presented first [16].

An ad hoc network can be represented as an undirected graph G. A graph $G = G(V, E)$ consists of a set of n nodes or vertices and a set of m node pairs or edges. $V = \{1, \ldots, n\}$, is the set of vertices that actually represents the motes deployed in the WSN; and the set of edges, denoted by E, represent the communication links between these sensor motes. As the assumptions in this work include that of a symmetric channel and as every member node is assumed to have similar capabilities, a network can be modeled as an undirected graph.

A *neighbor* of a node is any node that has a direct link or an edge with the node being considered. The *degree* of a node x, denoted as $d(x)$, is the number of neighbors of node x. A node of degree $d = 0$ is called an *isolated node*. Such nodes have no neighbors.

The minimum node degree of a graph G is denoted as

$$d_{min}(G) = \min_{\forall\ u \in G} d(u) \tag{1.4}$$

A graph is connected, if for every pair of nodes there exists a path, consisting of one or more edges, connecting them. The graph is deemed disconnected otherwise. This relates to WSNs as in typical deployments there might be cases when many islands of nodes that are disconnected from a larger connected chunk exist. For a truly connected network, all nodes in the deployment must be able to communicate with each either via direct or multi-hop communication.

There is also the metric of *k-connectivity* that is very significant to WSN deployments. A graph has k-connectivity, where $k = \{1, 2, 3, 4, 5, \ldots\}$ if for every pair of nodes there exists at least k disjoint and mutually independent paths connecting them. Another similar definition is that for any graph if after disabling *any* $(k - 1)$ links the graph remains connected then that graph is k-connected. This is equivalent to the case when if after the failure of any $(k - 1)$ nodes, the graph is still guaranteed to be connected, then that graph is k-connected.

The connectivity κ for a graph is the maximum value of k for which a connected graph is k-connected. It can be intuitively agreed that κ would be the smallest number of nodes, the failure of which would deem the network disconnected.

C. Problem Formulation and Thesis Contributions

This thesis aims to provide useful network deployment information for randomly deployed WSNs using a non-traditional communication model that can improve both connectivity and security when compared to omni-directional antenna based networks. Specifically, to be able to provide helpful suggestions to an agency or individual planning on mass sensor network deployments in cases when there are many crucial parameters that need to be carefully chosen. Poor choice of crucial network parameters could cause a catastrophic increase in the cost of deployment and operation and more importantly could drastically affect the error-free functioning of the deployment.

The primary problem this thesis deals with is parameter assignment for a new communication paradigm that can possibly be standardized for sensor networks over a wide range of applications by providing significant results in the realms of connectivity and security even at lower node densities. This communication paradigm is one that should work in tandem with any existing WSN protocol at the link layer, network layer or beyond. The model must be able to extend the physical capabilities of a sensor mote without drastically increasing the operating power. The improvements in physical capabilities must not reduce the battery life of a sensor mote with the new model when compared with a traditional mote using omni-directional communication. Another requirement is that of not markedly increasing the complexity of operation in terms of computational needs based on protocol changes at different layers in order to support the communication model. The legacy of sensor networks and the ability for mass deployment largely relies on low costs of production, deployment and operation. This assumption will stay and drives all design changes.

Parameters including node density, transmission radius and (for the case of networks that involve uni-directional antennas) antenna beamwidth have a very strong influence on network performance. For any communication model there is a need to comprehensively understand the effect of varying these parameters on common metrics of performance. The work in this thesis aims to provide insights on the effects of these parameters on metrics relating to connectivity including the probability of 100% connectivity, probability of k-connectivity and average number of disjoint paths available for all randomly deployed nodes in a sensor network.

In the area of sensor network security, the work in this thesis is intended to show that using the non-traditional communication model described will result in improved resilience towards Denial-of-Service attacks at lower layers and also network partition attacks. There is a need to reduce the probability of successful attacks and at the same time increasing the cost of launching attacks on a sensor network deployment, without drastic increases in computational complexity and operation costs.

A common theme that is of interest to the work in this thesis is studying the capability of a sensor network deployment to perform up to required standards even at lower node densities and transmission radii. For reasons mentioned in Section 1 operation at low node densities is very desirable for a wide range of applications. Extracting very desirable results from settings that include low node density, low protocol overhead and computational complexity along with negligible increase in operating costs is a requirement that can be mapped to satisfy many sensor network applications.

Specifically, this thesis addresses the issues outlined above by:

- Justifying the hybrid communication model and assumptions made for practical network deployment scenarios.

- Providing connectivity analysis resulting in improved 100% connectivity in low density network deployments in comparison to traditional omni-directional WSNs.

- Providing k-connectivity analysis resulting in improved average disjoint paths in low density network deployments in comparison to traditional omni-directional WSNs.

- Providing network security analysis for the *DoS Collision Attack* resulting in improved resilience to such an attack in the hybrid communication model in comparison to traditional omni-directional WSNs.

- Providing network security analysis for the *Network Partition Attack* resulting in improved resilience to such an attack in the hybrid communication model in comparison to traditional omni-directional WSNs.

- Empirically investigating the behavior of parameter values transmission radius, node density and antenna beamwidth with respect to their influence on connectivity and security.

- Conducting a feasibility study of the implementation, costs and protocol modifications involved for the use of the hybrid communication model.

CHAPTER II

THE HYBRID COMMUNICATION PARADIGM

A. The Hybrid Approach

The communication paradigm that is envisioned to be employed in this thesis to meet the demands of the problem formulated previously is termed the *Hybrid Omni/Uni Approach.* The approach utilizes the insights gained from the study of antenna gains in uni-directional and omni-directional antennas that were described in Section 2.

1. Node Details

Each sensor node in this approach is capable of both omni-directional and sectorized uni-directional communications. Depending on the antenna beamwidth α used, the number of sectors N_s varies. The node is capable of transmitting in N_s non-overlapping sectors where the antenna beamwidth α has an angle span $\frac{2\pi}{N_s}$ radians.

The node is capable of transmitting to a maximum range r' defined by Eq. 1.3 in each sector when compared with an omni-directional antenna of transmission radius r. Nodes are also capable of transmitting omni-directionally at a radius r. Reception at each node is modeled to be omni-directional.

According to the relationship in Eq. 1.3, nodes modeled using a hybrid approach as presented in this work are designed to consume the same power per transmission when compared with a traditional omni-directional antenna equipped sensor mote. Thus, in terms of battery life and system longevity, node following this communication model would see very similar performance to those adhering to an omni-directional model.

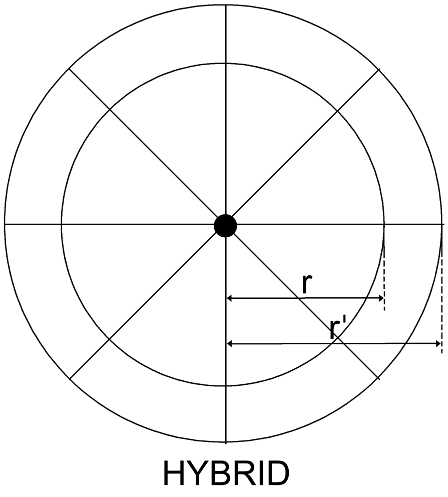


Fig. 5. The Hybrid Approach

Fig. 5 shows a node following the approach mentioned. A perfect radiation pattern is shown such that in each sector the node has an extra transmission reach of $r' - r$.

Table I. Transmission Range Comparisons for Omni-Directional and Hybrid Motes - Low r

r	$r'_{\frac{\pi}{3}}$	$r'_{\frac{\pi}{4}}$	$r'_{\frac{\pi}{6}}$
0.05	0.122474	0.141421	0.173205
0.10	0.244949	0.282843	0.346410
0.15	0.367423	0.424264	0.519615
0.20	0.489898	0.565685	0.692820
0.25	0.612372	0.707107	0.866025
0.30	0.734847	0.848528	1.039231

Table I compares the normalized transmission range of motes with omni-directional capability and those equipped with hybrid capable antennas. This table specifically

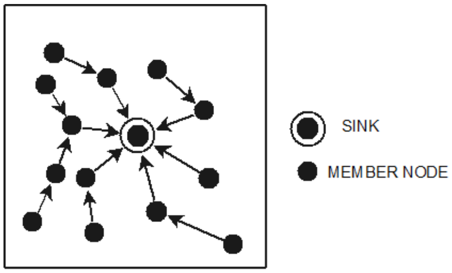


Fig. 6. Source to Sink Traffic in WSNs

lists the comparison for lower values of transmission radii, in contrast to the area of interest where the motes will be deployed.

Table II. Transmission Range Comparisons for Omni-Directional and Hybrid Motes - High r

r	$r'_{\frac{\pi}{3}}$	$r'_{\frac{\pi}{4}}$	$r'_{\frac{\pi}{6}}$
0.35	0.857321	0.989949	1.212436
0.40	0.979796	1.131371	1.385641
0.45	1.102270	1.272792	1.558846
0.50	1.224745	1.414124	1.732051
0.55	1.347219	1.555635	1.905256
0.60	1.469694	1.697056	2.078461

Table II tabulates the comparison of the transmission ranges for high transmission radius configurations.

2. Transmission and Traffic Modes

Fig. 6 graphically describes the most common traffic model seen in sensor networks. The typical case is that of a network of sensor motes, called the *member nodes* gathering information about the target environment and sending significant information to a, usually, centrally located sink. This traffic model is called a *Source-To-Sink* model. With such assumptions, the primary requirement for setting up paths at each node would involve computing paths towards the sink. It is to be noted that in applications that require collaboration between nodes, it is often needed to be able to send data to other member nodes, which would be equivalent to a point-to-point, ad-hoc traffic model. Certain applications [17] demand the collaboration of sensor motes to collectively work towards confirming an event and sending appropriate information to the sink. In this work, the issue of connectivity is looked at considering both models. Although, when security is considered, only the safeguarding of source-to-sink paths is looked at. The ability of member nodes to report sensed activity to the sink is a fundamental requirement in a sensor network deployment and hence receives the highest priority in terms of network security.

Traditionally, sensor networks could require both *unicast* and *broadcast* capabilities depending on the needs of an application. Unicast traffic is defined as traffic being sent to a single destination. Broadcast, on the other hand theoretically requires sending data to all devices or nodes in a network. At the node level, these definitions reduce to the classification of link layer transmissions. WSNs typically need to send sensed data to a centrally located sink and so usually have a neighbor that is the next-hop on a path towards the sink to which all data will be sent. This represents the unicast traffic at the node considered. Collaboration and requirements from routing protocols for example [18] would mean that nodes might have to send out occasional broadcasts to all of its neighbors for the desired functioning of the deployment. This would mean that each node must, at a minimum, have support for both unicast and broadcast traffic.

3. Omni-Directional Tx and Rx

In keeping with the requirements of reduced complexity, costs and computational capabilities, the model envisioned in this thesis also includes omni-directional transmission in-order to reduce the cost involved in broadcasts. Without omni-directional capability, the cost of a broadcast would incur more power and delay. In terms of the number of transmissions, it would take N_s transmissions and hence the total time required for the broadcast to be complete would also be proportional to N_s. In the hybrid approach, that would only be an upper bound as with a non-zero probability, we might only need a single omni-directional transmission or an omni-directional transmission along with a few uni-directional transmissions to complete a broadcast.

Thus for reasons of cost and reduced complexity, nodes are capable of either unicast transmission in one of the N_s sectors in the uni-directional mode or broadcast communication in the omni-directional mode. For similar reasons each node is modeled with omni-directional reception. The computational requirements involved with supporting a protocol that can synchronize and schedule nodes for directional reception is assumed to be prohibitive in terms of the needs of a sensor network being able to support cost-effective mass deployment.

Another motivation for retaining the omni-directional transmission in each of the hybrid-equipped nodes is the possibility of applying this work in the area of free space optical (FSO) sensor networks. Milner *et al* in [19] promote the use of directional optical sensors along with RF circuitry. The hybrid approach presented in this work analyses the possibility of using all sectors for communication along with omni-directional transmission and hence could be applied in the case when technology is available in the FSO area to be able to transmit in all sectors. The omni-directional transmission would help in situations when line-of-sight (LoS) is lost and optical communication fails.

4. Network Model

The network model that is assumed in this work is described in this section. Node deployment is considered to be random and following a uniform distribution. Nodes are also static and no form of mobility is assumed. The node deployment is assumed to be within a unit square with a centrally located sink at $(0.5, 0.5)$. As the primary interest in the area of smaller node densities and transmission radii, node densities in the set $[10, 100]$ and transmission radii in the set $[0.05, 0.45]$ are of particular importance. The channel is assumed to be symmetric such that if node x can reach node y through signal transmission then node y can also reach node x.

CHAPTER III

LITERATURE REVIEW

A. Related Work

The related work in the area of work that is of interest to this thesis can be divided into three categories. The first category is related to parameter assignment problems in traditional sensor and ad-hoc networks that are primarily theoretical in nature. The second category emphasizes on improvements via routing protocols, link layer protocols and topology control that provide insights on the use uni-directional antennas in sensor networks. The last category of related work deals with the use of such ideas in specific applications.

1. Parameter Assignment and Theoretical Studies on Connectivity

There is a tremendous amount of work in the area of connectivity in WSNs motivated by a variety of ideas originating from many different areas of networking and communication systems research [20–25]. The earliest work in the area of parameter assignment with regards to connectivity was in the '70s and the '80s. A large bulk of this work [26–28] concentrates on generating a *magic number* for the nearest neighbors at each node to be able guarantee connectivity and at the same time maximize capacity. The authors in [29] point out in a later publication that such a magic number does not really exist and for any deployment, as long as the target area is large enough it is easy to prove that the network is almost surely disconnected. Such a conclusion is extended in the more recent [30] with the result that each node in a deployment should be connected to $\Theta(\log n)$ nearest neighbors if the entire network is to be connected in a multi-hop setting.

The authors in [31] derive the critical transmission range of nodes placed randomly in a disc of unit area, so that the resulting network is connected with a probability of one as the number of nodes tends to infinity. The work in [32] considers an omni-directional communication model and includes results for the minimum node degree and connectivity with an emphasis on the importance of metrics like node density on those results. They also generate significant results in the realms of k-connectivity and the probability of node isolation.

The body of related work mentioned in this section is relevant to the work presented in this thesis as it motivates the study of connectivity and emphasizes on parameters like node density and transmission radius which is crucial while considering issues in this area. The work is also relevant because it motivates the fundamental approach used in this work, which is that of maximizing the transmission range physically possible for a given level of power consumption. The publications mentioned in this section helped identify the basic issues that could be dealt with in order to produce desirable results in the areas of connectivity and security.

2. Routing, Link Layer Protocols and Topology Control

Authors in [33] suggest the use of directional antennas in the context of routing in mobile ad-hoc networks when receiving nodes temporarily move out of the transmission range of a transmitting node. The work emphasizes on using the extended reach that is available via directional antennas to be put to use when necessary in situations like the network links being temporarily disconnected owing to the mobility of communicating nodes.

In [34] the improvements in the area of security achieved by using directional links. Most common network attacks on sensor network deployments [7] assume the use of bi-directional links. The authors in [34] discuss a secure routing protocol in the context of free space optical (FSO) sensor networks that use directional links with a stronger resilience towards common attacks, promoting the use of directional links.

The use of directional antennas in [35] is focused towards motivating the use of an energy efficient routing protocol. The work primarily looks at energy gains achieved from reduced interference using directional antennas. Unfortunately, the directional receive model used in this work increases the per-node cost. The lack of omni-directional capability could potentially also increases the per-node latency drastically. The cost of synchronization and coordination would be prohibitive for mass deployment.

There is significant work in [36] that looks at interference improvements that again comes via the use of directional antennas. The authors specifically look at the gains achieved in throughput and capacity by modeling transmission and reception using directional antennas. The analytical conclusion is that the throughput increases as the number of interfering neighbors decreases owing to the decrease in the interference area.

The body of work cited in this section goes further to motivate the use of directional antennas and specifically the gains in the areas of interference inhibition that is achieved from using them. The gains that are received from using directional antennas only motivate further the use of a new communication paradigm that will be proven to have superior performance in comparison with traditional approaches in the areas of connectivity and security in this thesis.

3. Application Specific Work

The use of directional antennas and beam steering techniques are investigated in *Mobisteer* [37]. The focus of the authors is to improve performance of 802.11 links in the context of vehicular ad-hoc networks, specifically to improve communication between automobiles and roadside infrastructure, through the use of directional antennas. A practical approach to implement beam steering is presented in the context of vehicular networks.

Analysis of the wormhole attack in sensor networks is done in [38]. The authors use directional antenna information to share sector information about neighboring nodes to identify adversary nodes masquerading as false neighbors. Wormhole endpoints are blacklisted via the directional information that is shared between neighbors. The use of directional antennas for improved security largely increases the probability of detecting the wormhole attack.

The *hybrid* work mentioned in [19] has been cited earlier. The authors motivate the use of omni-directional RF communication along with the use of a uni-directional FSO transceiver. The RF communication is enabled in cases when LoS is unavailable. The communication model considered in this work uses directional communication, activated in one sector that is randomly oriented based on deployment.

The body of work cited in this section motivates the use of directional for specific applications in the realms of sensor and ad-hoc networks. The work presented in this thesis uses a communication model that has not been studied in terms of the improvements that are possible in the areas of connectivity and security. The work in this thesis that deals with parameter assignment for node density, transmission radius, uni-directional antenna beamwidth for improved connectivity along with the details of attack configurations that can be defended against via the hybrid communication paradigm is not available in any existing work. This work is also unique as there is a strong emphasis on improving performance at lower node densities without an undesirable increase in operating costs and computational complexity.

CHAPTER IV

RESULTS[1]

A. Justification of Node Communication Model

To be able to perform analysis and simulation studying the improvements obtained from using a communication model as described in this work, analytical justification for the same is necessary. In this section, it is analytically proven that the assumptions used for the communication model employed are justified. This is done to be able to support the use of such a model for all further analysis and simulation work.

Lemma 1 *The minor lobes, represented by the side lobes and the back lobes in a uni-directional antenna's radiation pattern may be considered to be negligible, in comparison to the magnitudes of primary major lobes, for practical analysis while considering such antennas for a WSN application.*

Proof

The analysis presented in this section strongly follows results in [39]. To demonstrate using a simple example pattern, the radiation pattern graphically described in Fig. 2 is assumed to be achieved using an array of N antenna elements that have uniform amplitude and spacing. Let β be the *progressive phase lead* in the elements, which represents the phase which the current in each element leads the current of the previous element. d is the antenna spacing.

Thus, a *uniform array*, with identical elements of identical magnitude and each with a progressive phase is considered for the proof. The total field can then be

[1] Parts of this section are reprinted with permission from“Towards improved connectivity with hybrid uni/omni-directional antennas in wireless sensor networks” by S. Shankar and D. Kundur, IEEE INFOCOM Student Workshop April 2008.

formed by multiplying the array factor of the isotropic sources by the field of a single element. The field in the elevation plane when $\phi = 0$ is considered below. So the pattern becomes a function of θ.

The arrray factor is given by,

$$\begin{aligned} AF &= 1 + e^{+j(kdcos\theta+\beta)} + e^{+j2(kdcos\theta+\beta)} e^{+j3(kdcos\theta+\beta)} + \ldots + e^{+j(N-1)(kdcos\theta+\beta)} \\ &= \sum_{n=1}^{N} e^{+j(n-1)(kdcos\theta+\beta)} \end{aligned} \tag{4.1}$$

Eq. (4.1) can re-written as,

$$AF = \sum_{n=1}^{N} e^{+j(n-1)\psi} \qquad \text{where} \quad \psi = kdcos\theta + \beta \tag{4.2}$$

It can be seen that the total array factor for the considered uniform array is a summation of exponentials and this can be represented by the vector sum of N phasors each of unit amplitude and progressive phase ψ relative to the previous element. The above expression can be further simplified as shown below.

Multiplying both sides of Eq. (4.2) by $e^{j\psi}$,

$$(AF)e^{j\psi} = e^{j\psi} + e^{j2\psi} + e^{j3\psi} + \ldots + e^{jN\psi} \tag{4.3}$$

Substracting Eq.(4.2) from Eq.(4.3) the expression reduces to,

$$AF(e^{j\psi} - 1) = (-1 + e^{jN\psi}) \tag{4.4}$$

which can be further written as,

$$\begin{aligned} AF &= \frac{e^{jN\psi} - 1}{e^{j\psi} - 1} \\ &= e^{j[(N-1)/2]\psi} \left[\frac{sin(\frac{N}{2}\psi)}{sin(\frac{1}{2}\psi)} \right] \end{aligned} \tag{4.5}$$

When the reference point considered is the physical center of the array, Eq.(4.5) becomes,

$$AF = \left[\frac{sin(\frac{N}{2}\psi)}{sin(\frac{1}{2}\psi)} \right] \tag{4.6}$$

For small values of ψ, and also to normalize the values of the array factors to unity, the following may be done,

$$\begin{aligned} AF &= \left[\frac{sin(\frac{N}{2}\psi)}{sin(\frac{1}{2}\psi)} \right] \\ &\simeq \left[\frac{sin(\frac{N}{2}\psi)}{\frac{\psi}{2}} \right] \end{aligned} \tag{4.7}$$

$$\begin{aligned} AF &= \frac{1}{N} \left[\frac{sin(\frac{N}{2}\psi)}{\frac{\psi}{2}} \right] \\ &\simeq \left[\frac{sin(\frac{N}{2}\psi)}{\frac{N}{2}\psi} \right] \end{aligned} \tag{4.8}$$

Thus, the equation for the array factor that will be used in this proof is

$$AF = \left[\frac{sin(\frac{N}{2}\psi)}{\frac{N}{2}\psi} \right] \tag{4.9}$$

The interest of this analysis is to show that the minor lobes in the radiation pattern of a uni-directional antenna is negligible enough to be able to assume a pattern that can be put to great use in a WSN setting. As the equation represents a normalized pattern, the maximum amplitude of the main lobe is unity. The maxima of the first secondary minor lobe occurs when,

$$\frac{N}{2}\psi = \frac{N}{2}(kdcos\theta + \beta) \simeq \left(\frac{3\pi}{2}\right) \tag{4.10}$$

Using the value for θ_s which represents the orientation of the minor lobe and substituting in Eq.(4.9), the magnitude of the maximum of the first minor lobe is computed as $\frac{2}{3\pi}$. In dB, this is equal to *-13.46 dB.*

This proves that the side lobes and back lobes representing the minor lobes in a uni-directional antenna may be ignored for common analysis. Also, according to the array, spacing and individual magnitudes of antenna elements, even more negligible patterns may be produced. For complete and accurate expressions refer [39].

■

B. Connectivity Improvements via the Hybrid Approach

In this section, analysis and simulation results for improved connectivity in WSNs that employ the hybrid approach is presented. The connectivity issues studied can be broadly classified into two, viz. 100% Connectivity and k-connectivity.

1. 100% Connectivity - 1-Dimensional Analysis

100% connectivity is a very stringent requirement on WSNs, although it gives very strong insights on the improvements possible with the communication paradigm motivated in this work. 100% connectivity is defined as the case when every node in a network deployment is capable of communicating with every other node in the network either via direct transmissions or multi-hop paths. The fundamental communication model employed has a very strong influence on the connectivity of randomly deployed sensor motes.

A linear network of sensor nodes is considered first, before moving to results for nodes randomly deployed in a 2-dimensional plane. Analysis on linear networks provides very useful insights that usually extends to 2-dimensional analysis. A similar approach is employed in [24].

Lemma 2 *Let r be the transmission radius of a sensor node with an omni-directional antenna and r' be the maximum transmission range in the direction of peak gain for a sensor node with a uni-directional antenna. d_i is the inter-node distance between nodes i and $i-1$ in the linear network. Let $Pr\{\mathsf{max}\{d_i\} > x\}$ be the probability that the maximum inter-node distance in the network is greater than x.*

Then, $Pr\{\mathsf{max}\{d_i\} > r\} \geq Pr\{\mathsf{max}\{d_i\} > r^{'}\}$

Proof Consider a linear network where N nodes are distributed randomly over a line. The distribution of these sensor nodes conform to a Binomial process with a parameter p $(0 < p < 1)$. It is assumed that the inter-node distances conform to a series of independently and identically distributed geometric random variable $\{d_i\}$ with a parameter p. As consistently mentioned in this work, in the case of the omni-directional antenna the transmission radius is r and that in the case of the uni-directional antenna, the transmission range in the direction of peak gain is r'. The relationship between the two is as defined in Eq. (1.3). The network is deemed disconnected if the inter-node distance d_i between any pair of nodes is greater than the transmission radius of the antenna. If the inter-node distance between all neighboring nodes in the linear network is less than the transmission range of the antenna, then the linear network is 100% connected. This probability of the network being disconnected is systematically calculated below.

The probability distribution of the maximum inter-node distance $X = \mathsf{max}\{d_1, d_2, \ldots, d_{N-1}\}$ is characterized as follows.

$$\begin{aligned} Pr\{X \leq x\} &= Pr\{\mathsf{max}\{d_1, d_2, \ldots, d_{N-1}\} \leq x\} \\ &= Pr\{d_1 \leq x, d_2 \leq x, \ldots, d_{N-1} \leq x\} \\ &= \prod_{i=1}^{N-1} Pr\{d_i \leq x\} \\ &= [1 - (1-p)^x]^{N-1} \end{aligned} \tag{4.11}$$

Now, the probability that the network is disconnected with the antenna having a transmission range r can be calculated as

$$\begin{aligned} Pr\{\mathsf{max}\{d_i\} > r\} &= 1 - Pr\{\mathsf{max}\{d_i\} \leq r\} \\ &= 1 - [1 - (1-p)^r]^{N-1} \end{aligned} \tag{4.12}$$

Also from, Eq. (1.3) it can be deduced that the reach of the uni-directional antenna will always be greater than the omni case when a uni-directional beamwidth $\alpha \leq 2\pi$ is selected, which is the typical case.

$$r' \begin{cases} > r & \text{if } 0 < \alpha < 2\pi, \\ = r & \text{if } \alpha = 2\pi. \end{cases} \tag{4.13}$$

From Eq. (4.12) and Eq. (4.13) it can be concluded that

$$Pr\{\mathsf{max}\{d_i\} > r\} \begin{cases} > Pr\{\mathsf{max}\{d_i\} > r^{'}\} & \text{if } 0 < \alpha < 2\pi, \\ = Pr\{\mathsf{max}\{d_i\} > r^{'}\} & \text{if } \alpha = 2\pi. \end{cases} \tag{4.14}$$

Thus, in general,

$$Pr\{\mathsf{max}\{d_i\} > r\} \geq Pr\{\mathsf{max}\{d_i\} > r^{'}\} \tag{4.15}$$

■

The simulation set up for the following results is a linear network of nodes that are randomly distributed over a unit line. The interest of the simulation is in computing the probability of 100% network connectivity, which means that there is no inter-node distance in the randomly generated linear network that is greater than the transmission radius of the antenna . If t_r is the transmission range, which is r for omni-directional and r' for hybrid, then the linear network is disconnected if the inter-node distance between any pair of nodes is greater than t_r. The probability defined above is compared for motes deployed with omni-directional and hybrid capable antennas. 1000 random topologies were generated to be able to compute the probability.

It is to be noted that when the omni-directional transmission radius is r, the uni-directional case will have a radius that conforms to Eq. (1.3). To understand the relationship with node density and transmission radius, r was varied between 0.1 and 1.0 and n, the node density, between 10 and 100. Plots comparing the omni-directional only setting with a hybrid-capable network equipped with uni-directional antennas of beamwidth $\pi/4$ are shown below.

It is evident from the plots in Fig. 7 and Fig. 8 that in the regions for transmission radii between 0.1 and 0.2 the omni-directional configuration is inferior to that of the hybrid model by almost 75%. It is to be noted that these radii settings are the more practical settings in comparison with the length of the line which is considered here, which is unity. For the simulation setup, the omni-directional configuration was able

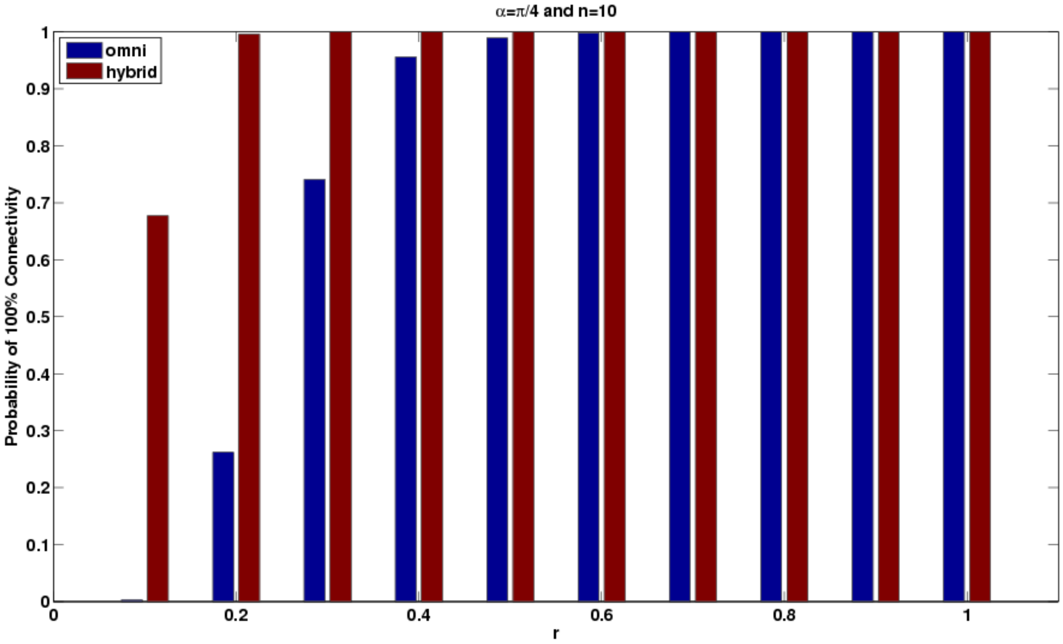


Fig. 7. Linear Network, 100% Connectivity - $\alpha = \pi/4$, r ranges from 0.1 to 1.0, n is constant at 10

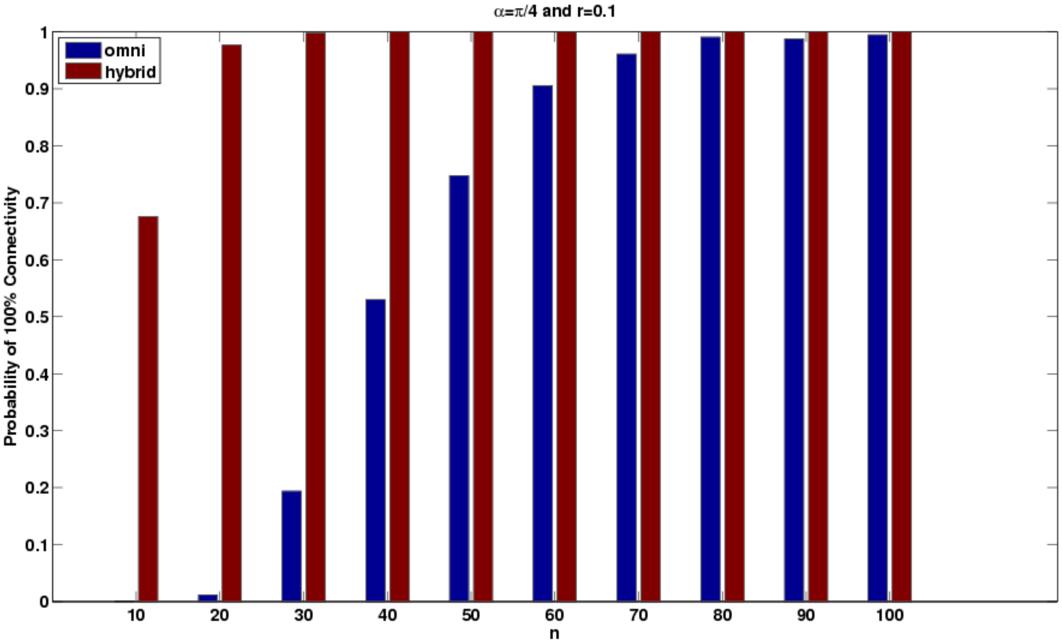


Fig. 8. Linear Network, 100% Connectivity - $\alpha = \pi/4$, n ranges from 10 to 100, r is constant at 0.1

to reach a probability of 1 only when the transmission radius was increased to almost 0.6.

For the study of varying node density, it is very motivating to notice that for node densities of 10 and 20, the improvements achieved from using the hybrid model almost reaches 90%. The improvement is very strongly evident until node densities of 50 and 60. It isn't until the node density is increased to around 90 and 100 that the omni-directional configuration actually matches the performance achieved from using a hybrid model.

2. 100% Connectivity - 2-Dimensional Analysis

a. Omni-Directional vs. Hybrid

For the 2-dimensional case, the analytical model and results assume a set of n network nods where n is any natural number. The nodes are independently and randomly distributed over a region A. A uniform distribution is employed so that a constant node density $\rho = \frac{n}{A}$ can be defined. The node density is a representation of the average number of nodes per unit area. For example, if A was considered to be a unit square then, $\rho = n$.

A wireless sensor network is represented as an undirected graph $G = G(V, E)$ where V represents the set of member nodes in the network and E is the set of edges between nodes that are able to communicate with each other. Undirected graphs are assumed because a unit disk model is assumed for communication, where the existence of a link between any two nodes u and v in the network is dependent on the euclidean distance between them. If $\parallel u - v \parallel \leq r$, then according to this model both u and v are capable of sending and receiving information from each other. r is the transmission radius of the omni-directional antenna in the network nodes. r' is the transmission range of nodes that are capable of hybrid communication.

Theorem 1 *Let $P_{HYB}(d_{min} > 0)$ be the probability that the minimum node degree is greater than 0 for a WSN with hybrid-enabled motes and $P_{OMNI}(d_{min} > 0)$ be that in the case of a WSN with omni-directional antennas.*

Then,

$P_{HYB}(d_{min} > 0) \geq P_{OMNI}(d_{min} > 0)$

Proof

An upper bound can be computed for 100% connectivity by considering the minimum node degree of the graph that is used to represent the network. The upper bound is basically the probability that every node in the graph is connected to at least one other node, which means that the minimum node degree needs to be 1. In other words, the minimum node degree needs to be non-zero.

Thus,

$$P(\text{G has 100\% Connectivity}) \leq P(d_{min} > 0) \tag{4.16}$$

It follows from [32] and [40] that for a network model as is described above the probability mentioned in Eq. (4.16) can computed as

$$P_{OMNI}(d_{min} > 0) = (1 - e^{-\rho\pi r^2})^n \tag{4.17}$$

In Eq. (4.17), ρ is the node density and r is the transmission range for the antenna under consideration. Also, let $P_{HYB}(d_{min} > 0)$ be the above probability for a network graph with each node capable of hybrid communication and $P_{OMNI}(d_{min} > 0)$ be that if each node is only capable of omni-directional communication.

Then, from Eq. (1.3) and Eq. (4.13) it can be directly concluded that

$$P_{HYB}(d_{min} > 0) \geq P_{OMNI}(d_{min} > 0)$$

■

The simulation set up is intended to provide better insights into the relationship between connectivity, beamwidth, node density and transmission radius. The 2-D model for the results shown below is a randomly distributed network of nodes in a unit square. The probability of 100% network connectivity, which guarantees that every pair of nodes can communicate with each other is computed. 1000 random topologies were generated to be able to compute the probability. To understand the relationship with node density and transmission radius empirically, the normalized r was varied between 0 and 0.5 and n, the node density, between 10 and 100. The effects of varying the beamwidth is demonstrated by three configurations, $\pi/6$, $\pi/4$ and $\pi/3$.

From the plots in Fig. 9 and Fig. 10, it is evident that along the lines of the results from the 1-dimensional case, the hybrid communication model out performs a strictly omni-directional model by phenomenal margins.

In the plot that details the probability of 100% connectivity with varying transmission radius it can be noticed that the omni-directional case only hits a non-zero value around a setting for r around 0.3. On the other hand, the hybrid setting at a beamwidth setting of $\pi/6$ has performance at $r = 0.1$ that is almost equivalent to that of the omni-directional case at $r = 0.35$. The difference is less than 2%. It is evident from the probability plot at $r = 0.3$ that the hybrid configuration out performs its omni-directional counterpart by more than 90%. This is very crucial information for WSNs that require limited transmission radius or operation power.

As seen in the plot over the lower transmission radius range, the difference in performance for various antenna beamwidth settings in the hybrid case is sharper at

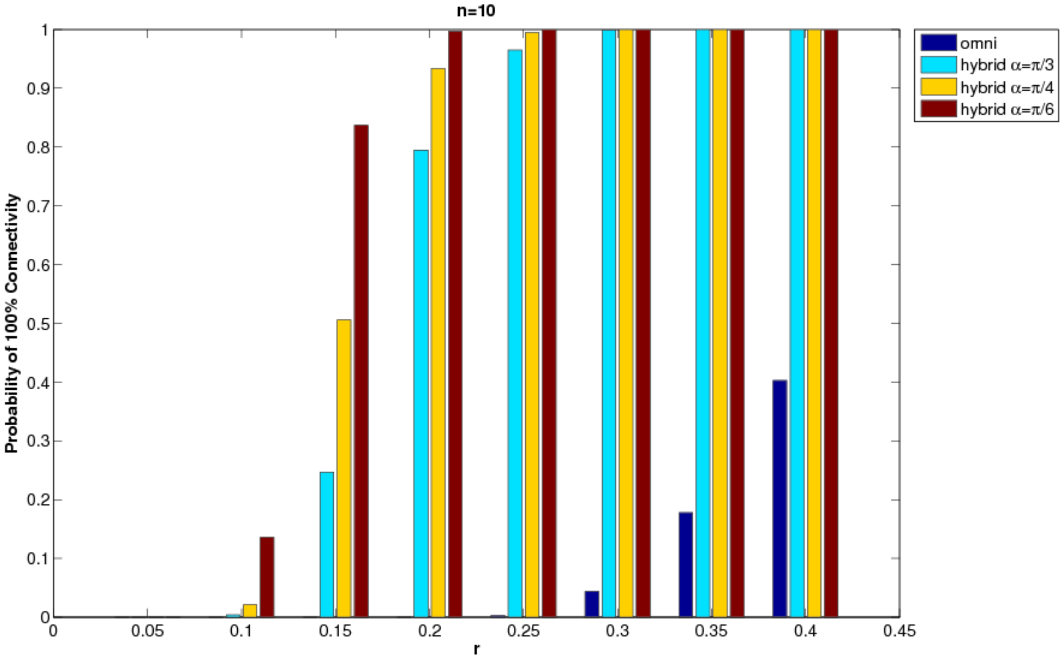


Fig. 9. 2-D Deployment, 100% Connectivity - $\alpha = \pi/3, \pi/4, \pi/6$, r ranges from 0.1 to 1.0, n is constant at 10

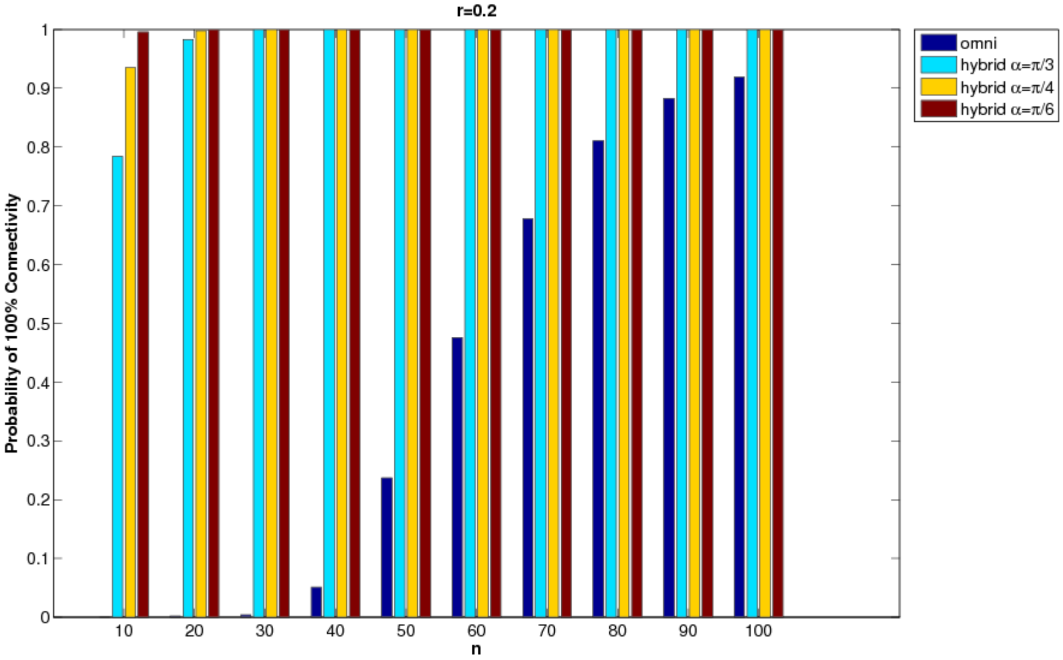


Fig. 10. 2-D Deployment, 100% Connectivity - $\alpha = \pi/3, \pi/4, \pi/6$, n ranges from 10 to 100, r is constant at 0.2

lower transmission radius settings. The benefits of using a very narrow beamwidth hybrid configuration evidently decreases with increasing transmission radii. This is rather intuitive considering n being constant at 10 for the plot in Fig. 9. The number of neighbors possible for each node would only marginally increase at higher transmission radii owing to such a sparse node deployment.

The ratio between r and r' is obtained by substituting for α as required in Eq. (1.3). As can be seen in Table I and Table II, there is a larger difference in the transmission range of varying beamwidths with increasing r. This will be more evident in the case of the varying n plot in Fig. 10.

In Fig. 10, r is set to a constant of 0.2 and the study of the effect of varying node density is done. It can be noticed that with increasing node densities, all communication models move towards a very high probability (close to unity) of 100% connectivity. Again, this is rather intuitive as with increasing node density, the average distance between any two nodes in the deployment reduces thus making it easier to achieve better connectivity with low transmission radii. In terms of improvements via the hybrid approach, it is interesting to note that at very low node densities of 10, 20 and 30, the least expensive hybrid configuration of $\pi/3$ out performs the traditional omni-directional approach by between 80 and 90%.

It is rather interesting to note that the hybrid configurations stay at a consistent probability of unity from a node density as low as 30. The omni-directional case on the other hand climbs slowly to around 88% only at a node density of 100. This suggests that there might be other gains that the hybrid approach brings beyond the node density setting of 30. These effects in terms of k-connectivity and the availability of multiple disjoint and independent paths will be studied in a later section.

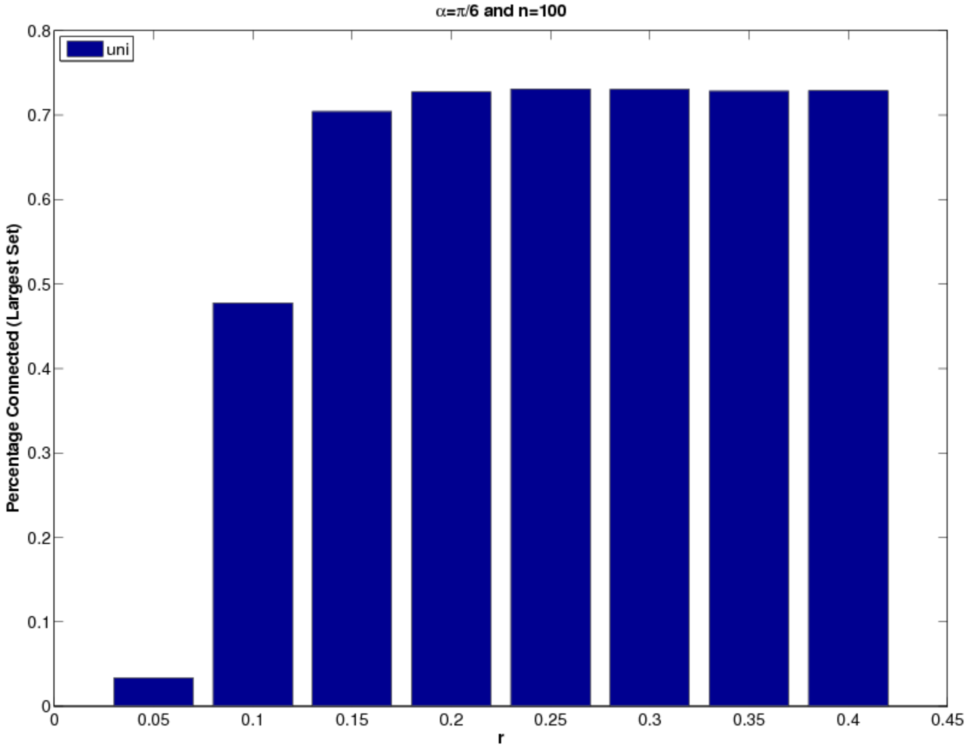


Fig. 11. Uni-directional Network with constant n 100

b. Uni-Directional WSNs

To elaborate on the degree of improvements obtained from a hybrid approach, in this section simulation results on connectivity for WSNs that have sensor motes that are equipped only with uni-directional antennas for communication are presented.

The simulation setup for the following results are exactly similar to the previous section. The only difference being that each mote is capable of uni-directional communication in one sector only. There will be a constant antenna beamwidth for all the deployed motes, although the orientation of each mote will be random. The relationships between the normalized transmission radii for r and r' remain as described in Table I and Table II.

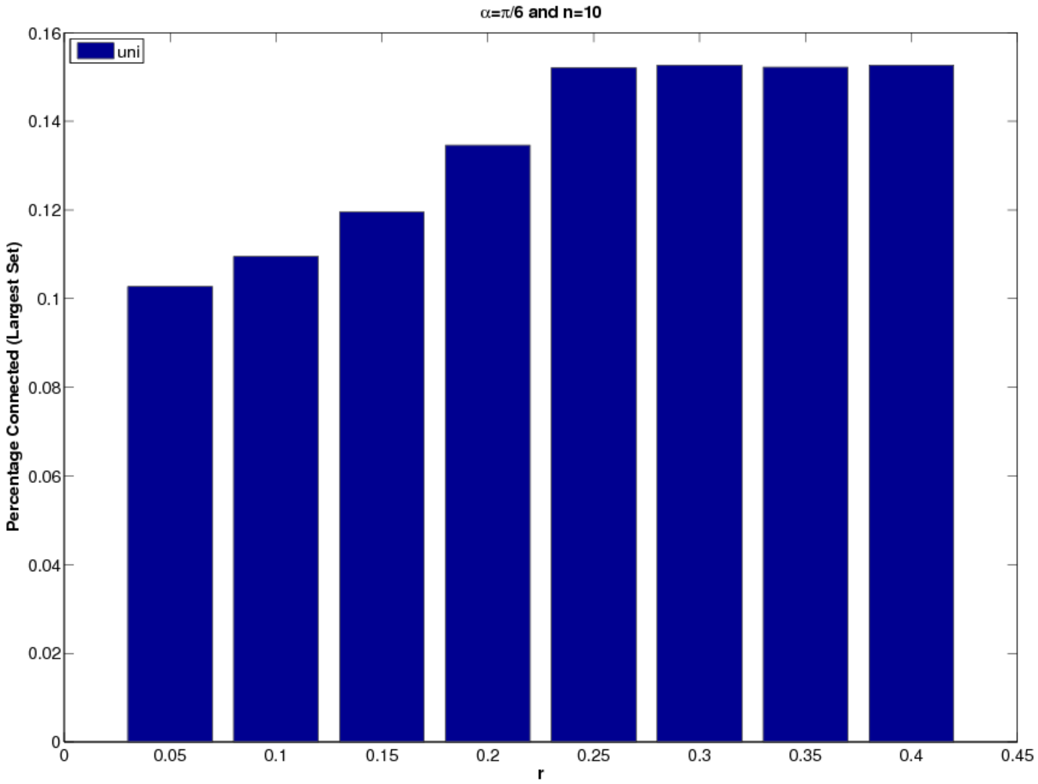


Fig. 12. Uni-directional Network with constant n 10

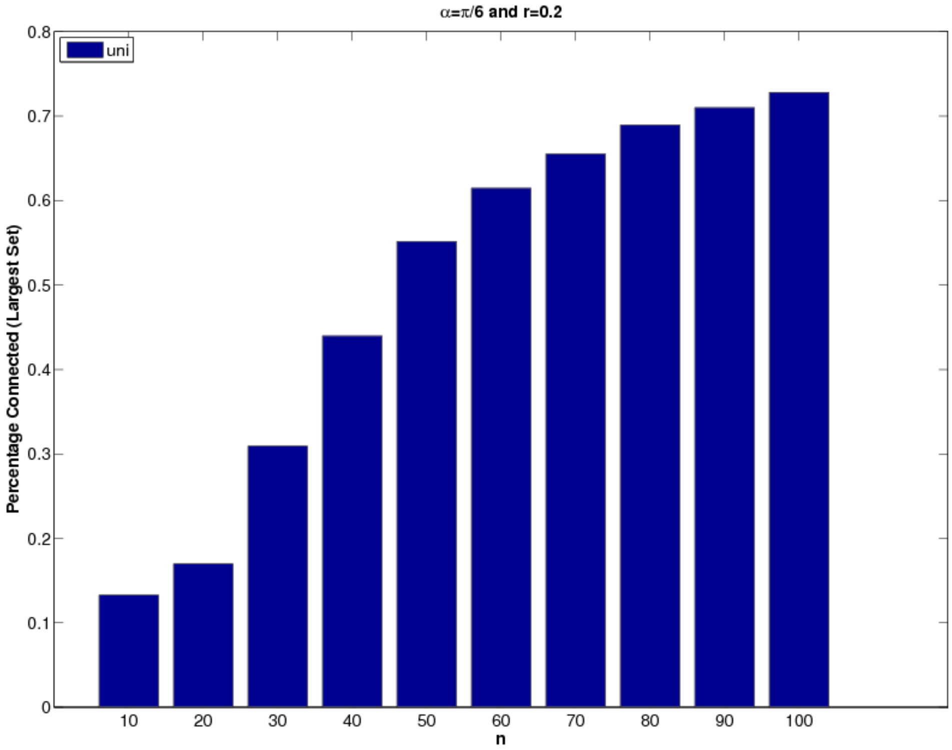


Fig. 13. Uni-directional Network with constant r 0.2

It is interesting to note that in the direction of the work presented in this thesis, the concentration and emphasis on low node densities and transmission radii would mean that a uni-directional WSN would require very large node densities to be able to generate non-zero probabilities of 100% connectivity. For this reason, the plots in Fig. 11 - Fig. 13 use the metric *Percentage Connected*, which represents the largest connected subset of nodes from the entire deployment as a percentage. For example, if from a deployment of 10 nodes, via uni-directional WSNs the largest connected component has say, 4 nodes, then the percentage is 40%.

From Fig. 11, it can be noticed that for a strictly uni-directional WSN with a constant node density n at 10, the largest connected subset of nodes varies between a little over 10% at a transmission radius r of 0.05. For the same set of transmission radii, but an increased constant node density of n set to 100, it can be seen that the largest set percentage improved drastically to vary between close to 50% at a transmission radius of 0.1 to more than 70% that is consistent from a transmission radius of 0.2 on.

Finally, Fig. 13 presents the rather linear improvement of the metric considered with increasing node densities and a constant transmission radius of 0.2. In keeping with the theme of the work presented in this thesis, only results from low node densities have been described.

3. k-Connectivity and Disjoint Path Analysis

In this section, analysis and simulation describe the performance of the hybrid approach as a communication model in WSNs in the area of k-connectivity and availability of disjoint paths. The graph theoretic definitions for k-connectivity were briefly described previously.

From the perspective of a communication network and WSNs, there is interest in providing multiple disjoint, mutually independent paths for each node to communicate with the sink or data collection center. The simulation results presented in this section do not consider the existence of multiple paths between all pairs of nodes, but only between each node and a centrally located sink. The motivation for such an approach is the typical traffic model for WSNs being source-to-sink as described earlier.

The network model for the results presented in this section are exactly similar to that in Section a.

The interest of the following analysis is to prove that the hybrid communication model which involves using sensor motes capable of omni-directional and sectorized uni-directional transmission is capable of superior performance when compared to a network using motes that only have omni-directional capability.

Lemma 3 *For a random undirected graph of n nodes if edges are added to the empty graph in an order chosen randomly and uniformly from the $\binom{n}{2}!$ possibilities, then almost surely the graph that results from the edge additions becomes k-connected when it achieves a minimum degree of k. For large n,*

$$Prob(G \textit{ is } k\textit{-connected}) = Prob(d_{min} \geq k) \tag{4.18}$$

where d_{min} is the minimum degree (defined in previous sections) per node.

The above has been proved for random graphs in [41] and [40] for graphs with pathloss models.

For the interest of this thesis in WSNs with low node densities, an upper bound for a probability of k-connectivity is computable by considering the probability that the minimum degree of each node in the network graph is greater than or equal to k. In topological terms, this is equivalent to every node in the network having n_{neigh}

neighbors such that $n_{neigh} \geq k$. Thus, the probability of $d_{min} \geq k$ would give the upper bound that is needed.

Results for the same exist in [32] in the context of wireless multi-hop networks with nodes capable of omni-directional communication. Following the nearest neighbor methods approach employed in that work and using standard graph theoretical results the upper bound can be computed.

Theorem 2 *If $P_{HYB}(d_{min} \geq k)$ if the probability of the average minimum degree being greater than k for a network with hybrid-enabled motes and $P_{OMNI}(d_{min} \geq k)$ was that for an omni-directional network then,*

$P_{HYB}(d_{min} \geq k) \geq P_{OMNI}(d_{min} \geq k)$

Proof

The minimum degree probability as a function of node density and transmission radius is known from [32].

$$P_{OMNI}(d_{min} \geq k) = \left(1 - \sum_{N=0}^{k-1} \frac{(n\pi r^2)^N}{N!} \cdot e^{-n\pi r^2}\right)^n \tag{4.19}$$

Here $\rho = n$, since by definition $\rho = \frac{n}{A}$ but in this case $A = 1$.

The approximation for computing the required bounds for k-connectivity via computing the probability for a minimum degree requirement on each node is expressed below.

$$P(\text{G is } k\text{-connected}) \leq P(d_{min} \geq k) \tag{4.20}$$

As justified earlier, the use of the hybrid approach enables activation of all sectors, thus extending the reach of the sensor mote along all directions. While analytically evaluating this approach, the capability of all sectors to be activated depending on uni-cast traffic awaiting transmission helps extend Eq. (4.19) by substituting for the transmission radius r with r' in accordance with the relationship in Eq. (1.3). In the following equations, the minimum degree probability in the omni-directional is denoted by $P_{OMNI}(d_{min} \geq k)$ and in the hybrid case as $P_{HYB}(d_{min} \geq k)$. Eq. (4.19) can now be re-written as,

$$P_{HYB}(d_{min} \geq k) = \left(1 - \sum_{N=0}^{k-1} \frac{(n\pi r'^2)^N}{N!} \cdot e^{-n\pi r'^2}\right)^n \tag{4.21}$$

Using Eq. (1.3) substituting r' as $r\sqrt{\frac{2\pi}{\alpha}}$ so that

$$\begin{aligned} P_{HYB}(d_{min} \geq k) &= \left(1 - \sum_{N=0}^{k-1} \frac{(n\pi \frac{2\pi}{\alpha} r^2)^N}{N!} \cdot e^{-n\pi \frac{2\pi}{\alpha} r^2}\right)^n \\ &= \left(1 - \sum_{N=0}^{k-1} \frac{(\frac{2n\pi^2 r^2}{\alpha})^N}{N!} \cdot e^{\frac{-2n\pi^2 r^2}{\alpha}}\right)^n \\ &= \left(1 - \sum_{N=0}^{k-1} \frac{(2n\pi^2 r^2)^N}{\alpha^N N!} \cdot e^{\frac{-2n\pi^2 r^2}{\alpha}}\right)^n \end{aligned} \tag{4.22}$$

From Eq. (1.3), Eq. (4.13) and with the expansion in Eq. (4.22) it can be concluded that,

$$P_{HYB}(d_{min} \geq k) \geq P_{OMNI}(d_{min} \geq k) \tag{4.23}$$

■

The hybrid case is equivalent to the omni-directional case when hypothetically, a beamwidth setting of 2π is used. For all other settings, the hybrid case will thus have a higher probability of disjoint paths in the network deployment.

The simulations below explicitly support this claim. The nodes are assumed to be static, with uniform random distribution and capable of both omni-directional and directional communications. Directional communications is modeled via sectorized uni-directional antennas, dividing the entire omni-directional region of 2π radians into a number of sectors according to the antenna beamwidth. Each sector can be activated, one at a time so that at any instant the node may appear to be equivalent to a uni-directional antenna and that reception is omni-directional. In the omni-directional mode, each node is capable of transmitting at a radius r. When switched to the uni-directional mode, each node is capable of transmitting at a radius r' related to r by Eq. (1.3), in each sector.

The results shown below are based on a randomly distributed network of nodes in a unit square. There is a centrally located sink at coordinates (0.5, 0.5). The interest of these simulations is in studying the effect of node density, transmission radii and uni-directional antenna beamwidth on the k-connectivity of a randomly deployed network of sensor nodes. The attempt begins by computing the probability of 2-connectivity, or the probability that every node in the network deployment will have at least 2 disjoint mutually independent paths to the centrally located sink. 1000 random topologies were generated to be able to compute the probability. Mutually independent paths are computed using standard disjoint path algorithms, using min-cut/max-flow techniques and link reversals that provide optimal sets of disjoint paths as mentioned in [42] and [43]. To understand the relationship with node density and transmission radius empirically, the normalized r was varied between 0.05 and 0.45 and n, the node density, between 10 and 100. This is basically the probability of 2-connectivity. The effects of varying the beamwidth from $\pi/6$ to $\pi/3$ was also demonstrated by appropriate configurations for the simulations. These plots are shown below.

Fig. 14 and Fig. 15 describe the probability of 2-connectivity over varying transmission radii, node density and antenna beamwidth.

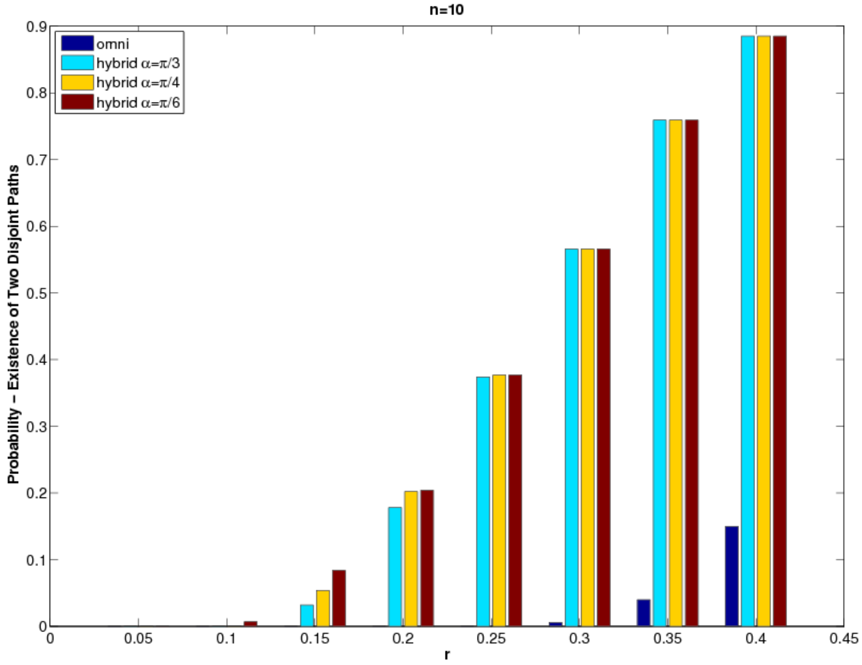


Fig. 14. Probability of Existence of Two Mutually Disjoint Paths for All Nodes in the Network- Varying Transmission Radius r

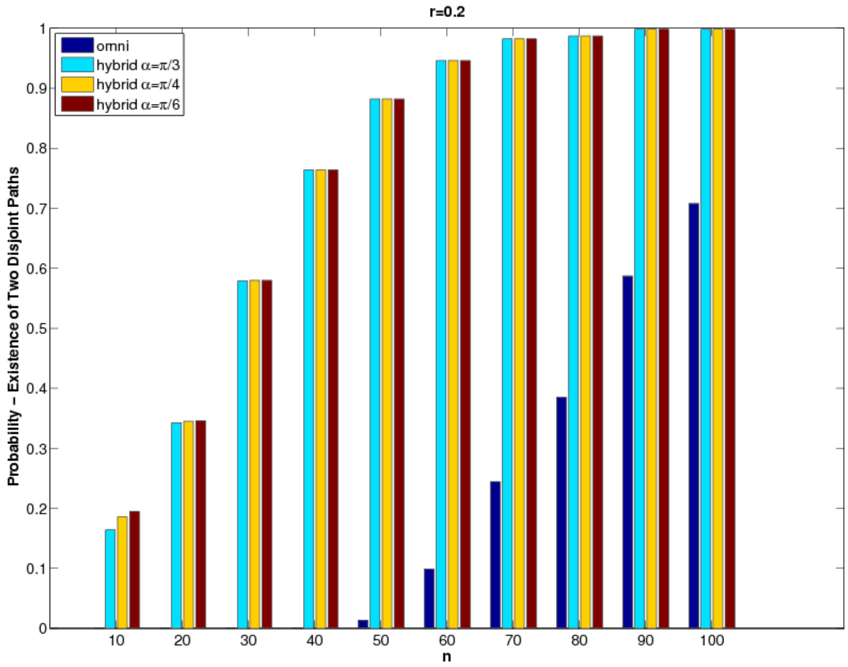


Fig. 15. Probability of Existence of Two Mutually Disjoint Paths for All Nodes in the Network- Varying Node Density n

It can be seen from the first plot with a constant n and varying r that again, the hybrid approach provides a very substantial non-zero probability even between the lower transmission radii settings of 0.15 and 0.25. At a setting of 0.25, the hybrid approach out performs the omni-directional setting by almost 40%. When the operational transmission radius is set to a high 0.4, the improvement is almost around 80% as can be seen.

The second plot in Fig. 15 describes the effect of varying node density n for a constant r of 0.2. Intuitively with increasing node density, the omni-directional setting is able to climb to higher probabilities, as seen for the maximum node density of 100 that is considered for these simulations, the probability for an omni-directional configuration reaches around 0.7. In contrast, the hybrid approach was at a probability of more than 0.7 around a node density of just 40. This emphasizes on the improved performance available when the hybrid approach is employed even at lower node densities. At the interim node density of 50, the hybrid approach out performs an omni-directional only setting by more than 90%.

To further demonstrate the improvements in terms of the availability of disjoint paths for each node, another set of simulations are presented that use the metric *Average Number of Disjoint Paths for the Network.* This metric represents the average number of paths all member nodes in the network deployment possesses towards the centrally located sink.

Results for varying n and r are presented in Fig. 16 and Fig. 17. For the first plot, a very low node density of $n = 10$ was considered. 10 nodes distributed over a unit square, is usually a very sparse deployment even for a normalized radius of say, 0.2 for an omni-directional configuration. Interestingly enough, the hybrid setting with r at 0.2, meaning that for $\alpha = \pi/6$, r' is around 0.69, the average number of

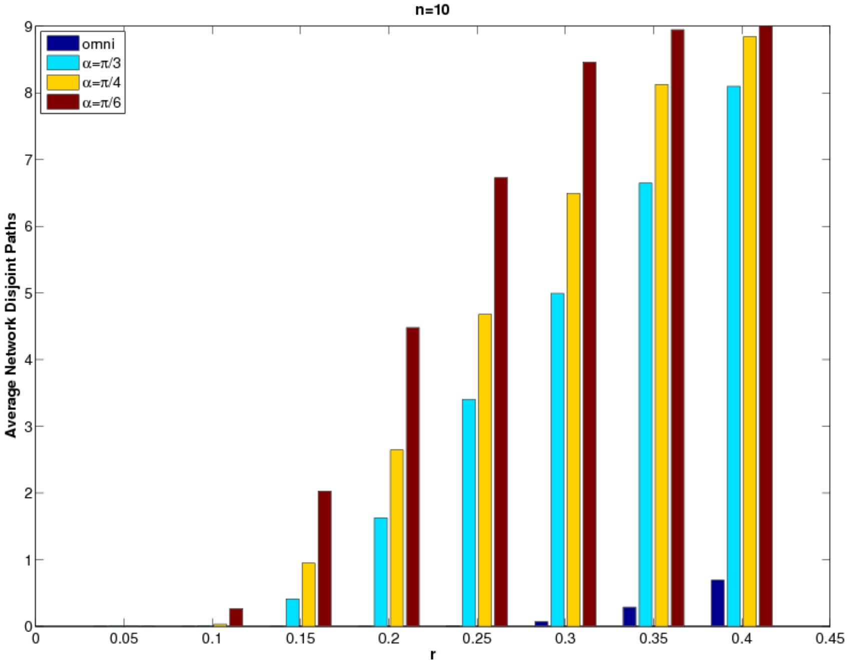


Fig. 16. Average Number of Mutually Disjoint Paths for All Nodes in the Network - Varying Transmission Radius r

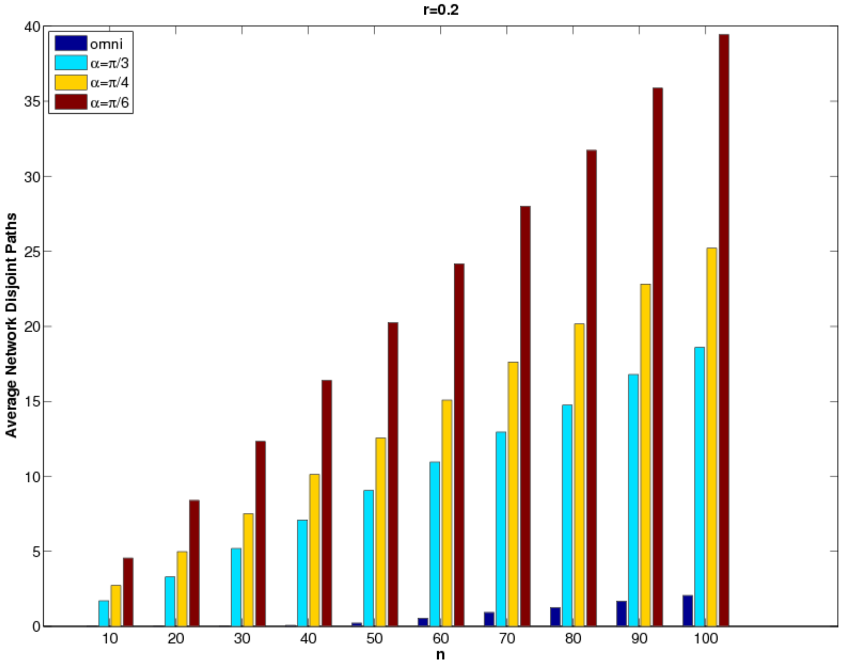


Fig. 17. Average Number of Mutually Disjoint Paths for All Nodes in the Network - Varying Node Density n

disjoint paths was around 7. For the omni-directional setting, the network was able to even reach 1-connectivity.

For varying n, there is an almost linear relationship in terms of the incremental gains achievable from using the hybrid approach. At the maximum setting of node density 100, the hybrid approach provides around 17, 25 and 40 disjoint paths on an average for the network at the beamwidth settings of $\pi/3$, $\pi/4$ and $\pi/6$ respectively. The omni-directional setting even at the maximum node density of 100 could barely make an average value of around 3 mutually independent paths.

C. Security Improvements via the Hybrid Approach

Network security is often as important as performance depending on the constraints under which the elements of the network are expected to function in a desirable manner. Securing a sensor network is very crucial to maintain the purpose of an installation, ensuring the capability of member nodes to report activity without any hindrance and disallowing non-member entities from obtaining sensed data.

In most critical environments, security of a deployed network is of utmost importance. A network is most secure when its member nodes cannot be compromised, messages exchanged cannot be deciphered by non-member nodes and the none of the links can be disabled by an adversary, even for a short duration of time. Network availability and reliability are frequent targets for adversaries who intend to deem the deployment incapable according to the requirements of the attack.

A variety of routing attacks on wireless sensor attacks are mentioned in [6]. An interesting area of sensor networks and communication networks in general is securing the deployment from *Denial-of-Service* (DoS) attacks [8]. Consideration of security issues during the design stage of sensor network protocols is necessary to keep the networks from being vulnerable to DoS attacks.

Yet another attack [6] [8] that is of interest to WSNs is the *Network Partition* attack. The approach towards both of the above-mentioned attacks are similar in that the adversary is interested in disabling links and nodes, eventually contributing to the success of the respective attacks.

In this section, analysis and simulation results are presented to prove the improved resilience of the hybrid approach against these attacks.

1. Concentrated Collision/DoS Attacks in WSNs

a. Introduction

A DoS attack is an attempt by an adversary or group of attacking adversaries to disable normal communications in a network by making resources unavailable to elements in the network. DoS attacks against sensor networks are usually the most crippling and are also the most complicated to devise countermeasures against to improve resilience. The interesting nature of such attacks is that an ongoing attack often goes undetected as the misbehavior perceived at each node is very subtle and could be misinterpreted by the unsuspecting member node as being caused by network and environmental conditions like poor link quality and traffic congestion.

In the context of WSNs, a specific type of DoS attack involves attacks based on collisions and interference at the transmission medium. This is sometimes referred to as a *MAC Collision Attack*, referring to the Medium Access Control layer in the network protocol stack or also the *Link-layer Collision Attack*.

The link-layer collision attack involves an adversary inducing a collision (even over one octet of a transmission) by broadcasting junk data to disrupt packets being transmitted over a channel. An attack of this kind is most effective in networks using cooperative scheduling schemes relying on carrier sense at the link layer, which are essentially contention based transmission scheduling schemes.

The effect of a collision attack on a network deployment is two-fold. Firstly, as the adversary only needs to cause collisions for a short duration to damage an entire frame, errors in reception increase at receiving nodes. Error correcting codes have been previously suggested as a countermeasure, although its use is usually more suitable for errors caused due to the time-varying characteristics of wireless channels, where there an upper bound on the variation in channel quality can be guaranteed. Attacking adversaries will intend to work towards corrupting more data than the network can correct [8]. Secondly, a naive MAC layer would repeatedly attempt retransmission ultimately leading to the exhaustion of battery resources at a node, leading to drastic effects on network connectivity.

In this section the benefits of using a hybrid communication model and more specifically the gains are analyzed by considering the metric of the *Probability of Successful Attack*.

b. Network Model

Network model considered is identical to previous sections. Node deployment is considered to be random and following a uniform distribution. Nodes are also static and no form of mobility is assumed. The node deployment is assumed to be within a unit square with a centrally located sink at $(0.5, 0.5)$. The channel is assumed to be symmetric such that if node x can reach node y through signal transmission then node y can also reach node x. Each node is capable of either omni-directional communication with a range r or of hybrid communication with a range r'. The relationship between

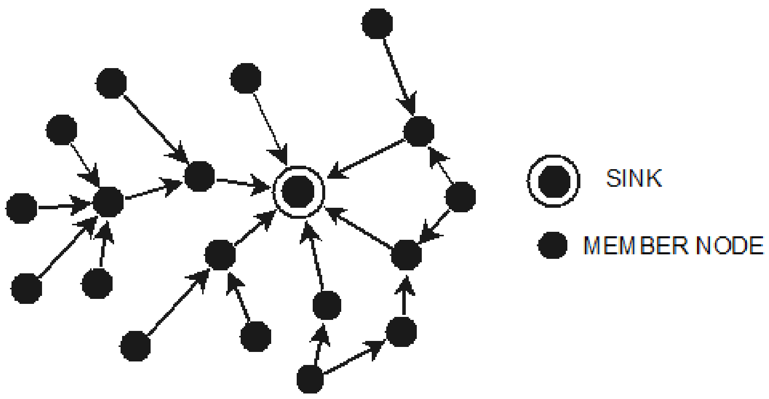


Fig. 18. Network Deployment Example

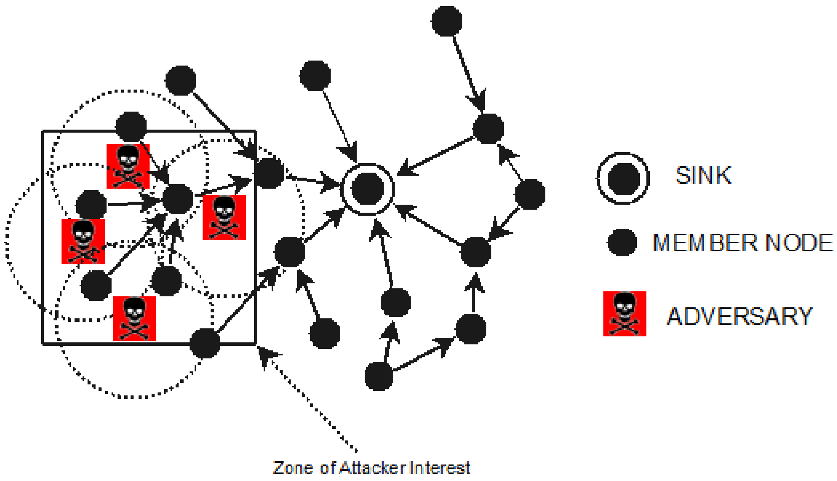


Fig. 19. Network Attack Scenario - Concentrated Collision Attack

r and r' is as described in Eq. (1.3). n member nodes are randomly and uniformly distributed over the unit square.

Fig. 18 shows an example of such a network deployment. This deployment may be considered as enclosed in a unit square.

c. Threat Model

The attacking adversary launches a covert attack on a WSN deployment by occasionally broadcasting junk data that causes collisions at the MAC layer for protocol-abiding sensor nodes. The collisions induce *Layer 2* retransmissions and subsequent malicious broadcasts will work towards draining out a member nodes battery and the eventual disconnection of the network.

An adversary needs to only be active for a small ratio of the total transmission duration for a link layer frame to get corrupted such that it will invoke a retransmission from the layers below. It is to be noted that even without the potential draining out of a member node such attacks cause considerable damage to the normal functioning of a network.

The specific attack of interest to the work in thesis is graphically described in Fig. 19 where an adversary is interested in disabling communication for a subset of the original n nodes deployed. This is a very crucial attack as the adversaries are interested in performing activity in a small region that is part of the unit square which is the environment of interest.

As seen in Fig. 19, the attacking adversary nodes are deployed in a smaller region, which is assumed to be a square of side d such that $0 < d < 1$. A total of m such malicious nodes will be deployed in the smaller region, the *Zone of Attacker Interest*. The intention of the adversary nodes is to disable the capability of nodes within the interest zone to report sensed information to a centrally located sink. Each of the adversary nodes is capable of omni-directional transmission with a maximum range of r.

In Fig. 20, the effect of the adversaries are seen in terms of the disabled links within the attacker's zone of interest. Any link that is entirely within the transmission

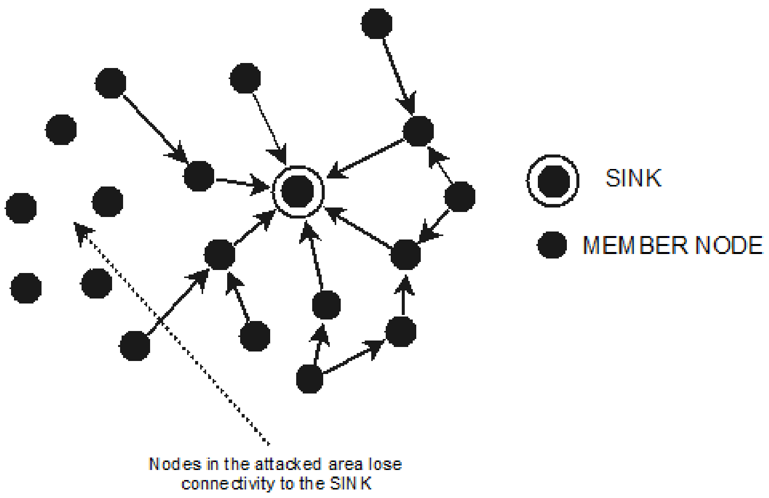


Fig. 20. Network Connectivity Post-Attack

range of any of the m attacking adversaries is disabled. Intuitively, the larger the number of adversaries inside the zone of interest, there will be more links disabled.

The zone of interest of the attacker is assumed to a remote area away from the sink. Attacking a network near the sink would compromise the covertness of the attack and hence lead to early detection. Therefore, the attacked area is assumed to be a smaller square that will not include the sink.

d. Metric of Comparison

The metric of comparison that will be used is the *Probability of Successful Attack*. The adversary is modeled as using m attacking malicious nodes and these nodes will be deployed in a square of side d as described earlier. The attack is deemed successful if all original member nodes within the small square, in the zone of interest have all their paths towards the sink broken.

e. Attack Analysis

Mathematical analysis and simulation results are now presented to prove the improved resilience against such an attack by using the hybrid communication model.

Theorem 3 *If a WSN deployment, where n member nodes are randomly and uniformly distributed inside a unit square. Each of the n nodes has a transmission range r_0, where r_0 can be r or r' depending on the communication model chosen, omnidirectional or hybrid respectively. Let $|A_{attack}|$ be a randomly chosen square with side d such that $0 < d < 1$. Let m attacking adversary nodes be deployed randomly and uniformly inside $|A_{attack}|$ such that each malicious node has a transmission range r. The adversaries intend to damage the network within $|A_{attack}|$ with a collision attack.*

Then,

The success of the attack is dependent on n, m, r_0 and d and it is decreasing in n, d, r_0 and increasing in m.

Proof

Let $G(V, E)$ be a geometric undirected random graph that is k-connected. This means that there exists at least k mutually independent disjoint paths between every pair of member nodes say u and v.

n member nodes are randomly and uniformly distributed in a unit square, forming the network deployment. A square of dimensions $d \times d$ is randomly placed in the unit square. d is such that,

$$0 < d < 1 \tag{4.24}$$

The smaller square is denoted as $|A_{attack}|$, which is the *Zone of Interest* for the adversary. $|A_{attack}|$ represents the area of interest for the attacker. m adversary nodes are deployed randomly and uniformly in $|A_{attack}|$, such that,

$$1 < m < n \tag{4.25}$$

Each of these m nodes are programmed to induce interference over a disk of radius r, which is the omni-directional transmission range. Any link between two nodes that are within the interfering region of any of the m adversary nodes will be disabled owing to the continuous broadcast of junk data by the adversary nodes. This means that either node on the edge could be within the transmission ranges of different adversary nodes. The entire length of the edge need not be within the adversary's range of transmission. It is assumed that,

$$r \ll d \tag{4.26}$$

As the n original member nodes were deployed randomly and uniformly in the unit square and since the $d \times d$ square, region $|A_{attack}|$ was also chosen randomly it can be stated that with a high probability,

$$s = \left\lfloor n \cdot d^2 \right\rfloor \tag{4.27}$$

s in Eq. (4.27) represents the number of original member nodes in the region $|A_{attack}|$. It is to be noted that for a general distribution of nodes in a given area, then the above equation would be modified so that the node density ρ would be used instead of n.

Each of the adversary nodes affect a disk area centered at this nodes of radius r. The probability that one of the s nodes in $|A_{attack}|$ actually falls within the transmission range of the disk of radius r centered at the adversary can be computed as below.

$$p = \frac{\pi r^2}{d^2} \tag{4.28}$$

In Eq. (4.28), it can be seen that d^2 is the area of $|A_{attack}|$ and πr^2 is the area of interference for each of the adversary nodes.

It is of the interest of this section to provide an upper bound for the probability that an attack launched with m adversary nodes is successful. The computation of this probability can be approximated as the probability for all of the s original member nodes that are inside the region $|A_{attack}|$ to have all of their k links broken. More specifically, in the region of the interest, the original member nodes may be either connected or disconnected. If they are connected they have at least one path towards the sink. Also, either all nodes have *at least* one path to the sink or there is *at least* one node that has no path towards the sink. This gives,

$$\begin{gathered} P(\text{All nodes have at least 1-connectivity}) = \\ 1 - P(\text{At least one node has no connectivity}) \end{gathered} \tag{4.29}$$

Now, by Eq. (4.20), the probability that an original member node has all k paths to the sink broken can be approximated to the probability that this node has k neighbors in the transmission range of an adversary node. Now the probability of having more than k points inside the transmission range of an adversary is given by the binomial formula ,

$$\gamma := \sum_{h=k}^{s} \binom{s}{h} p^h (1-p)^{s-h} \qquad \text{where} \quad s = \lfloor n \cdot d^2 \rfloor \quad \text{and} \quad p = \frac{r^2 \pi}{d^2} \tag{4.30}$$

Eq. (4.30) represents the probability with the presence of one adversary node. Since there are m adversary nodes and these were chosen randomly and independently in the region $|A_{attack}|$ with $r \ll d$ then the probability that the original member node inside this region is still at least 1-connected and the node remains secure becomes,

$$P_{SECURE} := (1-\gamma)^m \tag{4.31}$$

Similarly, the probability that the original member node is disconnected and hence attacked becomes,

$$P_{ATTACKED} := 1 - (1-\gamma)^m \tag{4.32}$$

From Eq. (4.30), Eq. (4.31) and Eq. (4.32) the following equations may be derived.

$$P_{SECURE} = \left(\sum_{h=0}^{k-1} \binom{s}{h} p^h (1-p)^{s-h} \right)^m \qquad \text{where} \quad s = \lfloor n \cdot d^2 \rfloor \quad \text{and} \quad p = \frac{\pi r^2}{d^2} \tag{4.33}$$

$$P_{ATTACKED} = 1 - \left(\sum_{h=0}^{k-1} \binom{s}{h} p^h (1-p)^{s-h} \right)^m \qquad \text{where} \quad s = \lfloor n \cdot d^2 \rfloor \quad \text{and} \quad p = \frac{\pi r^2}{d^2} \tag{4.34}$$

It is to be noted from the above equations that $P_{ATTACKED}$ depends on m, d, r_0 and n in a very interesting fashion. From Eq.(4.19) and Eq.(4.22), it can be deduced

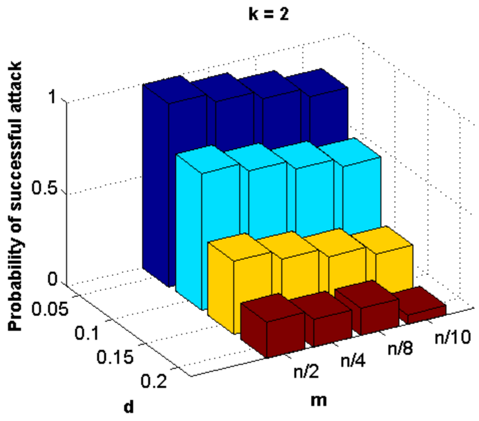


Fig. 21. Attack Probability for Low k

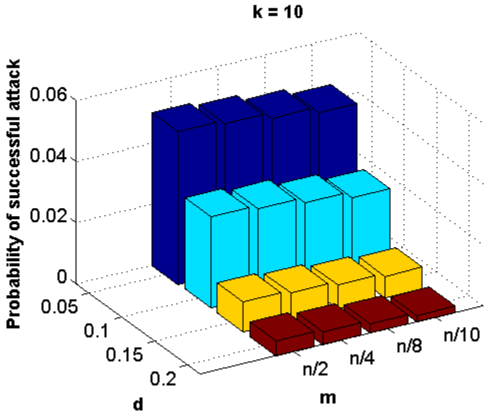


Fig. 22. Attack Probability for High k

that k is larger for larger n and r_0. From Eq.(4.34) it can be deduced that with a larger k the attack is less successful. Thus, the attack success decreases in n and r_0.

Also, in Eq. (4.34), p is dependent on d. This dependence shows that the success of the attack decreases with increasing d. Also, $P_{ATTACKED}$ increases with m.

Thus, the success of the attack is dependent on n, m, r_0 and d and it is decreasing in n, d r_0 and increasing in m.

The Eq. (4.34) was plotted for fixed values of n and r and setting the value of k to low and high configurations corresponding to the difference between omni-directional and hybrid deployments. The general trend followed by the analysis can be seen in Fig. 21 and Fig. 22.

The simulation set up for this problem is similar to what was described in Sec. b. n nodes are uniformly and randomly distributed over a unit square. A smaller square $|A_{attack}|$ is randomly chosen for every run with a side d. m adversary nodes are randomly and uniformly distributed over this region, which is the attacker's region of interest. m is chosen as a fraction of n and is varied as $\frac{n}{2}$, $\frac{n}{4}$, $\frac{n}{8}$ and $\frac{n}{10}$.

Once the network is set up and all network paths are established, the adversary nodes are dropped. All affected links will be removed and the network paths are established again with the updated graph. If all original member nodes within the region $|A_{attack}|$ lose all paths towards the sink, then the attack is deemed successful. The probability of such an attack being successful is computed over 1000 random realizations of deployments.

The plots in Figs. 23 - 26, show the probabilities of successful attacks when an omni-directional antenna based sensor network deployment is used. It can be seen that the primary dependence of the probability of attack success is on d and m. This is intuitive as the smaller the region $|A_{attack}|$ is, the density of the attacking adversary nodes in that region increases. The general trend noticed is that with increasing d, the probability of successful attack increases. When m increases, there is an increased density of adversary nodes in the area of interest, increasing the probability of the network being attacked again. This is also seen as a general characteristic from the plots.

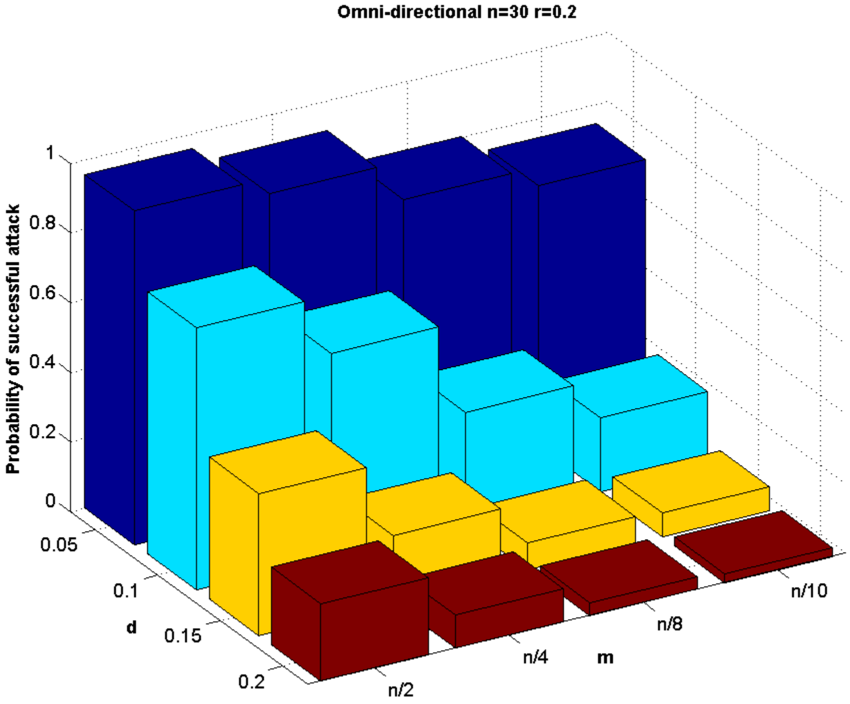


Fig. 23. DoS-Collision Attack: Node Density - 30, Transmission Radius - 0.2, Antenna Setting - Omni-Directional

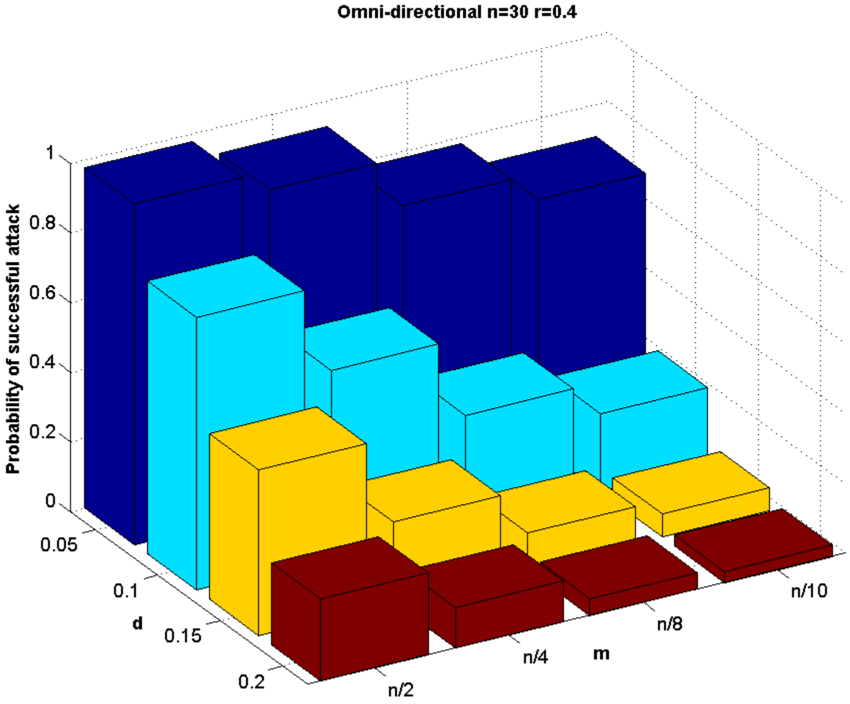


Fig. 24. DoS-Collision Attack: Node Density - 30, Transmission Radius - 0.4, Antenna Setting - Omni-Directional

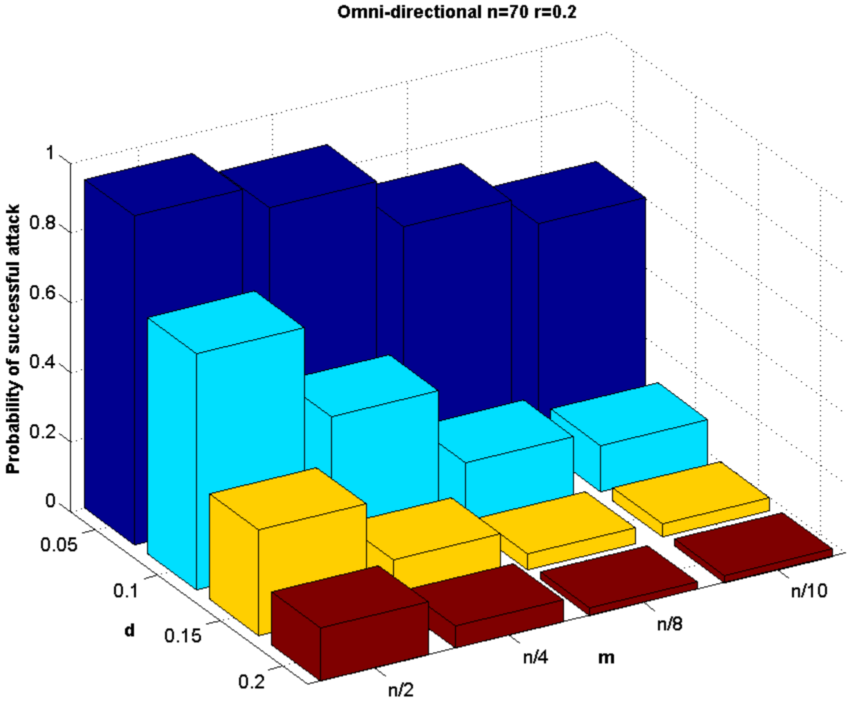


Fig. 25. DoS-Collision Attack: Node Density - 70, Transmission Radius - 0.2, Antenna Setting - Omni-Directional

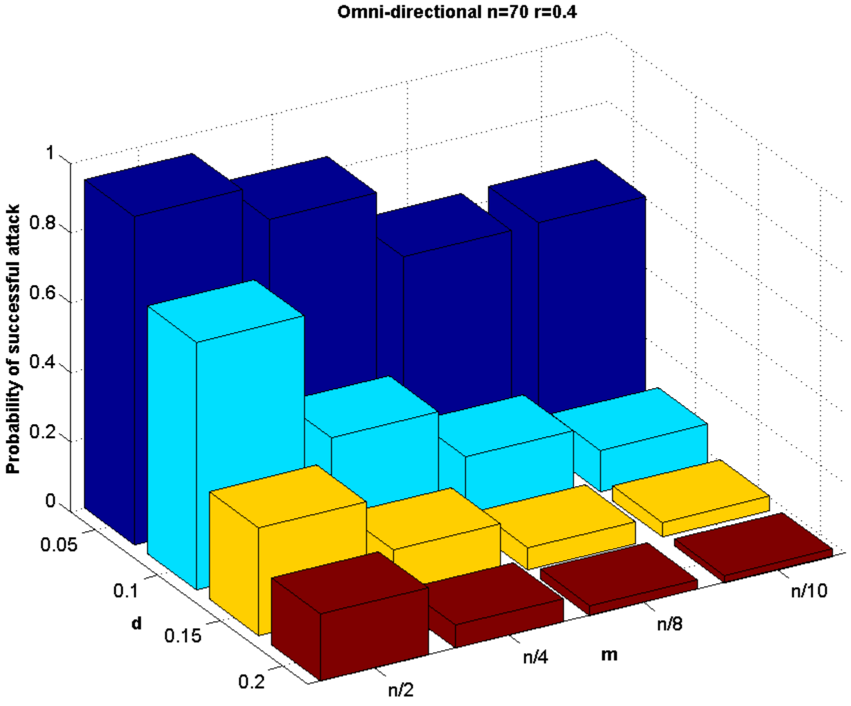


Fig. 26. DoS-Collision Attack: Node Density - 70, Transmission Radius - 0.4, Antenna Setting - Omni-Directional

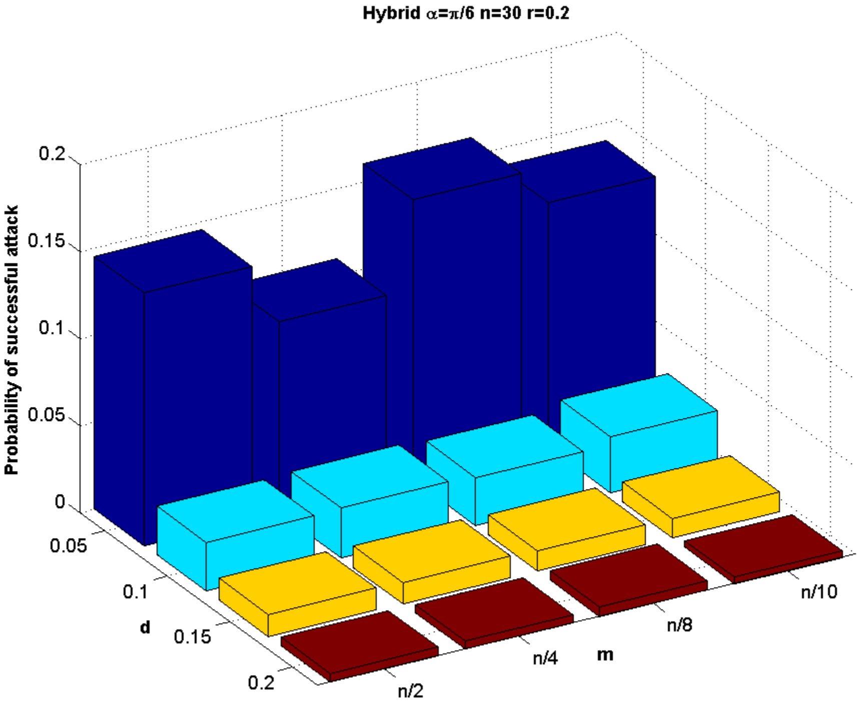


Fig. 27. DoS-Collision Attack: Node Density - 30, Transmission Radius - 0.2, Antenna Setting - Hybrid $\pi/6$

It can be seen that on an average, for the range of parameters considered, the attack will be most successful at a setting of $d = 0.05$ and $m = \frac{n}{2}$ with a probability very close to 1. With increased node density n, the probability reduces.

In Figs. 27 - 30 the improvements with the hybrid approach are clearly visible. It is noticed that at the worst case of $d = 0.05$ and $m = \frac{n}{2}$, the hybrid model, shown in these plots with a setting of $\pi/6$, the probability of successful attack is reduced to as low as just a little less than 0.15 for the case when the node density n is 30. The effect of increased node density is understood from the simulations for the case of the node density n set to 70. As m stays the same, increased node density for the original member node deployment would mean that more nodes would be present inside the

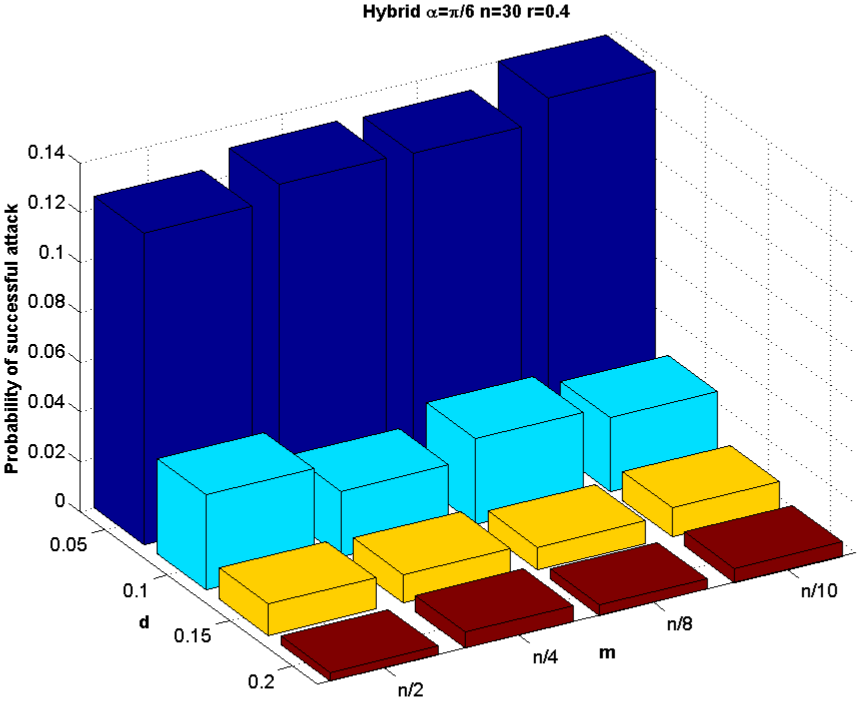


Fig. 28. DoS-Collision Attack: Node Density - 30, Transmission Radius - 0.4, Antenna Setting - Hybrid $\pi/6$

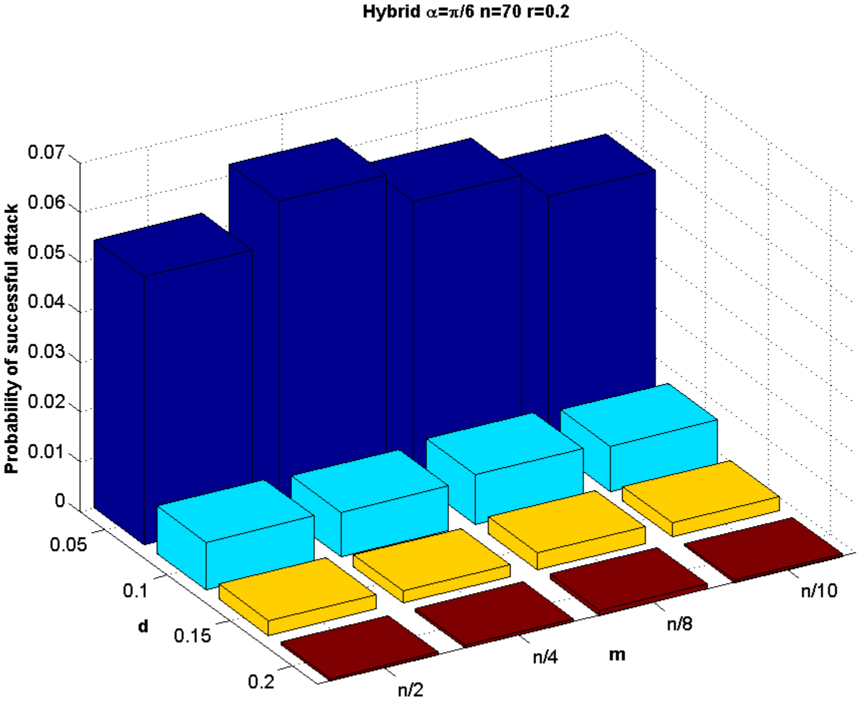


Fig. 29. DoS-Collision Attack: Node Density - 70, Transmission Radius - 0.2, Antenna Setting - Hybrid $\pi/6$

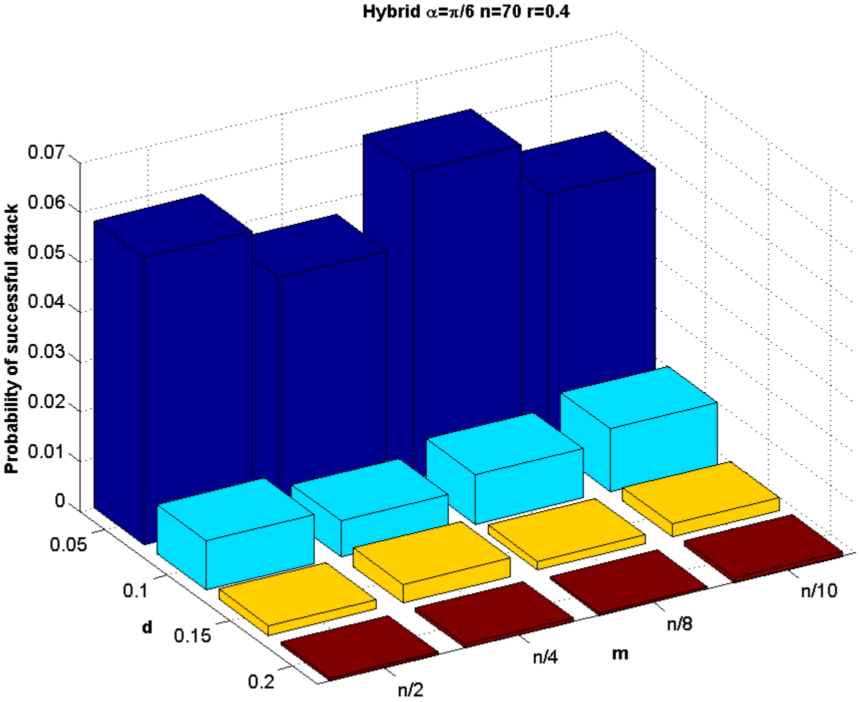


Fig. 30. DoS-Collision Attack: Node Density - 70, Transmission Radius - 0.4, Antenna Setting - Hybrid $\pi/6$

smaller square or $|A_{attack}|$. When the node density is 70, the probability of attack success at the worst case of $d = 0.05$ decreases to 0.05.

2. Network Partition Attacks in WSNs

a. Introduction

Network partition attacks are a class of attacks that is closely related to the previous network attack analyzed in this thesis. In the previous section, a concentrated attack was looked at, where the adversary is motivated to disable only a small subset of the network deployment in order to carry out an event that must not be detected and reported.

Sensor networks are envisioned to be able to observe an environment in great detail. For such a requirement, it would become necessary to ensure high levels of connectivity across the entire environment that is of an observer's interest. As a characteristic of the network deployment, it is also very desirable to have higher resilience and tolerance towards network partitions and *cuts*.

Network partition attacks and concentrated collision attacks described in the previous section are motivated for similar reasons. In the network partition attack, the attacker's primary objective is to disable communication between two subsets of the network deployment.

b. Network Model

The network model is identical to that considered in the previous attack analysis. There is a random and uniform deployment of n nodes in a unit square. Each of these member nodes is capable of either omni-directional communication at a transmission range of r or uses a hybrid model with a transmission range r'. The channel is assumed

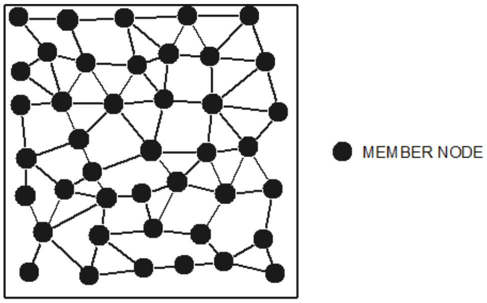


Fig. 31. Network Example - Before Attack

to be symmetric such that if node x can reach node y through signal transmission then node y can also reach node x.

While considering this attack, the traffic model is considered to be ad-hoc or point-to-point. For this reason, the existence of a sink node is not assumed at the center of the unit square. The example of a network deployment just before the attack is carried out is shown in Fig. 31.

c. Threat Model

For the network partition attack, the *Network Cut Coefficient* (NCC), represented by ϵ is an important parameter.

For a network deployment that contains n member nodes that is uniformly and randomly distributed in the environment considered, the effect of ϵ is as follows. If a partition attack with an NCC $= \epsilon$ is successful, then the two subsets of nodes, $n.\epsilon$ and $(1 - n).\epsilon$ will be unable to communicate with each other. This eventually leads to a partition in the network. It is to be noted that all nodes within either subset may not connected to each other after the attack. A linear cut across the unit square at $y = \epsilon$ will result such that there is no possibility of communication across the cut.

It can be understood that ϵ takes a value such that $0 < \epsilon < 0.5$, assuming the unit square as the region of interest to the network deployment observing physical

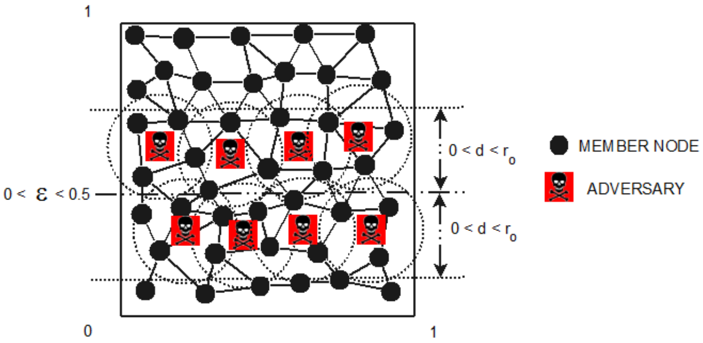


Fig. 32. Network Example - During Attack

phenomena. Values beyond 0.5 are not considered owing to the assumption of uniform distribution. Such a distribution would mean that for settings of ϵ between 0 and 0.5, the requirements to launch an attack would be similar for settings of $1 - \epsilon$.

As can be seen in Fig. 32, the attacker will be assumed to consider a linear cut in the unit square of randomly and uniformly deployed member nodes. There is also a parameter d, which is different from the context of the previously described attack. In the context of this attack, d is a value such that $0 < d < r_0$ that defines a region, which is a rectangle, over which the attacking adversary would be deploying malicious nodes to increase the efficacy of the attack and further contribute towards partitioning the network.

The adversary nodes work towards disabling links within their transmission ranges similar to the case of the previous attack. Each malicious node is capable of omni-directional communication with a transmission radius r.

The effect of such at attack is visible in Fig. 33. All links around the ϵ linear cut region were disabled. In the example shown it took 8 adversary nodes distributed in the region of attack to be able to disable communication between nodes across the ϵ line.

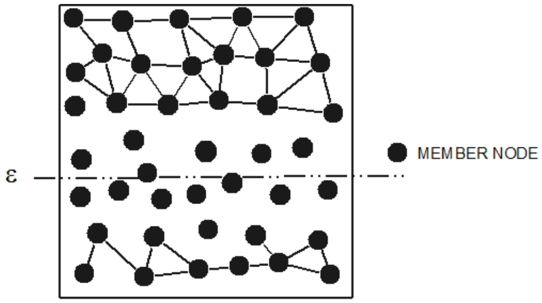


Fig. 33. Network Example - Post Attack

The model for dropping adversary nodes is chosen in such a manner, because in reality precise placement of adversary nodes is cumbersome from the perspective of the attacker. The larger rectangular area is a more realistic approximation of the model that will be followed by an attacker in real life to be able to create a partition in such a network deployment.

d. Metric of Comparison and Analysis

The metric of comparison between omni-directional based WSNs and a hybrid network is the *Cost of Launching Successful Attack*. This cost is measured using the number of adversary nodes that is required to be dropped into the region covered by the rectangular area.

Theorem 4 *Let n nodes be randomly and uniformly distributed in a unit square, each of transmission range r_0. r_0 can be r or r' depending on the communication model employed by the member nodes. Let $0 < \epsilon < 0.5$ describe a linear cut across which a network partition is required by attacking adversary nodes. Let $0 < d < r_0$ define the rectangular area of sides $2.d$ and 1 where the adversary nodes are randomly and uniformly dropped. Let each adversary node have a transmission range of r.*

Then, the cost of launching a successful attack increases in n, r_0 and ϵ and decreases in r.

Proof

The requirement for the attack to be successful is that all nodes on either side of the linear cut defined by ϵ must be unable to communicate with each other, across the cut. It is known that,

$$0 < d < r_0 \tag{4.35}$$

The area of the rectangle formed by the bounds between $\epsilon + d$ and $\epsilon - d$ is given by,

$$NPAttack_{Area} = 2 \cdot d \times 1 = 2 \cdot d \tag{4.36}$$

The success of the attack may be approximated as all original member nodes within the rectangle of area $NPAttack_{Area}$ losing all k neighbors that exist. If n_{adv} is the number of adversary nodes deployed to carry out the network partition attack, then following the results from Eq.(4.34), the probability can be computed as,

$$P_{PARTITION-ATTACKED} = 1 - \left(\sum_{h=0}^{k-1} \binom{s}{h} p^h (1-p)^{s-h} \right)^{n_{adv}} \tag{4.37}$$

where $\quad$ s=$\left\lfloor \text{n } \cdot 2d \right\rfloor$ $\quad$ and $\quad p = \frac{\pi r^2}{2.d}$

It is to be noted that the parameters s and p are modified for the model assumed for this attack. It has been justified in Sec. 3 that k increases with r_0. This implies that the probability mentioned in Eq.(4.37) decreases with r_0 leading to the conclusion that the cost of launching a successful attack increases in r_0. Eq.(4.37) also directly implies that the cost increases in n and decreases in r.

For the remainder of this analysis the fundamental motivation of the attacker, which is disabling links that exist on either side of the line of cut is considered. As the distribution of the member nodes is considered to random and uniform, then the number of original member nodes on either end of the line of cut can be computed on an average, with a very high probability as shown below.

$$n_{Subset_1} = \epsilon \cdot n \tag{4.38}$$

$$n_{Subset_2} = (1 - \epsilon) \cdot n \tag{4.39}$$

It is understood from the above equations that as ϵ ranges between 0 and 0.5, for smaller values of ϵ, the number of nodes in the first subset will smaller.

$$n_{Subset_1} < n_{Subset_1} \qquad \text{when} \quad \epsilon < 0.5 \tag{4.40}$$

According to the requirement of the attack, lesser number of nodes in one of the subsets, would mean that there will be a smaller number of links to disable for the attack to be successful. This is so because, there will be a smaller number of links formed across the cut with the nodes from the smaller subset. As the value of ϵ progresses towards 0.5, the number of nodes on either end will be comparable and the number of links to be broken would also increase.

Thus, with increasing ϵ the cost of launching a successful attack increases as it would require more malicious nodes to disable the increased number of links across the cut.

■

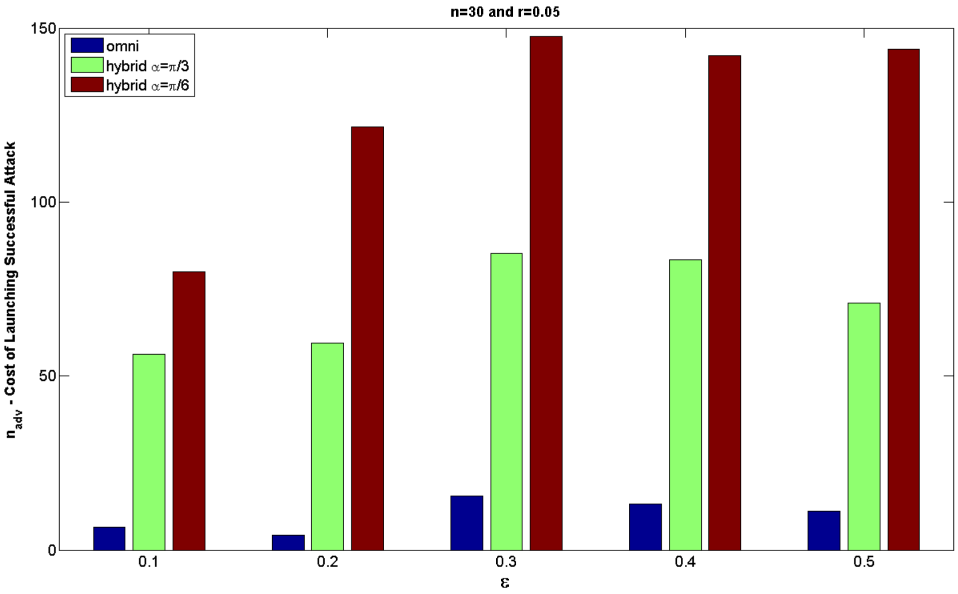


Fig. 34. Network Partition Attack Cost - $n = 30$, $r = 0.05$

The simulation set up for the following set of results is similar to those of previous settings. The interest of this set of simulations is to understand the loss of links across the cut. For this reason, an ad-hoc or point-to-point traffic model is assumed and the emphasis of the analysis is on paths between all member nodes in the network deployment. For the interest of the work presented in this thesis, d is chosen to be 0.3 on either side of the line of cut represented by ϵ.

The cost of a successful attack is computed in terms of the number of adversary nodes that must be deployed within the rectangle formed by the bounds between $\epsilon + d$ and $\epsilon - d$. Nodes on either side of the cut are organized into two sub-graphs. The adversary nodes n_{adv} are continuously deployed until no node in one sub-graph is able to communicate with any node in the other sub-graph. Two transmission radii settings of 0.01 and 0.05 are considered along with two settings for node density at 30 and 70.

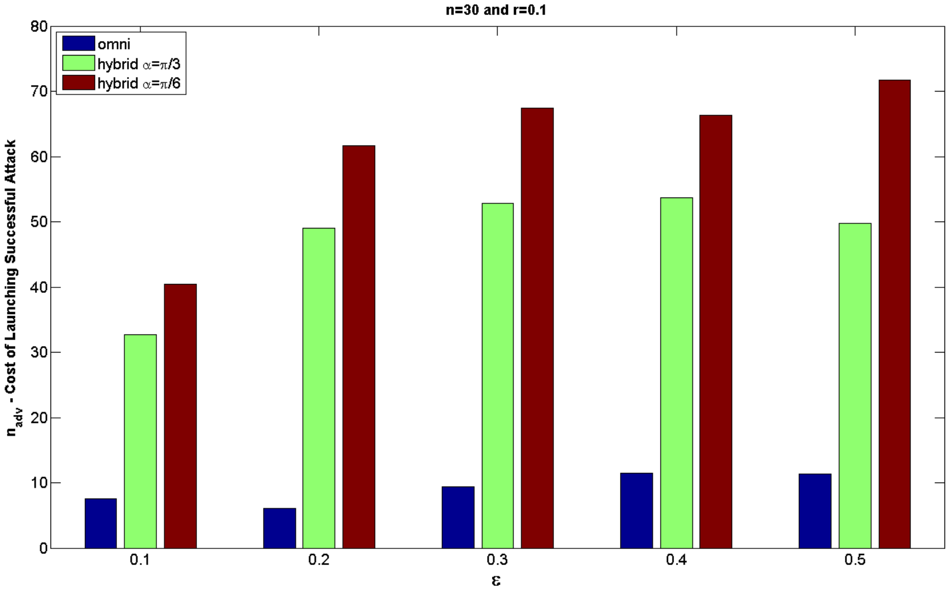


Fig. 35. Network Partition Attack Cost - $n = 30$, $r = 0.1$

As seen in Fig. 34 and Fig. 35 when the NCC is set to a small value of $\epsilon = 0.1$, there is an almost linear increase in the cost of the attack n_{adv} in both plots. With the plot that describes an increase in r, it can be seen that the cost of the attack decreases in comparison with the previous setting. This is justified by the reasoning that each of the adversary nodes have a communication radius r. And for the range of r chosen and the constant node density, the number of nodes that each adversary can disable increases.

Plots in Fig. 36 and Fig. 37 show the effect of an increased node density. With increased node density, the number of links that exist across the line of cut also increase as a consequence of which the number of adversary nodes needed to make the attack successful increases. The node density setting chosen for the second set of plots is $n = 70$.

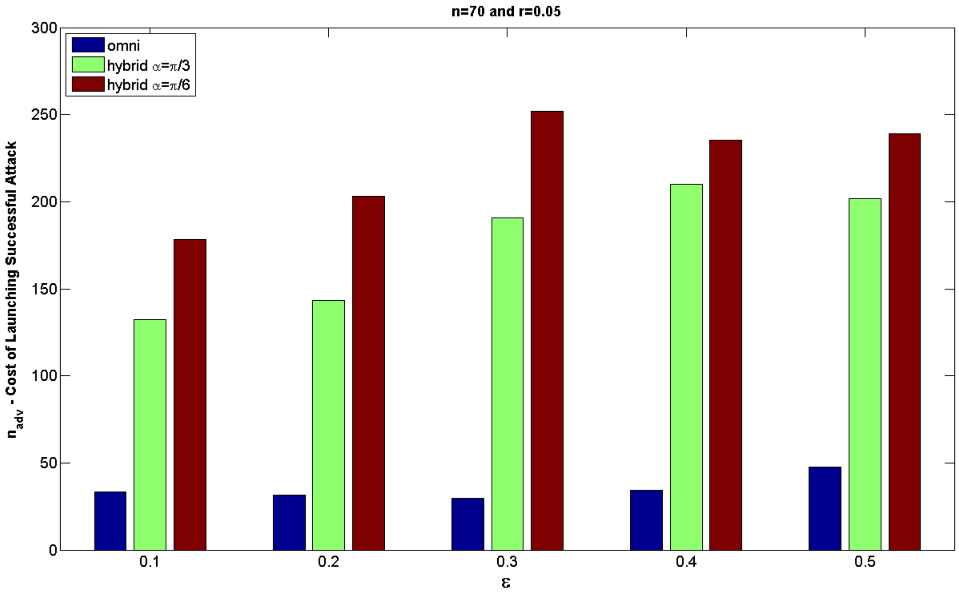


Fig. 36. Network Partition Attack Cost - $n = 70$, $r = 0.05$

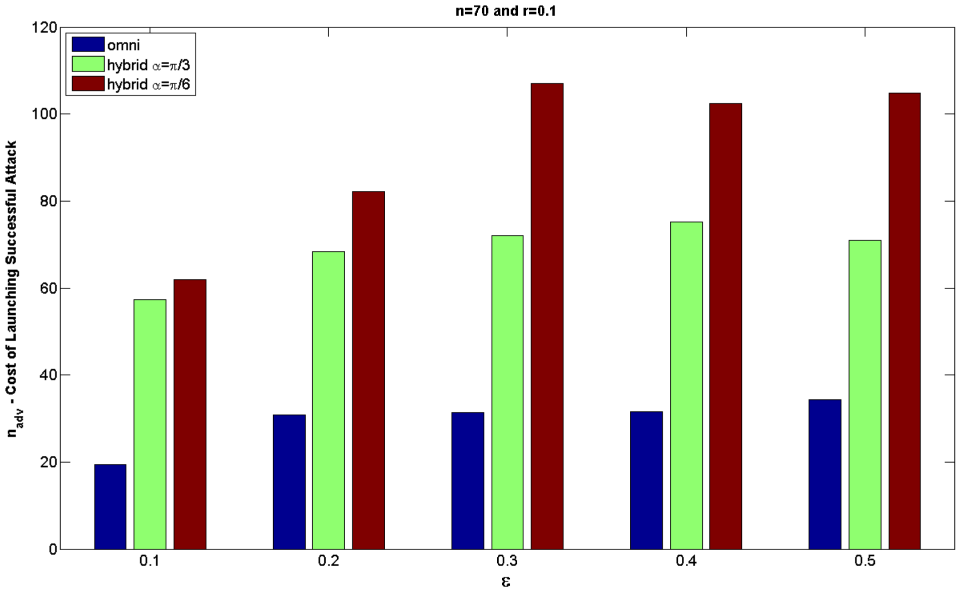


Fig. 37. Network Partition Attack Cost - $n = 70$, $r = 0.1$

CHAPTER V

CONCLUSION

In this work results on connectivity and security improvements using a hybrid approach towards antennas in sensor networks were presented. The results obtained are particularly interesting at lower node densities and transmission radii, motivating the use of a hybrid approach under these conditions for achieving better performance.

The standard communication paradigm that is currently employed in most sensor network deployments involves using omni-directional antennas, and the work presented in this thesis proves the capability of the new hybrid communication paradigm to out-perform the existing model in the areas of connectivity and security.

The specific information obtained from the results of this thesis in terms of the node densities and transmission radii is useful for network designers when considering the right network configuration required for providing certain levels of guarantees for connectivity and security against common network attacks.

Future work would involve the study of the effect of interference from using the hybrid communication paradigm. As transmissions are always restricted within sectors, intuitively the expected result is improved capacity. Another improvement in terms of the hybrid approach would be the use of directional reception. The improvements in connectivity from the use of directional reception would be interesting to consider. In terms of improved system longevity, the use of variable transmission and reception power is yet another technique that may be employed. The transmission power could be selected according to the distance between the transmitting and receiving nodes.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *Communications Magazine, IEEE*, vol. 40, no. 8, pp. 102–114, 2002.

[2] C.Y. Chong and S.P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[3] S.R. Gandham, M. Dawande, R. Prakash, and S. Venkatesan, "Energy efficient schemes for wireless sensor networks with multiple mobile base stations," in *Global Telecommunications Conference, IEEE GLOBECOM*, December 2003, pp. 377 – 381.

[4] D. Estrin, L. Girod, G. Pottie, and M. Srivastava, "Instrumenting the world with wireless sensor networks," in *IEEE International Conference on Acoustics, Speech, and Signal Processing*, May 2001, pp. 2033–2036.

[5] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in *Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications*, 2002, pp. 88–97.

[6] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[7] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[8] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[9] S.T. Rippe, "An Army and Air Force Issue: Principles and Procedures for AirLand Warfare. A Perspective of Operational Effectivenes on the Modern Battlefield," pp. 60–69, 1985.

[10] M. Trolle, "Mammal survey in the southeastern Pantanal, Brazil," *Biodiversity and Conservation*, vol. 12, no. 4, pp. 823–836, 2003.

[11] R.C. Johnson, *Antenna Engineering Handbook*, New York: McGraw-Hill Professional, 1993.

[12] J.D. Kraus and R.J. Marhefka, *Antennas for All Applications*, New York: McGraw-Hill, 2002.

[13] E. Kranakis, D. Krizanc, and E. Williams, "Directional versus omnidirectional antennas for energy consumption and k-connectivity of networks of sensors," *Proceedings of OPODIS*, 2004.

[14] J.C. Liberti and T.S. Rappaport, *Smart Antennas for Wireless Communications: IS-95 and Third Generation CDMA Applications*, Upper Saddle River, NJ : Prentice Hall PTR, 1999.

[15] B. Heile, "http://www.ieee802.org/15/," 802.15 Protocol Documentation, May 2008.

[16] B. Bollobás, *Modern Graph Theory*, New York: Springer, 1998.

[17] F. Zhao, J. Shin, and J. Reich, "Information-driven dynamic sensor collaboration for tracking applications," *IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 61–72, 2002.

[18] A. Woo, T. Tong, and D. Culler, "Taming the underlying challenges of reliable multihop routing in sensor networks," in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems*, 2003, pp. 14–27.

[19] S.D. Milner and C.C. Davis, "Hybrid free space optical/rf networks for tactical operations," in *Proc. IEEE Military Communications Conference*, November 2004, pp. 409– 415.

[20] X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated coverage and connectivity configuration in wireless sensor networks," in *Proceedings of the 1st ACM International Conference on Embedded Networked Sensor Systems*, 2003, pp. 28–39.

[21] S. Shakkottai, R. Srikant, and N.B. Shroff, "Unreliable sensor grids: Coverage, connectivity and diameter," *Ad Hoc Networks*, vol. 3, no. 6, pp. 702–716, 2005.

[22] H. Zhang and J.C. Hou, "Maintaining sensing coverage and connectivity in large sensor networks," in *NSF International Workshop on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks*, June 2005, pp. 347– 352.

[23] Y. Zou and K. Chakrabarty, "A distributed coverage-and connectivity-centric technique for selecting active nodes in wireless sensor networks," *IEEE Transactions on Computers*, vol. 54, no. 8, pp. 978–991, 2005.

[24] J. Ai, S. Ayorgun, and S. Shankar, "A transmission power control scheme for WSNs," *Los Alamos National Laboratory Technical Report*, August 2007.

[25] M. Kubisch, H. Karl, A. Wolisz, L.C. Zhong, and J. Rabaey, "Distributed algorithms for transmission power control in wireless sensor networks," *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, vol. 1, 2003.

[26] L. Kleinrock and J. Silvester, "Optimum transmission radii for packet radio networks or why six is a magic number," in *Proc. IEEE National Telecommunications Conference*, December 1978, pp. 431–435.

[27] H. Takagi and L. Kleinrock, "Optimum transmission ranges for randomly distributed packet radio terminals," *IEEE Transactions on Communications*, vol. 32, no. 3, pp. 246–257, March 1984.

[28] T.C. Hou and O.K. Victor, "Transmission range control in multihop packet radio networks," *IEEE Transactions on Communications*, vol. 34, no. 1, pp. 38–44, January 1986.

[29] T.K. Philips and S. Panwar, "Connectivity properties of a packet radio network model," *IEEE Transactions on Information Theory*, vol. 35, no. 5, pp. 1044–1047, September 1989.

[30] F. Xue and P.R. Kumar, "The number of neighbors needed for connectivity of wireless networks," *ACM Wireless Networks*, vol. 10, no. 2, pp. 169–181, March 2004.

[31] P. Gupta and P.R. Kumar, "Critical power for asymptotic connectivity in wireless networks," *Stochastic Analysis, Control, Optimization and Applications: A Volume in Honor of WH Fleming*, vol. 3, no. 20, pp. 547–566, 1998.

[32] C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in *Proceedings of the 3rd ACM International Symposium on*

Mobile Ad Hoc Networking and Computing. Lausanne, Switzerland, December 2002, p. 8091.

[33] A.K. Saha and D.B. Johnson, "Routing improvement using directional antennas in mobile ad hoc networks," in *Global Telecommunications Conference, IEEE GLOBECOM*, December 2004, pp. 2902–2908.

[34] U.N. Okorafor, K. Marshall, and D. Kundur, "Security and energy considerations for routing in hierarchical optical sensor networks," in *IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)*, 2006, pp. 888–893.

[35] A. Spyropoulos and C.S. Raghavendra, "Energy efficient communications in ad hoc networks using directional antennas," in *Proc. IEEE INFOCOM*, November 2002, pp. 220– 228.

[36] S. Yi, Y. Pei, and S. Kalyanaraman, "On the capacity improvement of ad hoc wireless networks using directional antennas," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing*, 2003, pp. 108–116.

[37] V. Navda, A.P. Subramanian, K. Dhanasekaran, A. Timm-Giel, and S. Das, "Mobisteer: Using steerable beam directional antenna for vehicular network access," in *Proceedings of the 5th International Conference on Mobile Systems, Applications and Services*, 2007, pp. 192–205.

[38] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proceedings of the 11th Network and Distributed System Security Symposium*, 2003, pp. 131–141.

[39] C.A. Balanis, *Antenna Theory*, New York:Wiley, 1997.

[40] M. D. Penrose, "On k-connectivity for a geometric random graph," *Random Structures and Algorithms*, vol. 15, no. 2, pp. 145–164, July 1999.

[41] B. Bollobás, *Random Graphs*, New York: Cambridge University Press, 2001.

[42] D. Torrieri, "Algorithms for finding an optimal set of short disjoint paths in a communication network," *IEEE MILCOM*, pp. 11–15, 1991.

[43] J.W. Suurballe and R.E. Tarjan, "A quick method for finding shortest pairs of disjoint paths," *Networks(New York, NY)*, vol. 14, no. 2, pp. 325–336, 1984.

[44] U.N. Okorafor and D. Kundur, "Efficient routing protocols for a free space optical sensor network," in *Proceedings of 2nd IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, December 2005, pp. 251–258.

[45] J.L. Volakis, *Antenna Engineering Handbook*, New York:McGraw-Hill Professional, 2007.

[46] S. Bellofiore, C.A. Balanis, J. Foutz, and AS Spanias, "Smart-antenna systems for mobile communication networks. Part 1. Overview and antenna design," *Antennas and Propagation Magazine, IEEE*, vol. 44, no. 3, pp. 145–154, 2002.

[47] D. Leang and A. Kalis, "Smart sensordvb: Sensor network development boards with smart antennas," in *International Conference on Communications, Circuits and Systems - ICCCAS*, 2004.

[48] J. Zhang and S.C. Liew, "Effective beam width of directional antennas in wireless ad hoc networks," *Information Theory - arXiv preprint - arxiv.org*, 2007.

[49] T. Ihara and R. Yamaguchi, "Adaptive array antenna," Jan. 28 2003, US Patent 6,512,934.

[50] J.H. Winters, “Smart antennas for wireless systems,” *Personal Communications, IEEE*, vol. 5, no. 1, pp. 23–27, 1998.

[51] R.A. Monzingo and T.W. Miller, “Introduction to adaptive arrays,” *New York: Wiley-Interscience*, 1980.

[52] J. Litva and T.K. Lo, *Digital Beamforming in Wireless Communications*, Norwood, MA: Artech House, Inc., 1996.

[53] T. Hammel and M. Rich, “A higher capability sensor node platform suitable for demanding applications,” in *Proceedings of the 6th International Conference on Information Processing in Sensor Networks*, 2007, pp. 138–147.

APPENDIX A

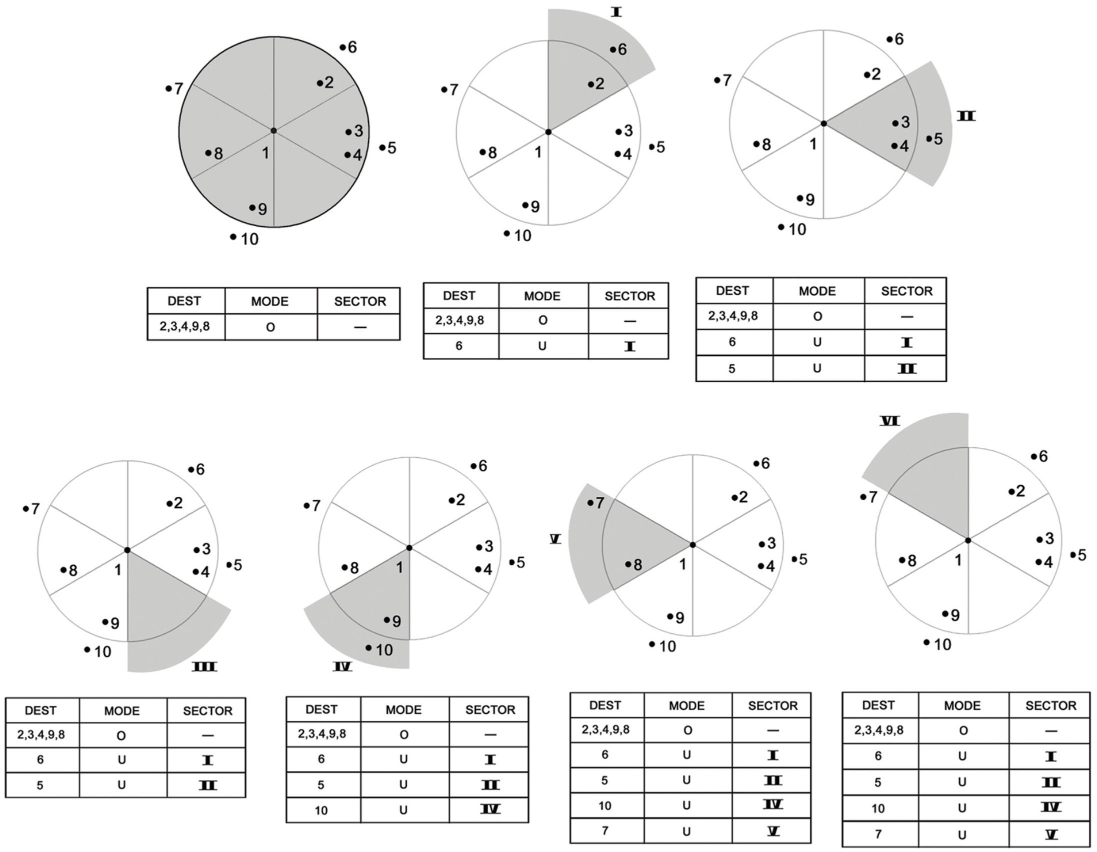
PROTOCOL ADDITIONS FOR NEIGHBORHOOD MANAGEMENT

In this section, a procedure that may be appended to any existing neighborhood management protocol is briefly described. This would explain in detail how a protocol can be modified so that it can perform the function of switching between sectors and also switching from a sector to the omni-directional mode. This also explains when switching is necessary. The most common and simple neighborhood discovery algorithm that is employed in sensor networks involves each member node broadcasting a $HELLO$ message so that any neighboring node within its omni-directional reach will be able to hear its transmission. Upon receiving such a packet, a neighboring node will respond with a $HELLO\ RESPONSE$ packet and both nodes update their neighbor tables with the identities of each other, which is included in every transmission. A modified version of such a protocol for uni-directional sensor networks is seen in [44]. For the hybrid approach a procedure that may be incorporated in existing sensor network stack implementations as an interface detail between the network and link layers is presented.

A very simple algorithm that may be used is described below:

Algorithm 1 Hybrid Approach - Neighborhood Management Extension

```
*Set* Antenna Mode = $OMNI$
*Run* Neighborhood Discovery Procedure
Populate Neighborhood Table
*Set* Antenna Mode = $UNI$
**for** $SECTOR = 1$ to $SECTOR = 6$ **do**
    *Run* Neighborhood Discovery Procedure
    Populate Neighborhood Table
**end for**
```



DEST	MODE	SECTOR
2,3,4,9,8	O	—

DEST	MODE	SECTOR
2,3,4,9,8	O	—
6	U	I

DEST	MODE	SECTOR
2,3,4,9,8	O	—
6	U	I
5	U	II

DEST	MODE	SECTOR
2,3,4,9,8	O	—
6	U	I
5	U	II

DEST	MODE	SECTOR
2,3,4,9,8	O	—
6	U	I
5	U	II
10	U	IV

DEST	MODE	SECTOR
2,3,4,9,8	O	—
6	U	I
5	U	II
10	U	IV
7	U	V

DEST	MODE	SECTOR
2,3,4,9,8	O	—
6	U	I
5	U	II
10	U	IV
7	U	V

Fig. 38. Neighborhood Management with Hybrid-equipped Nodes

For each node in a network, the antenna mode is first set to omni-directional and the *HELLO* message exchanges will be carried out followed by updating the neighborhood table. The same is repeated for each available sector; 6 sectors, each of beam width $\pi/3$ are used as an example in the algorithm described above. In addition to existing information, the sector and antenna mode will be stored at each node. In Fig. 38 an example of a node updating its neighborhood table is graphically described. As seen, the procedure begins with the omni-directional case for Node 1 and Nodes 2, 3, 4, 9 and 8 are enlisted. The shaded region shows the area over which the message broadcast can be received by any listening node positioned accordingly. The procedure continues with scans in Sectors I through VI and for those sectors where neighbors are found, entries are correspondingly made. As reception is modeled as omni-directional, the existence of a cheap compass at each node is assumed so that responses may be sent back to Node 1 in the right sector. Another low cost but sub-optimal approach is to send responses for node 1 in all available sectors until an acknowledgement is received for the same. Sending sectors may be appended to packets along with node identities for this reason. Fig. 38 also emphasizes on the fundamental advantage of using a hybrid approach for enhanced connectivity as seen in the shaded regions extending beyond the circle when each sector is activated.

Although the major traffic model employed for sensor networks is that of source-to-sink, where for a static network a node senses data and typically has the same next hop that would be used for the shortest path towards the sink, there are cases when data may have to be sent to other neighbors. Load balancing routing protocols and also applications that require collaboration between sensor nodes for data aggregation and other purposes are some examples where ad-hoc communication might be required. Thus, although switching sectors will not be required for a majority of the lifetime of a node, it is still a necessity for the operation of any sensor network deployment. The neighborhood management procedure described above will work in unison with an existing stack's routing protocol by switching sectors according to the destination of the packet in a node's transmit queue. Further optimization may be envisioned in terms of grouping packets in queue according to the sectors required for transmission based on the QoS requirements embedded into the packet.

APPENDIX B

COSTS - IMPLEMENTATION

The cost of using the hybrid approach is now analyzed in terms of hardware and implementation overhead. The hybrid paradigm is envisioned to be implemented using smart antenna technology. Smart antennas are basically *beamsteered* arrays where the radiation pattern is shaped according to a variety of optimum criteria [45]. Smart antennas have for many years been demonstrated to be able to support a variety of beamforming algorithms and have been used in cellular communication systems to improve capacity and range [46]. Beamforming is a technique that utilizes signal processing techniques to control the sensitivity and direction of antenna radiation patterns. For this reason, smart antennas have often been alternatively called *digital beamformed* (DBF) arrays. An electronically steerable linear array of antenna elements may be employed to achieve the antenna characteristics that is desired in the RF module present on the hybrid sensor nodes. It has to be noted that a circular array would provide improvements in terms of form factor and size. Smart antennas have very recently been considered specifically for sensor networks as seen in [47] which describes a smart antenna sensor mote platform. There is also significant work that uses components available off the shelf for applications in vehicular networks [37].

As mentioned in Sec. A the excitation voltages across the array elements plays a significant role in the radiation pattern the composite antenna produces. In terms of cost analysis, the most important factor would be the number of antenna array elements used. The number of elements also have a direct effect on the $effective$ beamwidth achievable by the antenna [48] as is seen below. An array factor of N is considered, such that there are $N + 1$ antenna array elements spaced at a distance

$D(D \leq \lambda/2)$ apart in a linear array, where λ is the operating wavelength. The position of the nulls and maxima are directly dependent on the number of antenna elements, the beamwidth being a function of the array factor and the effective path loss exponent. For the effective path loss exponent, α^* which is related to the path loss exponent α as $\alpha^* = \alpha/h$, the relationship between lgW_B and lgN was found to be linear [48], with a slope γ which is the *beamwidth decay index* and intercept b such that,

$$lgW_B = -\gamma lgN + b \tag{B.1}$$

This can be rewritten as,

$$W_B = 10^b/N^\gamma = b_1/N^\gamma \tag{B.2}$$

Eq.(B.2) confirms the notion that with increasing number of antenna elements in the phased array antenna, there will be more nulls, a sharper main beam and smaller side lobes in the resultant radiation pattern, this giving narrower beamwidths.

Thus, for the hybrid approach requirement using an array of 4 antenna elements would suffice for generating 6 sectors of beam width $\pi/3$ each. This is further justified via the following simplified relationship [49] [50] [51]:

$$n_e = \frac{\lambda}{d.sin(\alpha/2)} \tag{B.3}$$

n_e is the number of elements in the array, λ is the operating wavelength, d is the antenna spacing and α is the beam width.

As antenna elements are typically spaced $d = \lambda/2$ apart in an array, the number of elements can be generalized as

$$n_e = \frac{2}{sin(\alpha/2)} \tag{B.4}$$

Smart antennas are implemented today with digital beamformers [52] and so switching sectors does not incur any costs in terms of power or delay. Assuming such digital beamformers, costs may include a possible increase in the operating voltage and unit cost as components increase in terms of the number of antennas required for beamformimg. If we consider an omni-directional node to have a single antenna then n_e will be the additional number of antennas required. A detailed cost analysis per mote for a highly capable sensor node is found in [53]. Although a highly capable sensor mote is considered in this case, the intension of the following description is to provide an estimate of the increased cost of using the hybrid approach in terms of percentage of original cost of the mote.

Table. III follows from [53].

The antenna used in the mote described is replaced with a smart antenna, specifically an *ATMEL AT86RF211* as used in [47]. The module will operate in one of the configurable modes according to the requirements of the radiation pattern desired. This component can be purchased for a cost of 8.00 dollars. Thus the increase in cost as a percentage of the cost of the entire sensor mote for the example considered, Inc_{perc} will be such that $Inc_{perc} \leq 2\%$.

Table III. Sensor Mote Component Costs

Function	*Part*	*Cost in* $
Processor	Atmel AT91SAM7S256	8.70
Timing	Abracon ABM8-16.000MHz-B2-T	1.50
Modem	Chipcon CC2500	2.66
T/R Switch	NEC UPG2214TB (2x)	0.56
PA	NEC UPG2314T5N	2.00
LNA	Maxim MAX2641	0.80
Antenna	GigaAnt 3030A6111-01	3.00
Sensor	Panasonic AMN44122	26.74
Power Supply	Maxim MAX8621	3.70
Other/Misc	Misc. Parts	20.00
PCB Fabrication	1 board	30.00
PCB Assembly	1 board	30.00
Packaging	Case	60.00
TOTAL		257.66

VITA

Sonu Shankar has been a research assistant at the SeMANTIC group within the Wireless Communication Laboratory at Texas A&M University since December 2006. His research interests include security in wireless networks and lower layer protocol design. He worked as a design/development engineer at Midas Communication Technologies in 2005 and early 2006. During the summer of 2007 he worked as a research assistant at the Los Alamos National Laboratory in New Mexico. He holds a B.E. degree in electronics and commnunication engineering from Anna University. His permanent address is: 48275 Conifer St, Fremont, CA 94539.