SECURE INTEGRATED ROUTING AND LOCALIZATION IN WIRELESS OPTICAL SENSOR NETWORKS

A Dissertation

by

UNOMA NDILI OKORAFOR

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

DOCTOR OF PHILOSOPHY

August 2008

Major Subject: Electrical Engineering

SECURE INTEGRATED ROUTING AND LOCALIZATION IN WIRELESS OPTICAL SENSOR NETWORKS

A Dissertation

by

UNOMA NDILI OKORAFOR

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

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	Deepa Kundur
Committee Members,	Costas Georghiades
	Srinivas Shakkottai
	Eun Jung Kim
Head of Department,	Costas Georghiades

August 2008

Major Subject: Electrical Engineering

ABSTRACT

Secure Integrated Routing and Localization in Wireless Optical Sensor Networks.

(August 2008)

Unoma Ndili Okorafor, B.Sc., University of Lagos;

M.Sc., Rice University

Chair of Advisory Committee: Dr. Deepa Kundur

Wireless ad hoc and sensor networks are envisioned to be self-organizing and autonomous networks, that may be randomly deployed where no fixed infrastructure is either feasible or cost-effective. The successful commercialization of such networks depends on the feasible implementation of network services to support security-aware applications.

Recently, free space optical (FSO) communication has emerged as a viable technology for broadband distributed wireless optical sensor network (WOSN) applications. The challenge of employing FSO include its susceptibility to adverse weather conditions and the line of sight requirement between two communicating nodes. In addition, it is necessary to consider security at the initial design phase of any network and routing protocol. This dissertation addresses the feasibility of randomly deployed WOSNs employing broad beam FSO with regard to the network layer, in which two important problems are specifically investigated.

First, we address the parameter assignment problem which considers the relationship amongst the physical layer parameters of node density, transmission radius and beam divergence of the FSO signal in order to yield probabilistic guarantees on network connectivity. We analyze the node isolation property of WOSNs, and its relation to the connectivity of the network. Theoretical analysis and experimental investigation were conducted to assess the effects of hierarchical clustering as well

as fading due to atmospheric turbulence on connectivity, thereby demonstrating the design choices necessary to make the random deployment of the WOSN feasible.

Second, we propose a novel light-weight circuit-based, secure and integrated routing and localization paradigm within the WOSN, that leverages the resources of the base station. Our scheme exploits the hierarchical cluster-based organization of the network, and the directionality of links to deliver enhanced security performance including per hop and broadcast authentication, confidentiality, integrity and freshness of routing signals. We perform security and attack analysis and synthesis to characterize the protocol's performance, compared to existing schemes, and demonstrate its superior performance for WOSNs.

Through the investigation of this dissertation, we demonstrate the fundamental tradeoff between security and connectivity in WOSNs, and illustrate how the transmission radius may be used as a high sensitivity tuning parameter to balance there two metrics of network performance. We also present WOSNs as a field of study that opens up several directions for novel research, and encompasses problems such as connectivity analysis, secure routing and localization, intrusion detection, topology control, secure data aggregation and novel attack scenarios.

To Ekpe, Chisom and Apia.

ACKNOWLEDGMENTS

I want to express my deep and sincere gratitude to my academic advisor, Dr. Deepa Kundur, for her continuous guidance and support throughout my Ph.D. work at Texas A&M University, College Station. Her unparalleled understanding and encouragement have been invaluable and made my experience enjoyable.

I want to thank the members of my dissertation committee: Dr. C. Georghiades, Dr. E. J. Kim and Dr. S. Shakkottai, for their interactions and continuously instigating new ideas for me to explore. I also appreciate the time and service of Dr. N. Reddy. I am especially indebted to Dr. Karen Butler-Purry who continues to serve as an outstanding mentor, and has provided me with excellent advice, assistance and comfort.

I am very thankful to all of my colleagues, and especially members of the HoLiSTIC research group especially Alex, Will, Nebu, Sonu and Julien. They are fun, wonderful and interesting to work with.

I want to truly thank my husband, Ekpe, for his very strong shoulders that supported me in every aspect during my years in graduate study. Without him, this endeavor could not have been completed. My appreciation for my children, Chisom and Apia, is boundless. They always give me reason to fight on. Many thanks to my parents and parents-in-law, and my wonderful family for their continuous prayers, love and laughter. They are the best! There are friends, too numerous to name, whose genuine love and friendship I experienced on this journey. Thank you!

Finally, all the glory be to God almighty for whom I live, I move and I have my being. His Son has given me life, and His Spirit comforts, guides and illuminates my way, always.

TABLE OF CONTENTS

CHAPTER Page

CHAPTER Page

LIST OF TABLES

LIST OF FIGURES

FIGURE Page

FIGURE Page

FIGURE Page

CHAPTER I

INTRODUCTION

A. Overview of Wireless Optical Sensor Networks

The need for untethered communication and pervasive computing continues to drive advances in mobile communications and wireless networking. To serve this purpose, randomly deployed wireless sensor networks (WSNs) have been envisioned to consist of groups of sensor nodes that are randomly and densely deployed to observe ambient scalar data within a physical region of interest [1]. In many contexts, due to recent technological advances, the nodes are ultra-lightweight, comprised of small-sized wireless battery-operated nodes that are significantly *resource-constrained* in terms of power, storage, computational capability and bandwidth. Each sensor node comprises of a sensing, processing, communication, localization, mobilizer power source and power scavenging unit (some of which are optional, such as the mobilizer, power scavenging and location finding units). Figure 1 depicts a schematic diagram of the components of a typical sensor node.

Although individually, sensor nodes may be fragile and disposable, their usefulness comes from their easy and cost-effective deployment in large numbers to form an unattended network. In this way, they are able to aggregate inferences about their coverage area. For example, a WSN may contain several hundreds or thousands of these sensor nodes deployed over large geographical regions. Traditionally, the nodes form an ad-hoc network in order to communicate their sensor readings (about objects or events in their vicinity) to a centralized *sink* or *base station* via omni-directional radio frequency (RF). The network may be *stationary* or *dynamic*

The journal model is *Proceedings of the IEEE*.

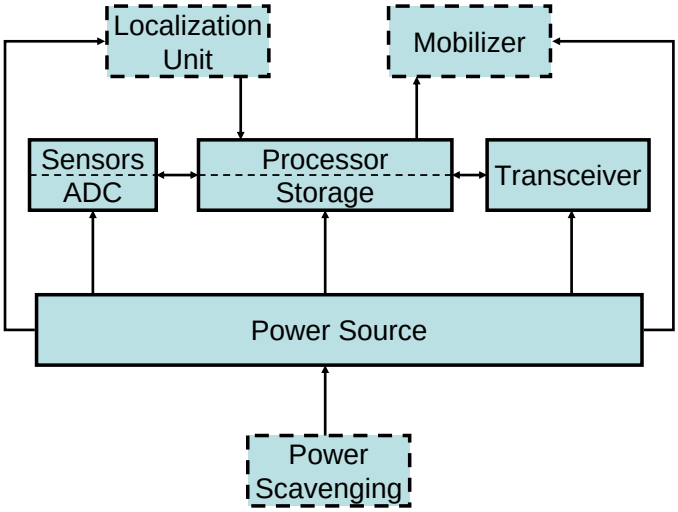


Fig. 1. A schematic diagram of the components of a sensor node.

with mobility-capable nodes. Their ability to be set up inexpensively, in large-scale, and quickly makes WSNs a promising candidate for a host of applications, including military surveillance, disaster relief, law enforcement applications, traffic control, infrastructure security and advanced health-care monitoring. For example, a WSN may be deployed to gather intelligence in a battle field by tracking enemy troop movement, monitoring a secured zone, or guiding a missile target system. Other possible applications of WSNs include monitoring environmental conditions such as temperature/humidity, collecting pollution data, monitoring structural weaknesses in buildings or equipment, inventory control, and detecting the presence of chemical or biological agents, to name a few. The system architecture of a typical sensor network habitat monitoring application is depicted in Figure 2.

Currently, through technological advances in miniaturization and micro-electro mechanical systems (MEMS), WSNs continue to evolve towards the so-called *smart dust* - dust-sized sensor nodes that can float in the atmosphere - based on the Uni-

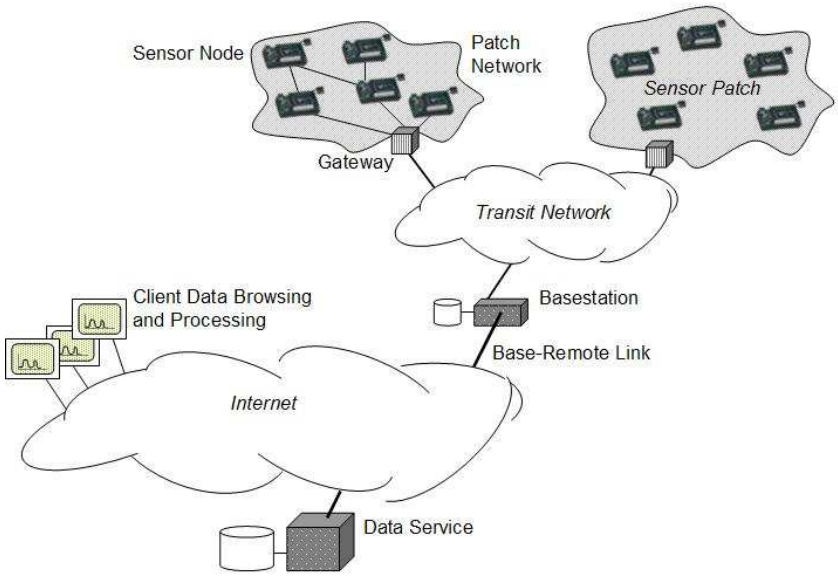


Fig. 2. The system architecture of a typical sensor network habitat monitoring application.

versity of California, Berkeley's Smart Dust project [2]. Recently, there has been increased interest in the development of *wireless optical sensor networks* (WOSNs) [3–10] as a viable contribution towards the feasible design of smart dust nodes. WOSNs are an emerging subclass of WSNs comprised of nodes whose *point-to-point* communication paradigm employs directed *broad-beam free space optics* (FSO), a high bandwidth communication technology that enables information transmission through the atmosphere using modulated light beams. The FSO transceiver unit of WOSN nodes achieves size reduction by a factor of up to twenty, when compared to the competing RF antennas [2]. Furthermore, FSO continues to stand out as the leading technology for the development of rapidly deploy-able and secure wireless sensor and surveillance networks, with the potential for broadband communication.

Classically, WOSNs possess the following distinctive features, many of which are shared by their RF counterparts:

- *spatially distributed*, in order to improve the performance and geographical range of sensing functions. To ensure effective collaboration amongst network entities, the *connectivity* of the network must be guaranteed;

- *resource constrained*, representing one of the biggest design challenges, necessitates the judicious use of communication bandwidth, memory, and computation to enhance the life span of the often portable and non-renewable power source;

- *hierarchical*, employing localized clustering of sensor nodes into subnetworks to improve network scalability;

- *location aware*, necessitated by event-driven applications that rely on the ability of nodes to gain knowledge of their location in order to localize, track and communicate activities of interest within the network;

- *redundant*, employing densely deployed nodes to obtain more accurate and complete readings of observed events;

- *vulnerable to attack*, due to a host of applications that deploy non-tamper resistant nodes within environments that are *hostile* or not monitored. Security paradigms must be considered at all network layers to guarantee privacy, confidentiality, availability and authenticity of the sensor data.

The fundamental question we pose and seek to address in this dissertation is as follows:

> What are the implications of link directionality to connectivity and secure routing for ad hoc wireless sensor networks?

The objective of this dissertation is to study the feasibility of employing FSO as the networking paradigm in *security-aware*, broadband, randomly and rapidly deploy-

able WSNs consisting of stationary nodes. Our investigation is primarily concerned with two main aspects of WOSNs: (1) the requirements for a probabilistic network connectivity guarantee in the *physical layer* with respect to the trade off between network parameters of node density, beam angle and communication radius; and (2) a novel secure routing and localization scheme suited for the unique *network layer* characteristics of the WOSN.

Connectivity as well as secure routing and localization under the WOSN paradigm is challenging due in part to the directionality of links resulting from the line-of-sight requirement for FSO communication. Because of the well known fact that incorporating security mechanisms after the design of network protocols is often non-trivial and superficial at best [11], it is beneficial to consider security objectives in the initial design of any protocol. Our security solution integrate routing and localization while leveraging the natural hierarchy and link directionality in WOSNs.

B. Motivation

As with any wireless medium, FSO is susceptible to routing attacks such as data replay, identity theft, or injection of unauthorized bits into the network. Worse, an enemy that is able to compromise an authentic network node, may easily launch more serious insider attacks, by extracting keying and security information from the compromised node, and then acting as an authentic network participant [11]. Unfortunately, an attack in the network layer can completely cripple the WOSN and undermine its purpose, in spite of best efforts aimed at securing other OSI layers of the network. As noted in [12], *if the routing protocol can be subverted, and messages altered in transit, then no amount of security on the data packets can mitigate a security threat at the application layer.* In addition, the vulnerability of sensor nodes to

physical capture and tampering, combined with the collaborative nature of *multi-hop* communication, makes network layer protection mechanisms even more crucial.

The WOSN architecture is motivated by a consideration for the viable and cost-effective choice that FSO presents for data transmission requiring enormous bandwidth while achieving reduced transceiver size. FSO communication carries light signals at extremely high frequencies, offering the highest capacity for wireless communications medium. The WOSN can provide full-duplex *gigabit-per-second* (Gbps) throughput for multimodal data such as multimedia, hyperspectral imagery and multi-variate heterogeneous data. Additionally, the FSO signal can be rapidly deployed because it is transmitted using unlicensed optical wavelengths that do not require expensive government licensing, and it is unaffected by interference with existing networks. As motivating examples, we identify three cutting edge applications of WOSNs.

Wireless Multimedia Sensor Networks comprising of sensors that collect multimedia information such as digital images, video, and audio, requiring Gbps link speeds [13, 14] for applications such as tactical battlefield and advanced pervasive health care surveillance, visual and other forms of broadband data that are imperative for monitoring and effective decision-making. The development of wireless multimedia sensor networks has been driven in part by recent improvements in embedded devices, MEMS technology, and the advent of inexpensive and low-resolution miniature hardware that acquire rich media content from the environment, such as cheap CMOS video cameras and microphones. It is widely believed that WOSNs present the most viable networking solution to the bandwidth bottleneck that will accelerate the realization of practical wireless multimedia sensor network systems.

Mission Critical Sensor Networks refers to networking for application domains where life or livelihood may be at risk, including critical infrastructure protection, emergency and crisis intervention, and military operations. Mission critical sensor networks aim to develop mechanisms to promote specialized network protocols that are ultra-dependable, rapidly-deploy-able and secure in the face of sudden and adverse conditions. Because the frequency spectrum used by FSO is free/unregulated, avoids interference with existing systems, and the signal often provides more secure communication, well designed WOSNs are a viable solution for rapidly deploy-able mission critical networks [15].

Hybrid Sensor Networks consists of robust systems that employ a *complementary* hybrid FSO-RF communication network to leverage the advantages of both technologies [16, 17]. Hybrid sensor networks provide differentiated network quality-of-service (QoS), motivated by an integrated heterogenous service delivery, such as simultaneous ultra-high bandwidth, low latency FSO channels and ultra-reliable RF links that are resilient to packet loss. Additionally, hybrid FSO-RF networks can withstand a wide range of adverse environmental conditions which either technology alone cannot provide, and are of particular interest to several military and intelligence-gathering applications.

For several applications such as the ones cited above, it is critical that network data be protected from intentional loss, modification, or unwanted access, necessitating the design of secure and privacy-enhancing WOSNs. In particular, it is necessary to provide solutions for secure neighborhood discovery in ad hoc deployments, and mechanisms to detect and recover from malicious attacks on the network. Without adequate security design at the network layer, WOSNs are vulnerable to attacks including passive eavesdropping, distributed denial-of-service (DDoS) and data cor-

ruption [11], that can easily lead to catastrophe for critical applications.

C. Comparison of Free Space Optical and Radio Frequency Technologies

Traditional wireless sensor networks often rely upon radio waves as the carrier signal for long range, dependable, broadcast communications. Due to its broadcast nature, the signature of the RF signal is omnidirectional (occupies 2π radians in a plane), and hence susceptible to eavesdropping and "jamming" attacks. By their nature, RF signals are not subject to the same degree of degradation from adverse atmospheric conditions (except for heavy rain) that FSO transmissions suffer, thereby providing a greater assurance of accurate and effective data transmission although at a somewhat lesser data transfer rate. A vast range of networking protocols have been studied within the RF WSN paradigm [18]. Omni-directional RF networks are often simply modeled as *geometric random graphs* (GRGs) [19] employing a disc model transmitter foot print (ignoring fading effects) as illustrated in Figure 3 (a). In the GRG model, two nodes establish a bidirectional link if they are within a fixed distance r known as *communication or transmission radius* [20].

Employing directional antennas, the energy of the RF beam can be spatially directed, resulting in a typical directed RF radiation pattern of *angular width* α but containing *side lobes* shown as in Figure 3 (b). Recent studies have demonstrated clear advantages of directional RF in terms of enhanced power usage, increased signal strength, longer communication ranges and reduced interference and multi-path components [21]. However, RF technology in general, does not provide the same bandwidth capacity, and suffers from expensive spectrum licensing limitations compared with FSO [2, 10].

On the other hand, directional FSO is a commercial, wireless, ultra-high band-

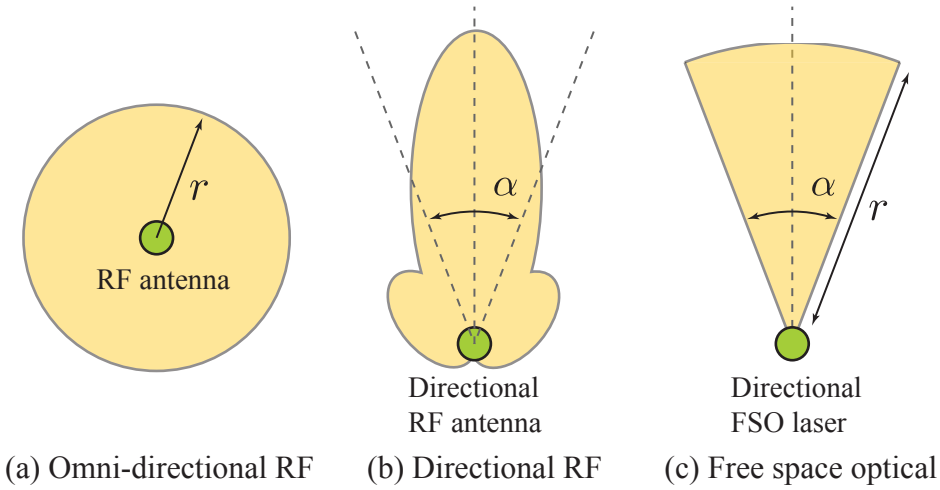


Fig. 3. The transmitter footprints of various communication models.

width line-of-sight (LOS) technology that is relatively new to the sensor network community. By employing a directed laser (Light Amplification by the Stimulated Emission of Radiation) or LED (Light-Emitting Diode) to transmit light beam signals, FSO achieves very high data rates, (Gbps) over a few kilometers using unlicensed frequencies in the order of hundreds of terahertz [6]. For example, current FSO systems employing 1550nm lasers attain up to 1.25 Gbps over distances up to 6km, with an ON-OFF keying (OOK) modulation scheme [22]. The directional broad beam FSO's transmitter signature is represented well, simply by a circular sector, as illustrated in Figure 3 (c).

We note here that for the FSO transmitter, two configurations are possible; a narrow beam highly focused energy signal with a beam diameter of a few milliradian (mrad), and the broad beam signal with diffused energy and significantly larger beam diameters, greater than $\pi/18$ [17]. The FSO receiver may be employed in three configurations: a directed, diffused or omnidirectional detectors, so that different

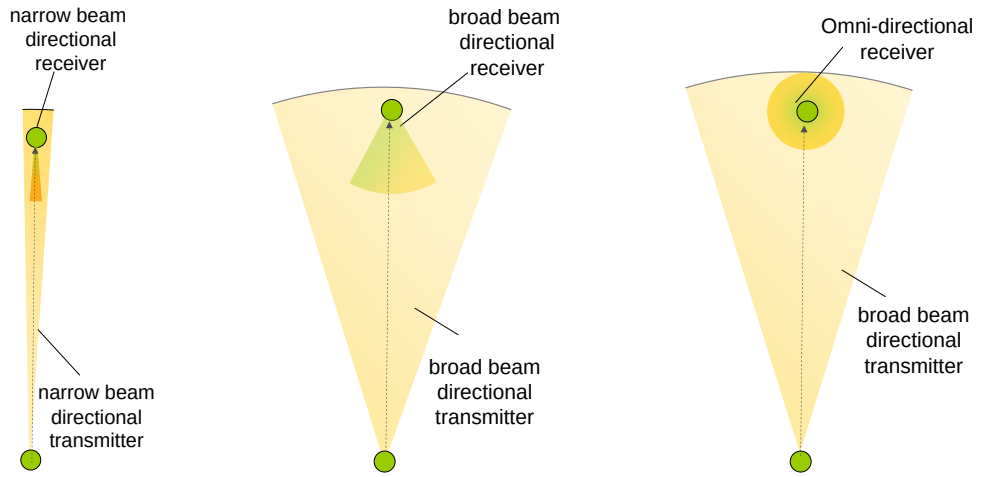


Fig. 4. Various transmitter-to-receiver configurations available for FSO communication.

transmitter/receiver link configurations are possible including, a narrow beam-to-narrow beam as depicted in Figure 4 (a), a narrow beam-to-broad beam as illustrated in Figure 4 (b), or a broad beam-to-omni directional configuration shown in Figure 4 (c). For this dissertation, we adopt the *broad beam-to-omnidirectional* model of Figure 4 (c) proposed for the Smart Dust [2], as it offers the most viable high bandwidth networking solution in a randomly deployed ad hoc network scenario. Within the WOSN a directed link is established from a node s_a to s_b if and only if s_b falls within s_a's communication sector, defined by the communication radius r and the beam width α of the sector [9].

1. Advantages of FSO over RF Communication

WOSNs have a number of distinct advantages over RF WSNs [21], including:

Bandwidth: It is well known that FSO enables transmission bandwidths on the order of Gbps which the current state-of-the-art RF technology struggles to pro-

vide [13]. For example, the IEEE 802.11x standard is limited to link throughputs on the order of 10s of megabits per second (Mbps) [17], while current 802.15.4 compliant sensor nodes achieve nominal rates of about 250Kbps [13]. Even with the much anticipated development and deployment of ultra-wide-band (UWB) RF transmission techniques capable of theoretical throughput rates in excess of 675 Mbps for 1.3GHz pulse-UWB systems, the pulses are very short in space (less than 23cm for a 1.3 GHz bandwidth pulse), and their achievable bandwidth drops significantly with increased ranges (lower than 802.11a at modest ranges of $r \geq 15$m) [17]. On the other hand, FSO offers up to 1.25Gbps over link distances over one kilometer [22] which easily satisfy the bandwidth-hungry demands of multimodal high capacity sensor networks.

Form Factors (Size and Power per bit): Due to the simple analog circuity required for the OOK modulation scheme, the WOSN nodes can be small, and consume less power. The size of the FSO equipment can be as small as a laser pointer (i.e., a few millimeters), making dense integration of multiple FSO transceivers on to a single node chip possible. Semiconductor lasers and LEDs used for active FSO communications require very little power (a few milli-watts) making them suitable for power limited ad-hoc sensor network scenarios. Additionally passive FSO communication employing corner cuber retroreflectors (CCRs) which require negligible power from the nodes may also be employed. An illustration of the transmission range achievable versus energy per bit for active and passive FSO compared to RF is shown in Figure 5, which illustrates the huge power advantage of FSO over RF.

Spatial Reuse: By focusing energy in one direction, the potential for spatial reuse is increased while interference and energy are reduced for a comparable trans-

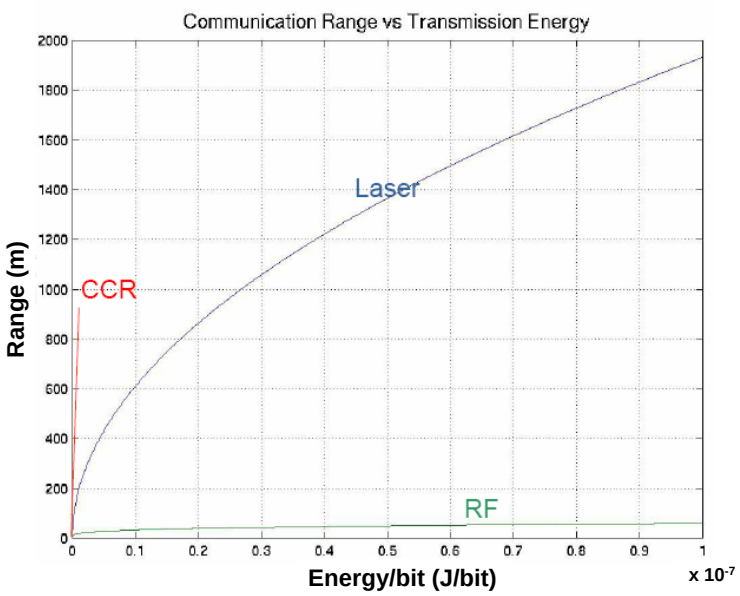


Fig. 5. Illustrating the transmission range versus energy per bit for FSO compared to RF.

mission range. FSO also yields increased signal strength, longer communication ranges, and reduced multi-path components compared to RF.

Security: Directed FSO communication is more secure than broadcast RF due to the reduced spatial signature of energy from a broadcast disk model for the GRG model, to the RSSG model, thereby reducing the chances of successful eavesdropping. The physical difficulties in intercepting the FSO beam, its non-susceptibility to jamming attacks, and the associated high chance of detection with eavesdropping enhance the security property of WOSNs. This advantage is more significant for applications deployed in unsecured or hostile environments.

Licence-free quick installation Optical wavelengths are license free, so FSO deployment does not require any permissions as long as they are eye safe. Deploying WOSNs save time and money, while avoiding interference issues that plague

traditional broadband RF. For this reason, WOSNs can be rapidly deployed, typically within a few hours.

2. Challenges

WOSNs face two major challenges compared to RF WSNs, including; (1) a need for the existence of line-of-sight between communicating nodes resulting in the directionality of links; and (2) the reduced transmission quality observed in adverse weather conditions. These challenges are described in some detail below:

Requirement for Clear Line of Sight and Alignment: Clear line-of-sight requirements for the reception of an FSO signal has direct implications on network connectivity especially in an ad hoc WOSN. One proposal to alleviate the line-of-sight limitation includes employing an accurate point-and-track beam-steering actuator for aligning narrow beam FSO systems (i.e. the trans-receiver of a node is a mobile unit, capable of swivel motion to align the sender's transmitter to the receiver) [17]. With the broad beam-to-omnidirectional transmitter/receiver configuration employed in this dissertation, our approach to network connectivity entails studying the constraints on the physical layer properties of the network (node density, communication radius and beam width of the FSO signal) that guarantee a probabilistic measure of network connectivity [23].

Signal degradation with adverse weather: For the FSO signal, reduced bit rates are encountered in adverse atmospheric conditions as fog, heavy snow and rain. Table I presents the typical attenuation effects of various adverse weather conditions on a 1550 nm laser. Additionally, light from other sources (e.g., direct and intense sunlight), temperature, and physical obstructions (e.g., flying birds, smoke) may temporarily interrupt or hamper the effectiveness of the

Table I. Attenuation effects of adverse weather conditions on a 1550 nm laser.

Condition	Attenuation (dB/Km)	Max range (Km)
Clear air	< 1.5	> 6
Heavy rain (25mm/hr)	5	3.2
Extreme downpour (75mm/hr)	13	1.7
Heavy Snow/Light fog	20	1.25
Snowstorm/heavy fog	30	0.92
Very dense fog	$60 - 100$	0.35 - 0.55

system. Conventionally, two approaches are taken to mitigate the effects of adverse weather conditions, which include; (1) designing a hybrid FSO-RF sensor network in which the RF serves as a backup channel during down times of the FSO channel; and (2) considering a dense (enough) network with shortened link distances and route redundancies which counter failed links in adverse weather using multipath routing. In this dissertation, we are more concerned with the latter solution by proffering connectivity analysis that incorporate models for channel fading effects due to adverse weather and atmospheric conditions.

Safety The safety of FSO used to be an important concern since high power laser beams (e.g., wavelengths between 400 nm to 1400 nm) can cause injury to the eye and skin. However, lasers in the 1550 nm wavelength range have been shown to be reasonably safe, and better able to operate in unfavorable meteorological conditions [22].

In Table II, we summarize the significant differences between FSO and RF for ad hoc wireless sensor networking.

Table II. Comparison between FSO and RF communication for ad hoc sensor networks.

Property	FSO	RF
Frequency spectrum	Unregulated, free	Restricted, govt. licensed, expensive
Comm. channel	LOS, directional	Broadcast, omni-directional
Interference	Physical Obstruction,	EM interference
Weather Attenuation	Fog, snow,	Heavy rain
Distances	< 6km	> 100km
Transmit Energy	10pJ/bit over 10-100m	100nJ/bit over 10-100m
Receive Energy	Negligible	$30 - 50$nJ/bit
Channel Loss	$\propto 1/d^2$	$\propto 1/d^{2\rightarrow 7}$
Energy saving device	CCRs 167pJ/bit	pico radios 16nJ/bit
Size of Node	mm^3	cm^3
Bandwidth	up to 1.25Gbps	up to 100Mbps

D. The Wireless Optical Sensor Network Model

Deployment Model: Consider a set $\mathcal{S}_n = \{s_i : i = 1, 2, \cdots n\}$ of n stationary WOSN nodes, randomly and densely deployed in a bounded, unit area[1], planar square region $\mathcal{A} = [0, 1]^2$ according to a uniform distribution. Each sensor has an equal and independent likelihood of falling at any location in $\mathcal{A}$, and facing any orientation. We emphasize that once a node falls, it is stationary, that is, incapable of altering its location or orientation. Let vectors $\overline{x} = (x_1, x_2, \cdots x_n)$ and $\overline{y} = (y_1, y_2, \cdots y_n)$ represent the (x, y) position coordinates of $\mathcal{S}_n$ such that $(x_i, y_i) \sim \text{Uniform}(0, 1)^2$. For ease of reference, let $\Upsilon_i = \binom{x_i}{y_i}$ be s_i's point position where $\overline{\Upsilon} = \binom{\overline{x}}{\overline{y}}$. The vector

[1]Simple scaling can be applied to obtain other dimensions.

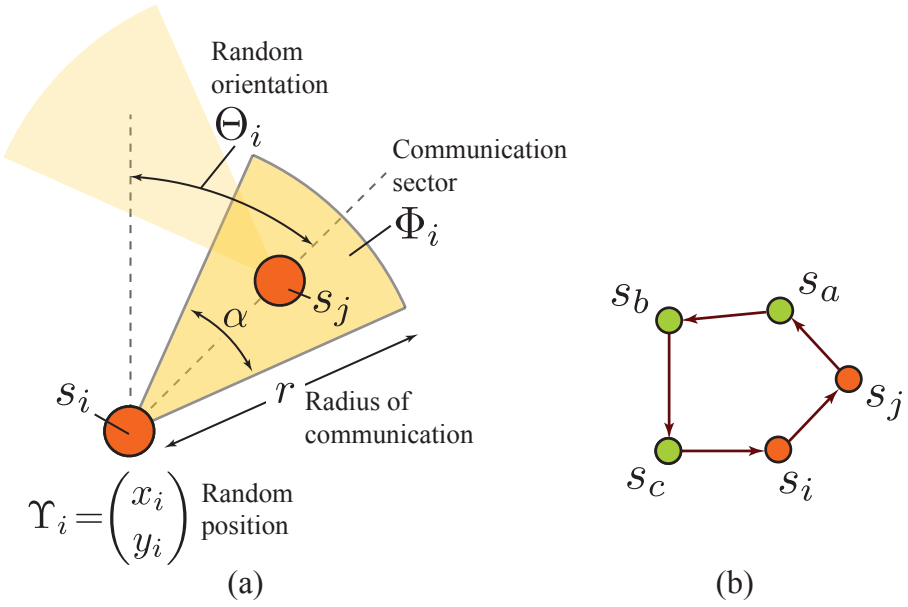


Fig. 6. (a) Each sensor s_i transmits within a sector Φ_i defined by the 4-tuple $(\Upsilon_i, \Theta_i, r, \alpha)$, which are parameters of the system. (b) Node s_j only hears s_i if s_j falls into s_i's communication section, but s_j talks to s_i via the back channel $s_j \rightarrow s_a \rightarrow s_b \rightarrow s_c \rightarrow s_i$.

$\overline{\Theta} = (\Theta_1, \Theta_2, \cdots \Theta_n)$ depicts the random orientations associated with $\mathcal{S}_n$ such that $\Theta_i \sim \text{Uniform}[0, 2\pi)$, $\forall s_i \in \mathcal{S}_n$. The spatial distribution of the nodes has been well modeled as a homogenous Poisson point process [24, 25] of density $n/|A|$, where $|A|$ is the area of $\mathcal{A}$, which is one in our case making n the network density of the unit area deployment region.

The Node: WOSN nodes employ a directed broad-beam FSO transmitter suitable for short-range networking applications [26]. By scanning a laser beam across an angular sector, each node s_i can send data within a contiguous, randomly oriented communication sector $-\alpha/2 + \Theta_i \leq \Phi_i \leq +\alpha/2 + \Theta_i$ of radius r, and angle $\alpha \in [0, 2\pi)$ radians, as depicted in Figure 6(a), where Θ_i is the orientation of s_i. The

communication sector Φ_i which is completely defined by the 4-tuple $(\Upsilon_i, \Theta_i, r, \alpha)$ is associated with each node s_i.

The node's receiver is omnidirectional (employing several photodetectors [26]) implying that s_i may directly talk to s_j (denoted $s_i \rightarrow s_j$) if and only if $\Upsilon_j \in \Phi_i$. However, s_j can only talk to s_i via a multi-hop back-channel or reverse route denoted $s_j \rightsquigarrow s_i$, with other nodes in the network acting as routers along the reverse path (unless of course $\Upsilon_i \in \Phi_j$). In the illustration of Figure 6(b) an example of a reverse route for $s_j \rightsquigarrow s_i : s_j \rightarrow s_a \rightarrow s_b \rightarrow s_c \rightarrow s_i$ is shown. Naturally, in discovering a multi-hop directed reverse communication path, the notion of a circuit, first proposed for WOSN routing in [27] results, and serves as the fundamental mechanism for bidirectional communications in WOSNs.

The Network: The random multi-hop network cooperatively formed by $\mathcal{S}_n$ is the WOSN, defined by parameters n, r and α. As previously noted, this network architecture has recently been modeled as a random scaled sector graph (RSSG) [9], with the case of $\alpha = 2\pi$ converging to the GRG model. The RSSG network model is formally defined in Chapter II. Figure 7 depicts a sample simulation scenario WOSN node graph, with $\mathcal{A} = 1$ km^2, $n = 200$ nodes, $r = 0.2$ m and $\alpha = 2\pi/9$ radians. The circles in the Figure represent nodes while the associated triangular patches represent their communication sectors.

Cluster-Based Hierarchy: As is common, a fraction of the WOSN nodes play the functional role of *cluster heads* (CHs) [2]; network gateway nodes that employ advanced hardware such as passive cornercube retroreflectors (CCRs) [7] to establish a bidirectional communication link with the base station. We assume that all nodes are equipped with these CCRs, which are simple optical devices that reflect incident

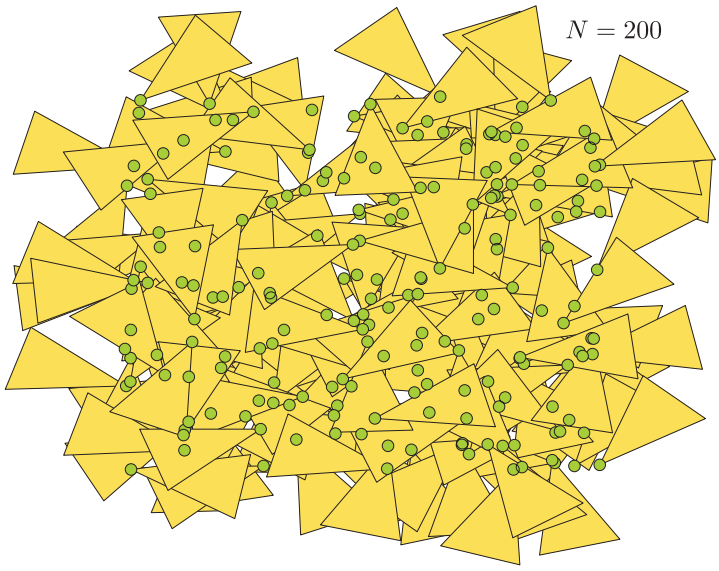


Fig. 7. A sample WOSN deployed in a unit area square region of 1 m^2, with $n = 200$ nodes, $r = 0.2$m and $\alpha = 40^o$. The circles represent nodes while associated triangular patches represent corresponding communication sectors.

light back to source, and is used by the nodes to modulate an interrogating beam from the base station. The use of passive bidirectional communication between CHs and the base station yields huge energy savings for the nodes compared to active laser, as illustrated in Figure 5, and offers an attractive solution because most of the optical energy for communication is supplied by the base station, with a negligible energy burden used for the modulating circuitry of the CCR placed on CHs. In general, CCRs are good for WOSNs due to their small size, ease of operation and negligible power consumption.

After random deployment, nodes that, by virtue of their orientation, have a direct line-of-sight communication path to the base station become CHs. This implies that they exploit their CCRs and line-of-sight view to communication directly with the base station [7, 10]. The set of CHs depend on individual node orientation (which is

uniformly random), and the base station's location, so that cluster heads are uniformly distributed in the network. This leads naturally to a hierarchical structure in which nodes route data to the upwards "closest" cluster head for onward forwarding to the base station (*uplink*), or receive data or broadcasts from the base station (*down-link*) via another downwards "closest" cluster head. In this case, "closest" is measured in terms of number of hops. This hierarchical architecture is tied to currently existing FSO and CCR technology, and has also been studied, under Berkeley's Smart Dust Program [2, 7, 10].

CHs can send or receive data directly to or from the base station on behalf of other nodes in their associated clusters, respectively. We denote P_{CH} as the probability that a node is a cluster head, and mark node s_k which is a CH with an asterisk to give s_k^*, and denote the set of cluster head nodes by $\mathcal{CH}$.

Medium Access Control: The medium access control data communication sub-layer is that part of the data link layer that provides addressing and controls channel access by dealing with issues such as channel reservation and sharing, packet collision detection, and packet re-transmissions. In particular, for FSO used in WOSNs, a packet switch mounted on each node enables media access control layer addressing of data packets. In addition, the packet switch performs address-based routing of packets received by the access device so as to route packets through the optical network and detects packet collisions from devices coupled to other nodes and schedules packet retransmissions. The well known IEEE $802.11x - 802.16$ medium access control protocol interfaces for fixed broadband wireless access systems may be adapted to the WOSN scenario [28].

1. Graph Theoretic Framework

We model the n-node WOSN topology simply as a *directed random graph* $G_n(\mathcal{S}_n, \mathcal{E})$ consisting of a vertex node set $\mathcal{S}_n$ and edge set $\mathcal{E}$, where every edge is an ordered pair of distinct nodes. A random graph is one in which the vertices are randomly placed in the plane, while a directed graph is one in which each edge has a unique direction (i.e., edges are not bi-directed). The matrix $\mathcal{E}$ is represented as the $n \times n$ *adjacency matrix* of $G_n(\mathcal{S}_n, \mathcal{E})$ [29] with one row and one column for every node, such that the matrix elements are assigned values:

$$\mathcal{E}(i,j)_{1\leq i,j\leq n} = \begin{pmatrix} 1 \text{ if } \Upsilon_j \in \Phi_i \\ 0 \quad \text{otherwise} \end{pmatrix}$$

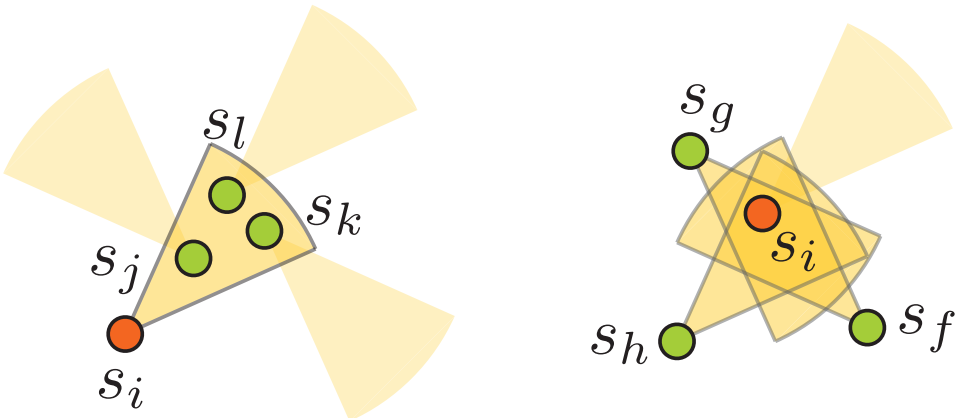
to indicate that there is, or there is not, an edge from s_i to s_j respectively, and $\mathcal{E}(i,i) = 0 \quad \forall i$ disallows self loops. Directionality implies $\mathcal{E}(i,j) \neq \mathcal{E}(j,i)$ necessarily, $\forall i, j$. An in-depth study on random graphs is provided in [19, 29], and an example of a WOSN node graph and its associated adjacency matrix is given in the Appendix. We further assume a virtual bidirectional grid connects all cluster heads via the base station, so that $\mathcal{E}(k,l) = \mathcal{E}(l,k) = 1, \forall s_k^*, s_l^* \in \mathcal{CH}$. In contrast to the GRG model [19], the adjacency matrix for WOSNs is sparser and non-symmetric.

The directional paradigm necessitates that two sets of neighbors be defined for each WOSN node: *successors* and predecessors [29] illustrated in Figures 8 (a) and (b), respectively.

Definition 1 Successors

In $G_n(\mathcal{S}_n, \mathcal{E})$, s_i's successors consists of the set $\mathcal{S}_i$ of nodes that fall within Φ_i such that s_i can transmit data to them. Formally, we define the set $\mathcal{S}_i$ as

$$\mathcal{S}_i =: \{s_k\}, \forall k : \mathcal{E}(i,k) = 1,$$



(a) Node s_i's successors s_j, s_k, s_l. (b) Node s_i's predecessors s_f, s_g, s_h.

Fig. 8. Distinct neighborhoods of a WOSN node.

The cardinality of $\mathcal{S}_i$ is denoted as δ_i^+, and is equivalent to s_i's in degree[2].

Definition 2 Predecessors

In $G_n(\mathcal{S}_n, \mathcal{E})$, s_i's predecessors *consists of the set $\mathcal{P}_i$ of nodes whose communication sector s_i falls into, implying that s_i can receive data from such nodes. Formally, we define the set $\mathcal{P}_i$ as:*

$$\mathcal{P}_i =: \{s_h\}, \forall h : \mathcal{E}(h, i) = 1,$$

The cardinality of $\mathcal{P}_i^-$ is denoted as δ_i^-, and is equivalent to s_i's out degree.[3]

We define a multi-hop *path* from node s_1 to s_k denoted $s_1 \rightsquigarrow s_k$, as a sequence of nodes $[s_1 \cdots s_k]$ such that $\mathcal{E}(i, i+1) = 1$ for all $i \in [1 \cdots k-1]$. Note that the labeling of nodes on a path used here for illustration, is not necessarily sequential. A

[2] *The in degree is obtained as the sum along the i^{th} column of $\mathcal{E}$.*

[3] *The in degree is obtained as the sum along the i^{th} column of $\mathcal{E}$.*

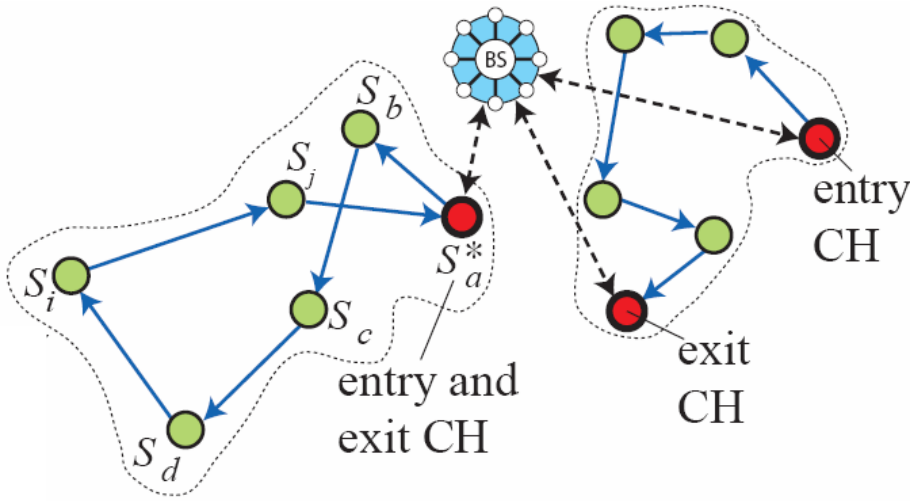


Fig. 9. The BS-circuit is the concatenation of node s_i's uplink and downlink paths. The entry and exit cluster head may be the same or two distinct nodes. Uplink path for s_i: $s_i \rightarrow s_j \rightarrow s_a^* \rightarrow BS$. Downlink path for s_i: $BS \rightarrow s_a^* \rightarrow s_b \rightarrow s_c \rightarrow s_d \rightarrow s_i$.

circuit is a closed path or loop which starts and ends at the same vertex. We define a base station-circuit *(BS-circuit)*, illustrated in Figure 9 as a circuit which necessarily includes the base station. The BS-circuit facilitates the definition of an *uplink* route for each node s_i consisting of the path $s_i \rightsquigarrow BS$ to enable data forwarding from s_i to the base station. Similarly, s_i's *downlink* route is the path $BS \rightsquigarrow s_i$ for receiving data from the base station. As shown in Figure 9, node s_i's uplink paths $UL(s_i)$ and downlink paths $DL(s_i)$ must necessarily include *exit* and *entry* cluster heads respectively, which may be distinct or the same nodes. Furthermore an exit cluster head in one BS-circuit may act as an entry cluster head for a different BS-circuit. Every individual UL and every individual DL matches up to produce a distinct BS-circuit.

2. Threat Model

The threat model enumerates the various attacks that may be launched on the WOSN, assuming that the network is deployed in a hostile environment, and the nodes are not tamper resistant. The routing threat model impacts the integrity and availability of network services, by considering the proportion of vulnerable or attacker-controlled communication channels. It has been noted [12] that the notion of confidentiality is mute if an attacker commands majority of the data transmission paths. Following convention, we classify the network layer threats for the WOSN as follows:

(1) Outsider routing attacks: These refer to a scenario in which the opponent has no special access to the WOSN. In the worst case scenario, the attacker deploys its own network of alien nodes in a distributed manner in the region, to monitor the authentic network. We do not consider the case in which alien nodes move to block or jam physical communication channels of nodes, since this is a physical layer attack different from a routing or network layer attack. In general, cryptographic primitives including encryption/decryption for privacy as well as message authentication codes (MAC) and one way key chains for authentication, work to mitigate outsider attacks. In this dissertation, we assume that the threat from the outsider attacker encompasses three of the well known threats: passive eavesdropping to decipher communication patterns or route setup; injecting false routing packets to confuse the network; and replay attacks that disrupt routing [11].

(2) Insider routing attacks: In these attacks a motivated attacker can compromise (via physical or remote exploitation) a subset of authentic nodes, gaining access to their keys and cryptographic materials, and then launching attacks by masquerading as authentic network participants. Traditionally, the routing threat from node compromise is measured by its impact on confidentiality data integrity, and availabil-

ity of network services by considering the proportion of attacker-influenced communication channels. That is, we must consider whether secret keys of un-compromised nodes can be obtained and/or whether routing packets may be arbitrarily modified by malicious insiders. Even though insider attacks are restricted to the limited capabilities of the original nodes, their access to trusted infrastructure and network resources makes them potentially debilitating. They are also more difficult to recognize and stem, as cryptographic primitives do not mitigate against them.

With insider attacks, often, the best that can be done is to ensure a graceful degradation of network performance with compromised nodes, while designing efficient and robust intrusion detection and recovery mechanisms that identify malicious nodes and isolate them from future participation in network protocols. A metric for evaluating tolerance to insider node compromise is the proportion of network services degraded with the fraction of nodes compromised. One of our goals in this dissertation also entails constraining insider attackers to packet dropping as the only viable attack. Routing threats from an insider attacker include all the above mentioned outsider threats, in addition to spoofed or altered routing signals aimed at confusing routing functions, and denial of service attacks that waste other node's resources.

3. Assumptions

The BS is a resource-rich, powerful, location-aware and trusted entity that cannot be compromised. In a disaster exploration situation, the BS may, for example, be set up prior to first responder action. Nodes are homogeneous, with a fixed r and α selected to satisfy connectivity constraints [23]. Node s_i is pre-deployed with a unique *individual key* K_i and *password* PW_i it shares only with the BS, and with a *network-wide key* K_N shared with every node, all of which are 64-bit random values. Nodes are aware of a preset positive integer δ representing the *maximum hop count*,

and each node $s_i \in \mathcal{CH}$ with probability p_{CH}.

Nodes are not tamper resistant and with probability p_a may be subverted by an attacker. Each node s_i is uniquely identified by its name, and is aware of its orientation Θ_i by employing an inexpensive compass. Nodes are unaware of their relative positions as the resource constraints on nodes impedes the use of global positioning systems (GPS) or other costly localization hardware. Lightweight security primitives employing pre-deployed symmetric keys are assumed. We denote $A|B$ as the concatenation of message A with message B if both messages emanate from the same node, and $A||B$ otherwise, while $\mathbb{E}_K[M]$, $\mathbb{D}_K[M]$ and $MAC_K\{M\}$ respectively denote the *encryption*, *decryption* and *message authentication code* (MAC) of message M with key K [30], all of which use a symmetric 64-bit key. Where appropriate, the lightweight RC5 scheme and the HMAC-MD5 algorithm (with a 128-bit authenticator value) are utilized [31], and the XOR function $\oplus$ is employed to avoid byte expansion.

E. Dissertation Contributions

The research in this dissertation is focused on three important contributions.

1. **Probabilistic connectivity analysis:** We undertake the connectivity analysis of WOSN systems in order to demonstrate their feasibility in random deployments. Employing probabilistic arguments, we specifically address the *parameter assignment problem* for WOSNs, stated as follows: How should physical layer parameters of the WOSN including node density, communication radius and transmitter beam divergence, be selected such that, with a given (high) probability, the WOSN is connected? The tool sets we use in our analysis include random graph theory, probability theory and statistical spatial theory. Our analysis provides a closed form expression relating the network parameters

to a tight upper bound on the probability that the WOSN is connected, and therefore is of practical importance in enabling design engineers to trade off parameter value choices for network level design of ad hoc WOSNs.

2. **Secure Routing and Localization:** We address secure neighborhood discovery, route set up and localization of individual nodes within the WOSN. We introduce SIRLoS, a novel lightweight *secure integrated routing and localization scheme* for WOSNs. SIRLoS exploits a novel paradigm based on hierarchical cluster-based directional circuit-based routing to offer enhanced security based on simple symmetric cryptographic primitives that leverage the powerful base station and an energy-saving location estimation algorithm in one step. SIRLoS guarantees that routing and location information are protected against eavesdropping and unauthorized manipulation, while providing broadcast authentication, data confidentiality, integrity and freshness. We demonstrate novel insights to security benefits of link directionality within the SIRLoS framework, and provide performance evaluations that demonstrate the potential of SIRLoS to outperform comparable algorithms.

3. **Security and Attack Analysis and Synthesis:** We provide detailed security and attack analysis and synthesis. The strengths and possible security vulnerabilities of SIRLoS are discussed, as well as its performance under various known WSN routing attacks. In particular, we discuss the BS-circuit collusion attack and wormhole attacks, and present countermeasures to thwart these attacks, employing directionality and the connectivity of the graph. Through our analysis, we show that r is a high sensitivity parameter for network connectivity as

well as security, and further demonstrate the fundamental tradeoff that exists between connectivity and security for directional sensor networks.

1. Organization of the Dissertation

The remainder of the dissertation is organized as follows: In Chapter II, we present an overview of related literature in the areas of connectivity, routing, localization and security in WSNs. Contribution 1 is addressed in Chapter III, which includes the discussion of WOSN connectivity in the presence of fading channels. Chapter IV is dedicated to addressing contributions 2 and 3. Finally we present concluding remarks and directions for future work in Chapter V. A summary of the notations used in this paper is presented in Appendix A. In Appendix B we present details on computing distances in the WOSN employing the toroidal distance metric, and present Kosaraju's algorithm in Appendix C.

CHAPTER II

LITERATURE REVIEW

A. Background Survey on Connectivity in Wireless Sensor Networks

Generally, a connected network - defined as one in which a path connects every pair of sensor nodes [19] - is desirable for the optimal functioning of the network. Network protocols such as routing, broadcasting, clustering and medium access control, rely heavily on the guaranteed connectivity property of the network's physical layer. However, in designing connected WSNs, characteristics of the communication technology, channel medium as well as considerations for energy constraints on the nodes must also be taken into account. As the energy consumed by a node is exponentially proportional to its transmitting range r, a smaller value of r not only results in reduced energy usage, but also in reduced signal interference within the channel, and thus increased network capacity. Therefore, in order to minimize power consumption and maximize throughput, there is a great need to explore the *minimum* possible density of nodes needed to achieve a connected wireless network [32]. A closely related problem involves determining the *critical transmission range* r, i.e., the minimum value of r that guarantees connectivity.

In traditional RF WSNs in which connectivity follows a range-dependent model, the problem of guaranteeing connectivity while minimizing some measure of energy consumption has been termed the *range-assignment problem* [32]. The solution to this problem is crucial in defining guidelines in the design of WSN [33] including answering questions such as: how many sensor nodes should be dispersed, or which transceiver (classified by the value of r they attain) should be used with individual nodes in order to minimize cost? Formally, we define the range-assignment problem

as follows: *given a set of n randomly deployed nodes, all having the same r, what is the minimum value of r that ensures the resulting GRG network is connected?*

We first identify variations of the network connectivity analysis problem for WSNs, which we shall not address or review in this dissertation. Some definitions of the range assignment problem encompass a more general version in which each individual node s_i is assigned a unique transmission range $r_i \in (0, r_{max}]$ where r_{max} denotes the maximum transmitting range possible. The solution to this version of the problem leads to an optimal topology control protocol for the network, which has been shown to be NP-hard (i.e., nondeterministic polynomial time hard) in deployment region dimensions higher than one [34]. For our analysis in this dissertation, we have assume all nodes transmit using the same range $r = r_{max}$.

A number of papers have addressed the problem of assuring connectivity when node positions are assumed to be known with certainty. In [35], for example, nodes are carefully arranged in a grid pattern, and then fail with a specified probability, so that the randomness arises due to node failure rather than initial node placement. Others, for example [36, 37] have been primarily concerned with the coverage problem in WSNs, including (1) ensuring that sensor nodes *cover* every point on a region of interest, so that any event within the region may be *sensed* by at least one node; (2) defining the fraction of area covered by the sensor network; and/or (3) determining the fraction of nodes that may be removed without reducing the area coverage of the network. Even though it has been shown that connectivity is not directly related to coverage [35, 38], some papers [37, 39] have conjectured a connection between the two.

Researchers have also investigated the connectivity property of dynamic ad hoc networks with mobile nodes or *agents*. In [40], for example, the authors consider the problem of controlling a network of nodes by placing differentiable constraints on

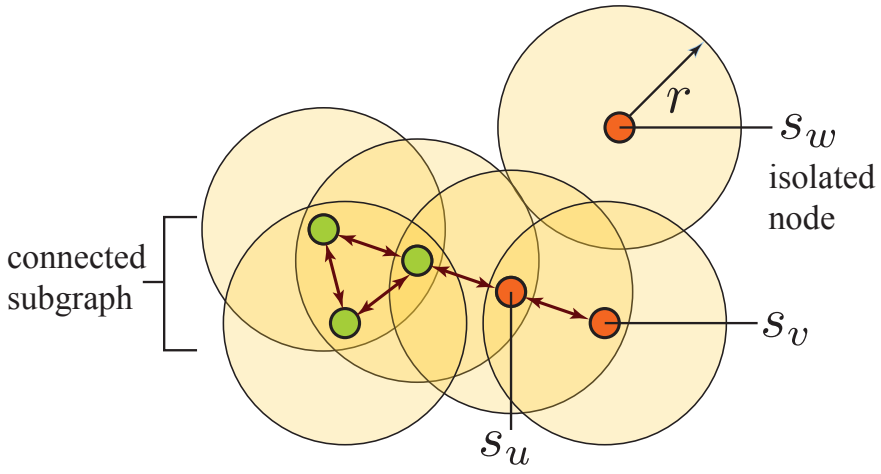


Fig. 10. An GRG network model for a traditional RF omnidirectional sensor network. All links in the network are bidirectional. A node s_w is isolated if it is not within the communication range r of any other node in the network.

individual node motion, so that the connectivity property of the network is always preserved, while in [33] the effect of various node mobility models on the connectivity of the network is investigated. Even though the papers highlighted in the above paragraphs are, in some cases, related to our defined range assignment problem, the assumptions of *a priori* known deployment locations, node mobility, and the coverage problem are strictly inapplicable to the work of this dissertation, and therefore will not be the focus of our literature review.

Instead, we discuss some recent work in the range assignment problem for ad hoc packet radio WSNs where there has been recent effort to provide a random graph theoretic framework to study ad hoc networks of sensors. For the omnidirectional RF WSN, a suitable model is the *geometric random graph* (GRG), also known as the *random scaled disc graph* [19, 20, 32, 36, 41–43], formally defined as follows:

Definition 3 *[44] To construct a random geometric graph, pick points from the plane by a Poisson process with density n nodes in the region. Then join each pair of*

points by a line if they are at distance less than or equal to r.

Definition 3 induces a topology in which given r, two nodes can communicate if the distance between them is less than r. Obviously, the GRG with the r-radius model for all nodes, relates to a simple omnidirectional network (without consideration to channel fading) in which all links are necessarily bidirectional, so that if link $s_v \rightarrow s_u$ exists, then $s_u \rightarrow s_v$ must also exist. We denote this bidirectional link as $s_u \leftrightarrows s_v$. For RF WSNs, r is a function of transmission energy, size of antenna and network density. An *isolated node* in a GRG is then defined as one that falls outside the communication range of every other node. The GRG network model illustrating a connected subgraph and an isolated node s_w is depicted in Figure 10.

One approach to the range assignment problem in GRG networks applies *asymptotic* reasoning by providing connectivity assurances as the region size or n grows to infinity, and applies to dense networks. In one of the pioneering papers on the *critical* power a node needs to transmit in order to ensure that the network is connected, Gupta and Kumar [20] employ results from continuum percolation theory [45] and random graphs [46], to derive the sufficient condition on r as a function of n for the asymptotic connectivity of the GRG network. Their results show that for n nodes uniformly deployed in a planar unit area disk, if $r \geq \sqrt{[\log(n) + c(n)]/\pi n}$, then the network is asymptotically almost surely (a.a.s.) connected (as $n \rightarrow \infty$ with probability one), only if $\lim_{n\rightarrow\infty} c(n) = +\infty$, where $c(n)$ is a constant for the n-node network. In [33], the authors present connectivity results for real world sparse networks by introducing a geometric parameter that bounds the deployment area to a finite region.

Others have analyzed asymptotic connectivity of the GRG with respect to the minimum number of neighbors required by each node in a k-neighbor model. In [47],

Kleinrock and Silvester optimize an objective throughput function based on the average number of neighbors, and suggest that a fixed *magic* number of neighbors equal to *six* is sufficient to guarantee network connectivity, regardless of the value of n. Takagi and Kleinrock [48] later revised this magic number to *eight*. In [43], Xue and Kumar show that there is no magic number, but rather that the number of neighbors required for asymptotic connectivity grows as $\Theta(\log n)$. In particular they show that this number must be larger than $0.074 \log n$ and less than $5.1774 \log n$. In [41], the authors provide an improved lower bound for the number of neighbors required as $0.129 \log n$.

In [19], Penrose studied the more general problem of k-connectivity of GRG networks deployed in d-dimensional cubes with $d \geq 2$, and proved that the graph becomes k-connected almost surely at the instant r attains the critical value at which each node has a minimum number of k neighbors. Simply stated, this important result implies that as $n \to \infty$, the probability that the minimum r that achieves k-connectivity of the network equals the minimum r that yields a minimum of k neighbors for all nodes tends to one. Therefore, for the problem of connectivity, it suffices to adjust r until each node has at least one neighbor, i.e., no isolated node exists in the network. The results in [19] hold for any L_p-norm distance metric, where $1 < p < \infty$.

Employing a *probabilistic* approach and nearest k-neighbor methods, Bettstetter [42] show that for a ρ-density network, with probability at least p, no isolated node occurs if $r \geq \sqrt{-\ln(1 - p^{1/n})/\rho\pi}$. He then leverages the results of [19] discussed in the preceding paragraph to empirically demonstrate that for nodes densely deployed in a bounded region (with $n \to \infty$), and for probability values close to one, the probability that no isolated node occurs in the network yields a tight upper bound, (and therefore a good approximation using the same parameter values) for the probability

that the network is connected, if boundary conditions are compensated for. In several of the cases cited above, a related analysis of range assignment in the presence of fading links have also been considered. However, as with all the prior work cited here so far, Bettstetter only focused on omnidirectional RF WSNs as modeled by GRGs.

For WOSNs, there has been relatively little research aimed at the corresponding *parameter assignment problem*, stated as follows: *given a set of n randomly deployed WOSN nodes, all having the same r and α, what is the minimum value of r that ensures the resulting network is connected?* The equivalent problem of finding the minimum n or α that ensures that the underlying network is connected has also not been previously addressed. The parameter assignment problem for WOSNs necessitates that we present a random graph model of the network (applicable also to directional RF), termed the *random scaled sector graph* (RSSG), and first defined in [9] as follows:

Definition 4 *[9] For any natural n, fixed angle α and range r, let $\mathcal{S}_n = \{S_i\}_{1\leq i\leq n}$ be a sequence of independently and uniformly distributed (i.u.d.) random coordinate of points in $[0,1]^2$, and let $\Theta = (\Theta_i)_{1\leq i\leq n}$ be a sequence of i.u.d. angles in $(0, 2\pi]$ associated with $\mathcal{S}_n$. Let $\mathcal{E}$ represent the $n \times n$* adjacency matrix *such that the matrix elements are assigned values: $\mathcal{E}(i,j)_{1\leq i,j\leq n} = 1$ if and only if $s_i \rightarrow s_j$ exists. The graph $G(\mathcal{S}_n, \mathcal{E})$ is termed the random scaled sector graph.*

The RSSG is a generalization of GRGs for a network of sensors using wireless optical communication, and with α set to 2π, the RSSG converges to the GRG model. To address connectivity within the RSSG model, Diaz et al. [9], employ similar asymptotic connectivity arguments to show that for exactly the same constraint on r as obtained in [20], as $n \rightarrow \infty$ the directed graph induced by the WOSN is connected as the number of cells in the grid dissecting the deployment region goes to infinity. They

Table III. Comparing related work on range assignment for WSNs.

Reference	**Comm.**	**Analysis**	**Deployment**	**Other**
[39]	RF WSN (O)	Random	Geometric	Coverage
[50]	RF WSN (O)	Probabilistic	Deterministic	Coverage
[32]	RF WSN (O)	Random	Deterministic	Coverage
[35]	RF WSN (O)	Probabilistic	Grid	Coverage
[42]	RF WSN (O)	Probabilistic	Random	k-connectivity
[20]	RF WSN (O)	Asymptotic	Random	None
[51]	RF WSN (D)	Probabilistic	Random	Coverage
[52]	RF WSN (D)	Probabilistic	Random	Scheduling.
[49]	RF WSN (O/D)	Probabilistic	Stochastic	None
[9]	WOSN	Asymptotic	Random	None
Our Work	WOSN	Probabilistic	Random	Clustering

show that, if the ratio of r to the length of the side of the cells is kept constant, then with probability approaching one, and as the number of cells grows there is a directed path connecting any two nodes in the WOSN. Furthermore, they demonstrate that with high probability, any edge in the undirected associated GRG to any WOSN may be emulated by a path of length at most four in the directed RSSG. The authors of [9] also provide sharp bounds on the expected maximum and minimum in and out degree of nodes in a WOSN. However, the results for connectivity of WOSNs in [9] are asymptotic results, which though of great theoretical interest, lack real-world applicability in sensor network scenarios involving finite area deployment regions and number of nodes.

The work of this dissertation follows the probabilistic analysis flavor of [42] and applies the relevance of the node isolation property to network connectivity discussed in [19] with respect to WOSNs. The differentiating features of our research in this regard include consideration for generalized directional sensor network models, which encompass the omnidirectional case considered in [42]. We also consider the effects of hierarchy and clustering on the connectivity of heterogeneous WOSNs that include a sparse network of cluster heads placed randomly within the network. Our analytically

and empirical derivations are presented in Chapter III. Table III presents a limited summary comparing some previous work that has addressed the range assignment problem (and related versions of the problem) for WSNs in general. In the table, `comm` refers to the mode of communication: omnidirectional (RF) based on GRG model or directional; `analysis` refers to the methodology of connectivity analysis: asymptotic or probabilistic; `deployment` refers to the deployment method: deterministic with prior knowledge of location, (e.g., grid), random uniform distribution or stochastic based on any distribution; and `other` refers to other objectives of the methodology employed, such as coverage, energy efficiency, routing or scheduling.

B. Background Survey on Routing and Localization

A rich body of literature has considered various routing and localization techniques specifically designed for WSNs, where energy awareness and consideration for traffic patterns are essential design issues [18, 53–55]. *Routing* is defined as the process of determining and using, in accordance with a set of rules, the route for the transmission of a message from a source to a destination, while *localization* is the process of determining and updating the position of nodes. Because of differences in functionality, network configuration, traffic patterns and hardware constraints between stationary WSNs and mobile ad hoc networks, many of the routing and localization protocols designed for mobile ad hoc networks are not directly applicable to WSNs and will not be reviewed in this dissertation. Distinguishing features which make routing and localization in WSNs challenging include:

- *Constraints in energy supply* of sensor nodes necessitating innovative routing designs that consider strict energy-awareness at all layers of the networking protocol stack in order to extend the WSN's lifetime, while localization schemes

based on costly, energy-draining *geographic positioning systems* (GPS) are infeasible.

- *Traffic patterns* of WSNs in which the flow of data is mainly from multiple sources to a particular destination or vice versa - i.e., nodes-to-base station and base station-to-nodes, in contrast to the flat node-to-node or multicast traffic patterns of ad hoc networks. This encourages a more energy efficient *hierarchical* or clustering routing structure.

- *Data generation pattern* of sensor nodes, typically *data-centric*, resulting from response to a base station query or an event rather than *periodic* in which subsets of nodes periodically send their sensor readings to the base station. In data centric WSNs, attribute-value data is requested or reported based on certain local attributes. For example, the base station may send a [temperature $> 80^o$F] query to the network, and only nodes that sense temperatures greater than 80^oF need report their readings. WSNs are also *application specific* and have a strong requirement for *location awareness* in order to report data collected at their location.

- *Highly correlated* data in the WSN which is typically based on a common phenomena. That is, there is a high probability that data collected by several nodes within the same region will be correlated. Such redundancy needs to be exploited by routing protocols to improve energy and bandwidth utilization via techniques such as *data aggregation* (e.g., duplicate suppression) and *in-network processing*.

- The possibility of *node failure* which may cause frequent and unpredictable topological changes in the network, necessitating fault tolerant designs and ef-

ficient route maintenance.

Due to these differences, a number of efficient and practical routing and localizations schemes that have taken into account the inherent features of WSNs, along with the application and architecture requirements have been proposed. We will not review routing and localization schemes that have been proposed for mobile ad hoc or cellular networks, even if, in some cases, they may indirectly apply to WSNs.

In general, many routing protocols for WSNs attempt to minimize energy usage for the routing protocols while maximizing network life time. Others incorporate various other optimization considerations including data aggregations, data dissemination latency, scalability and low complexity or storage requirements. One naive approach to routing in WSNs is *flooding* or *gossiping*, in which a node simply broadcasts or randomly forwards its data to its local neighborhood or one neighbor, who then recursively broadcasts or forwards this data to their own neighborhoods until the data inadvertently reaches the base station. While nodes have no need to perform neighborhood discovery or to maintain state (i.e., store routing tables), flooding and gossip based routing protocols for WSNs is hugely wasteful of energy and bandwidth, and easily result in packet implosion within the network [18].

To improve on the deficiencies of classic flooding and gossiping, Heinzelman et al. [53] propose a family of adaptive *negotiation based* routing protocols called SPIN, that employs meta-data negotiation and resource (energy) adaptation. SPIN is a simple 3-stage protocol in which nodes send three types of messages: ADV to advertise new data, REQ to request data and DATA which is the actual message. A node with new data to share broadcasts an ADV containing meta-data. Nodes interested in its data, typically the base station, then responds with a REQ message and then the actual DATA is sent by the node to the interested party. Even though nodes are

also not required to maintain any per-neighbor state, the advertisement mechanism of SPIN requires flooding, and it does not guarantee delivery of the data.

In TinyOS flooding [10], the base station sets up routing tables by periodically broadcasting a routing packet to all the nodes in the network. All nodes that receive the broadcast packet from the base station mark the base station as its parent and re-broadcasts the routing packet to all its neighbors. This algorithm continues recursively until all the nodes in the network have received a routing packet, and hence know their parent node in the reversed next hop path toward the base station. Asimilar protocol, the minimum cost forwarding algorithm (MCFA) [54] exploits the fact that the direction of node-to-base station communication is always known (towards the base station) to set up a cost field in the network.

In [55, 56], Intanagonwiwat et al. propose directed diffusion, the first *data centric* and application aware routing paradigm that achieves in-network consolidation of redundant data for WSNs. In directed diffusion the sink floods interests for an attribute-value query through the network. A *query* is an interest defined by an attribute such as name of objects, interval, or geographical area, coupled with the required value, such as "larger than a given threshold". As the interest propagates, they are cached at nodes, who compare any received data with requested values in the query. Gradients are set up to forward any data satisfying the interests back to the base station, using reverse paths. Gradients are reply links to neighbors characterized by the link data rate, duration and expiration time derived from the received query's fields. Therefore by utilizing queries and gradients, multiple paths of varying qualities are established between sink and sources, and one of the paths is selected using reinforcement.

Several other data centric routing schemes that are variants of directed diffusion, such as [57, 58] propose the use of multiple paths to send data concurrently, or

the use of sub-optimal paths with a given probability, to increase network lifetime. Another approach based on directed diffusion, named rumor routing [18] employed flooding to inject queries to the network using long lived agents. However, in contrast to directed diffusion in which data may be routed via multiple routes, rumor routing maintains only one route between source and destination. Another variant of directed diffusion is gradient base routing (GBR) proposed by Shurgers et al. [59], in which nodes measure their "height" as the minimum number of hops required to reach the base station. Packets are then forwarded along the path with the largest gradient, calculated as the difference between a node's height and that of its neighbors. Directed diffusion and its variants do not require node addressing, and there is no need to maintain global network topology. Also data aggregation and interest caching produce huge energy savings and improved latency. However, since they are query driven, they prove unsuitable for applications that require continuous data delivery, such as environmental monitoring.

Another class of routing algorithms for WSNs exploits *hierarchy* or *clustering* to achieve data aggregation, energy efficiency and/or scalability. Hienzelnam, et al. [53] introduce LEACH, the first hierarchical routing algorithm for WSNs. In the setup phase of LEACH, a predetermined fraction of nodes randomly and dynamically elect themselves as cluster heads, who aggregate data from their local clusters before forwarding it directly via one hop to the base station. Each cluster head advertises itself to the rest of the nodes, who then decide to which cluster they should belong based on the signal strength of all their received cluster head advertisements. During the steady state phase of LEACH, nodes sense and transmit data directly to cluster heads. After a certain predetermined period, the network returns to the setup phase again and so that a different set of cluster heads are selected, and so on.

In [60], PEGASIS, a chain-based enhancement over LEACH was proposed, with the idea of only neighbor-to-neighbor communicate for optimal energy and bandwidth utilization. The chain in PEGASIS, formed in a greedy fashion, consists of nodes that are closest to each other forming a path to the base station, while data is aggregated along the path. PEGASIS has been shown to increase network lifetime by about 200% over LEACH by eliminating the overhead of dynamic cluster formation and decreasing the number of required transmission and the average transmission range. A tree-like multi-layer hierarchical extension to PEGASIS which reduces the delay incurred for packets from nodes distant from the base station was introduced in [61]. Unlike event driven routing such as directed diffusion, hierarchical schemes are most appropriate for continuous data collection in WSNs.

Several other hierarchical routing protocols [18] have been proposed. For example, TEEN [62] and its extension APTEEN [63] provide a multi-layer hierarchical routing protocol within a data centric model designed to be responsive to sudden changes in the sensed attributes, calibrated by a soft threshold. Other hierarchical routing protocols include a heterogenous energy-aware routing for cluster-based sensor networks, the self organizing protocol [64], the sensor aggregates routing protocol [65], the virtual grid architecture routing [66] and the hierarchical power-aware routing [67].

Another general class of routing protocols for WSNs are the *location based* algorithms that employ the relative position of nodes to make routing decisions instead of flooding. Nodes are simply assumed to know their locations. One of the earlier papers on geographic routing proposed greedy perimeter stateless routing (GPSR) [68], a non-energy aware protocols which employs planar graphs to route data around the perimeter of obstacles (holes). In geographic and energy aware routing, (GEAR) [69] all routing is directed towards a particular geographical region using energy aware

neighbor selection to route a packet towards the sink's general location, and recursive geographic forwarding or restricted flooding to disseminate the packet inside the destination's vicinity. In the geographic adaptive fidelity (GAF) protocol [70], the network is dynamically divided into fixed zones that form a hierarchical virtual grid. Within each zone, an elected node stays awake to perform sensing and communication for a given period of time while other nodes sleep. This function is then rotated amongst nodes in the zone. Other geographic routing algorithms for WSNs include the greedy other adaptive face routing (GOAFR) [71], SPAN, most forward within radius (MFR), DIR and the geographic distance routing (GEDIR) [72].

One of the main problems with location based routing algorithms is that the position of nodes are assumed to be known. In addition to geographic routing, several WSN applications such as target tracking (requiring nodes to indicate the geographic origin of their sensor data), rely on the ability of the nodes to gain knowledge of their location. Location information can also help security and collaborative signal processing algorithms in WSNs. This necessitates that light weight algorithms for location discovery that are independent of existing infrastructure be explored as resource constraints of nodes preclude the use of expensive and complex localization hardware such as GPS. These algorithms aim to enable randomly distributed, low cost and low complexity nodes to automatically determine their position with respect to some reference point.

Existing location discovery techniques for WSNs have been categorized into two classes: *range based* and *range free*. Range based methods such as [73] employ absolute point-to-point distance or angle estimates, and then apply trilateration or multilateration techniques to find the unknown position of the node. The distance or angle estimates may be obtained from received signal strength indicator (RSSI) measurements, recursive time of arrival (TOA), time difference of arrival (TDOA), or angle

of arrival (AOA) of a signal. Unfortunately, these techniques do not provide enough accuracy in WSNs or require additional hardware. Because range free solutions make no assumptions on the availability or validity of range estimation hardware or mechanisms, it is being pursued as a cost effective alternative to the more expensive range based approaches for WSNs [74].

Many range free methods depend on deducing the geometry of the network based on interactions amongst nodes. While some explore the connectivity information of the communication graph, others depend on the use of a small proportion of beacons or anchors (special class of sensor nodes that are aware of their location e.g. using GPS). Bulusu et al. [75] proposed a crude localization approximation scheme called centroid in which nodes estimate their position as the centroid of the locations of all beacons heard. A variant of centroid uses multiple power levels to provide a better localization accuracy at the expense of increased communication cost. Niculescu and Nath [76] propose DV-hop where each node determines the number of hops to beacons, determines its distance to the beacons using average hop size estimates, and then employs multilateration to determine their absolute location. He et al. propose APIT, in which each node tests to determine if it is within a triangle defined by a 3-tuple of anchors heard by the node. The location of the node is estimated to be the center of gravity of the triangles overlapping region. A similar approach using directional antennas for beacons is employed by Lazos and Poovendran [77]. These algorithms are fully distributed and use local broadcast for communication with immediate neighbors, implying that they have to executed before any multihop routing schemes such as GAF or GEAR is established.

Several of the routing and localization protocols discussed here have optimized for the limited resources of the nodes without consideration for security, and have also considered routing and localization as separate problems. Furthermore, the al-

gorithms have been designed to work in a (mostly) bidirectional network modeled by the GRG, with a few considering link asymmetries due to the use of directional RF antenna [78] or link fading. These schemes, including TINY OS, directed diffusion and their variants, implicitly or explicitly assume that all (or a large proportion) of the network links are bidirectional, and have therefore employed *reverse path routing* in some form. This assumption considers that if a node is able to receive a packet from a neighbor, with probability one, it may consider a return uplink path toward the base station through this neighbor.

Furthermore, in many of the routing protocols for bidirectional networks, listening to periodic messages from neighbors is sufficient to determine a nodes direct neighbors, whereas in a directed network such a mechanism only reveals predecessors, and additional mechanisms are required to provide knowledge of successors. Some popular ad hoc network routing schemes such as dynamic source routing [79], link state routing [80] and distance vector routing [81] have provided modifications that accommodate the discovery of successors in the presence of a limited fraction of directional network links, by either ignoring such links or providing a bi-directional abstraction known as *tunneling* [82–86]. However, the underlying assumption of reverse path routing does not hold for directional WOSNs in which the vast majority of network links are directional. Therefore, previously proposed protocols are inapplicable to WOSNs.

In [27], a novel protocol based on the detection of circuits for routing in purely directional networks was first discussed. The protocol employs link advertisement messages to gain knowledge of a local topology graph. This protocol deals only with point-to-point links. Building upon [27] Huang et al [81] present a similar circuit-based routing algorithm for point-to-multipoint path discovery. Based on the distance vector routing information protocol, each node maintains a “FROM” and “TO” table

of all possible destination which presents a problem for scaling to large networks. In [87], Lou and Wu extend the complexity of the algorithm by designing a multi path routing scheme that stores one optimal circuit per successor to each destination. While all these protocols are cheaper than flooding for directional networks, they only work in small networks and do not scale well to the network size envisioned for WOSNs. Also, special consideration has not been given to hierarchy, security or efficient resource utilization that characterize routing protocols for WSNs.

Besides our work, Diaz et al. [9] are the only other researchers that have considered (separately) routing and localization for hierarchical WOSNs. For localization, they assume cluster heads receive their coordinates from the base station while the remaining nodes recursively employ trilateration to compute their locations based on receiving the coordinates of three other nodes and the angle of incidence of the incoming laser beams. They show that as the network density tends to infinity, with probability one, all network nodes can compute their location within a limited number of iterations. They also discuss a distinct two-part route establishment protocol for the WOSN consisting of the simple-bro protocol initiated by the base station for down-link broadcasting from base station-to-nodes; and the node initiated simple-link protocol for uplink communication from nodes-to-base station. This two step routing scheme is not circuit based, and therefore does not exploit some of the redundancies available within the double procedure. Security is also not considered in this scheme.

C. Security Considerations for Routing and Localization

Current routing protocols suffer from many security vulnerabilities ranging from susceptibility to simple attacks such as injecting malicious routing information to the network to DDoS, and replay attacks. It is therefore crucial to consider security in

the design of network layer protocols [88] in order to safe guard the data and application layers. In [11], a taxonomy of well known routing attacks for WSNs have been highlighted including: the *sybil attack* [89] in which an insider attacker presents itself using multiple identities for the purpose of underscoring fault tolerance schemes; the *sinkhole attack* in which a malicious node strives to lure network traffic to itself by several means, such as advertising itself as the base station or as having a high rate low latency path to the base station; a laptop class form of the sinkhole attack called the *HELLO flood attack* which employs a powerful device to flood advertisements to the entire network; and the powerful *wormhole attack* [90] easily accomplished by an outsider, involving a node tunneling packets through a low latency link to another part of the network, from which it easily launches a replay attack. An attacker may try to exploit the vulnerabilities of a routing algorithm in arbitrary ways, therefore security must be considered at the onset of routing mechanism design. The authors of [11] also point out the various vulnerabilities of popular WSN routing schemes to various attacks.

Several routing protocols for WSNs that have considered security in their design can be broadly categorize into two groups, namely: those requiring asymmetric cryptography solutions, and those that rely on symmetric cryptography. The latter solution is widely popular for WSNs, due to the assumption that the sensor nodes do not have the resources to support the storage and processing requirements for public key cryptography. The most commonly utilized mechanisms that symmetric cryptography solutions rely on to secure the routing function include hash functions, key chains and message authentication codes. A one-way hash function is a function that takes an input of arbitrary length and returns an output of fixed length. Hash functions have the property of being computationally infeasible to reverse, that is, if $h = f(m)$, it is impossible to computer m such that $f(m) = h$.

In [31], Perrig et al. introduce "SPINS" comprised of *Sensor Network Encryption Protocol* (SNEP) for two party data authentication, privacy, integrity and freshness, and μ-Tesla for authenticated data broadcast. μ-Tesla assumes a loosely time-synchronized network and uses the one-way key chain with delayed key disclosure to achieve broadcast authentication in a TinyOS routing scheme. Other secure routing protocols for WSNs have specifically focused on preventing only one or two of the known routing attacks. Secure localization algorithms have even been fewer, with [91] as the pioneer work that discusses robust localization and counter measures for wormhole attacks.

In this dissertation, we introduce an integrated and security-aware routing and localization protocol for directional WOSNs. Our protocol is the first to offer the following distinctive features: Security consideration integrated localization and routing scheme for WOSNs. hierarchical circuit based. The routing protocol incorporates the three crucial components of hierarchy, data centricity and location awareness to yield a robust design that is scalable, secure and resource aware. To the best of our knowledge, this is the first integrated and security-aware routing and localization scheme for a fully directional distributed WSN. Our algorithm is able to establish secure ad hoc routing mechanisms to identify, track and communicate critical data such as the presence of adversaries.

CHAPTER III

CONNECTIVITY ANALYSIS OF THE WOSN

The connectivity of an ad-hoc WSN is one of its essential properties, and is of particular significance in order to maintain communication among nodes. Often, connectivity is viewed as a metric of the robustness, survivability or fault tolerance of networks, and has been related to the network's value [19]. Before we can adequately discuss effective medium access and network layer protocols for WOSNs, such as neighborhood discovery, routing and localization mechanisms, it is imperative to reasonably guarantee the connectivity of the network at the physical layer. In this section, we employ the traditional definition of a *connected* network: for every possible node pair, there exists at least one path (sequence of nodes and edges) connecting them. Considering edge directions, a *strongly connected* directed network is one in which, for every node pair (s_a, s_b), $\exists\ s_a \rightsquigarrow s_b$ and $s_b \rightsquigarrow s_a$ [29]. Unless confusing, we shall refer here to the "strongly connected" property of WOSNs simply as "connected".

This section addresses the fundamental probabilistic parameter assignment problem for WOSNs by asking the question: How can the physical layer network parameters of n, r and α be chosen such that, with high probability p_c, the underlying network graph $G(\mathcal{S}_n, \mathcal{E})$ of the WOSN is connected? Our analysis provides a methodology for, and is of practical importance in choosing parameter values for network level design of ad hoc WOSNs, and more general models of WSNs. We make three important contributions in this section:

1. First, we investigate the node isolation property of WOSNs, and obtain an analytical closed form expression for the probability p_d that no isolated node occurs as a function of network parameters r, n and α.

2. Second, in order to study the tightness of the upper bound that p_d provides as an estimate for p_c, we compare our analytical values of p_d with empirical results of p_d and p_c. Our results demonstrate that similar results derived [42] for omnidirectional WSNs hold in WOSNs as $\alpha \to 2\pi$.

3. Third, we analyze the impact of hierarchy on the connectivity property of WOSNs as a function of the fraction of nodes acting as cluster heads, and empirically demonstrate the enhanced connectivity due to clustering.

A. Relating Node Isolation and Network Connectivity

The occurrence of isolated nodes is undesirable, as their existence undermines the goal of achieving a highly connected network; the existence of a single isolated node implies that the network is necessarily disconnected. However, even though guaranteeing that no isolated nodes occur is not a sufficient condition for connectivity, it is certainly a necessary one, and therefore an important first step towards achieving network connectivity: a connected network implies no isolated node; however the converse is not true [42], as a network with no isolated node does not necessarily imply that the network is connected. Figure 11 illustrates this insufficiency condition in a WOSN scenario. Even though there exists no isolated node, the network is not connected due to link directionality and possible network partitions; for example, path $s_b \rightsquigarrow s_a$ does not exist, even though $s_a \to s_b$ exists. Note that in this example, we have defined as isolated node in the traditional graph theoretic sense for undirected graphs, that is, each node has at least one link connecting it to another node. To consider true network connectedness for WOSNs, in which every pair of nodes is contained in at least one a circuit, it is imperative that we re-define the notion of a *connected* and an *isolated* WOSN node.

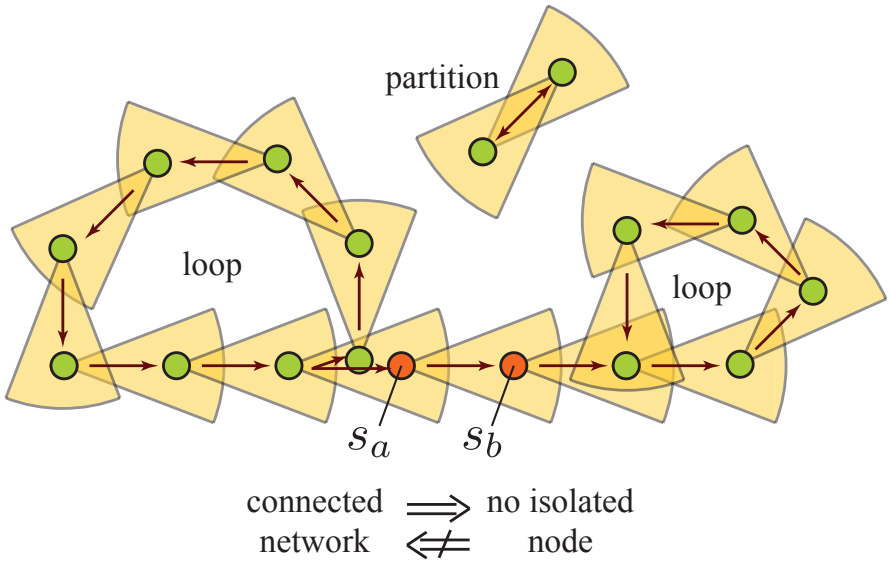


Fig. 11. The WOSN has no isolated nodes, since every node has both an incoming and an outgoing link. However the overall network is not (strongly) connected due to the network partition and link directionality; for example, $s_a \rightarrow s_b$ exists, however $s_b \rightsquigarrow s_a$ does not exist.

An important approach to connectivity analysis in ad hoc networks relates the conditions under which no isolated network nodes exist, to network connectivity. Since an exact closed form analytical expression for the probability p_c of network connectivity in terms of network parameters $(r, \alpha, n/A)$ cannot be obtained, a highly accurate estimate involving the probability p_d that the network contains no isolated node (easily expressed in closed form), is obtained.

Recent studies show that for dense omnidirectional WSNs, (as $n \rightarrow \infty$), the underlying graph is connected with high probability, at the moment (and for the r value) at which no isolated network node occurs [19, 42]. Simply stated, this result implies that p_d provides a *tight upper bound* for p_c as $n \rightarrow \infty$ and for probabilities

close to one[1], and motivates our study of parameter relationships that ensure a "no isolated node" property for WOSNs, and its relevance to network connectivity. One question we answer in this dissertation is; do similar results as obtained in [42] hold for the WOSN network model?

We previously stated the necessity to define two sets of neighbors for each WOSN node within the directed graph paradigm: successors and predecessors. The distinction between successors and predecessors is significant to the connectivity analysis of WOSNs since a given node's successor is necessarily not a predecessor, and as we show later, the probability that a successor is also a predecessor is dependent on the value of α. Before we proceed, it is necessary to define the concept of a *connected* and an *isolated node* in $G_n(\mathcal{S}_n, \mathcal{E})$. The definition of an isolated node is somewhat different for omni-directional networks in which node s_m is isolated if the ball $\mathbb{B}(\Upsilon_m, r_0)$ of center Υ_m and radius r_0 is empty.

- A node $s_i \in \mathcal{S}_n$ is *forward$_K$-isolated* or simply *f$_K$-isolated* if $\delta_i^+ < K$, otherwise it is *f$_K$-connected*, with *b$_K$-isolated* and *b$_K$-connected* similarly defined with respect to δ_i^-. For example, s_i is f_1-isolated if $\delta_i^+ = 0$, and f_1-connected if $\delta_i^+ > 0$.

- A node is *K-connected* if it is both f_K-connected and b_K-connected.

- A node is *directionally-isolated* (or *disolated*) if $\mathcal{S}_i = \emptyset$ but $\mathcal{P}_i$ is non-empty, or vice versa. Similarly, it is *directionally K-isolated* if it is either f_K-isolated or b_K-isolated.

- Node s_i is *completely-isolated* if $\mathcal{S}_i = \mathcal{P}_i = \emptyset$.

[1]This holds for high probability values, which is the interesting case for WSNs.

- Our definition of isolated nodes in $G_n(\mathcal{S}_n, \mathcal{E})$ encompasses both completely isolated and disolated nodes. In our analysis, we desire that no isolated node occurs in order to achieve a fully connected WOSN as per our definition.

- For ease of reference, the 1-connected and directional 1-isolated properties are simply referred to as connected and directionally-isolated, respectively. Where there is no risk of confusion, we will refer to a directionally-isolated WOSN node simply as an isolated node.

- There is no K-isolated WOSN node in $G_n(\mathcal{S}_n, \mathcal{E})$ if $\forall s_i \in \mathcal{S}_n, \delta_i^+ \geq K$, and $\delta_i^- \geq K$.

- Finally, an event A is said to occur almost surely (a.s.) if the probability of event A denoted as Pr[A] is greater than 0.99.

B. Analysis on Node Isolation

Consider the following r-assignment problem for the n-node WOSN stated as follows: what is the minimum r, such that for a fixed α value, with high probability p_d, a node is not isolated? A similar α-assignment problem is: Given n nodes with a fixed r, what is the minimum α such that no isolated node occurs in the WOSN with probability p_d?

1. Probability of No Isolated WOSN Node

To gain insight to these parameter assignment problems, our first step is to consider the probability p_d^i that a node $s_i \in \mathcal{S}_n$ is not isolated. Let p_f^i =Pr$[\delta_i^+ > 0]$ and p_b^i =Pr$[\delta_i^- > 0]$ denote the probabilities that s_i is not f_1-isolated and b_1-isolated, respectively. Recall that the set of directionally isolated nodes consists of the union

of f_1-isolated and b_1-isolated nodes, and the probability that s_i is isolated is:

$$\Pr[\{\delta_i^+ = 0\} \cup \{\delta_i^- = 0\}],$$

while s_i is connected (i.e., not isolated) if it is both f_1-connected *and* b_1-connected with probability p_d^i given as:

$$p_d^i = p_{f \cap b}^i = p_f^i . p_{b|f}^i \tag{3.1}$$

where $\cup$ and $\cap$ are the union and intersection operators, respectively, and $p_{f \cap b}^i$ denotes the probability that s_i is both b_1-connected and f_1-connected, and $p_{b|f}^i$ is the conditional probability that s_i is b_1-connected given it is f_1-connected. Our next step towards determining p_d^i is to evaluate p_f^i and $p_{b|f}^i$.

a. Evaluating p_f^i

Lemma B.1 For $n \to \infty$ and $r \ll 1$, s_i is f_1-connected with probability:

$$p_f^i = Pr[\delta_i^+ \geq 1] = 1 - e^{\frac{-n\alpha r^2}{2}} \tag{3.2}$$

Proof of Lemma B.1 For this proof, we employ quadrat[2] statistical methods which is an approach taken to quantify spatial point patterns (see Chapter 8 of [25]). Under this model, quadrats of random location and orientation are sampled, the number of events in the quadrat are counted, and statistics derived from the counts. It is well known [24, 25, 36, 49] that the number of points located in a quadrat of area A_q, follows a Poisson distribution of parameter λA_q, where λ is the intensity of the Poisson process. Viewing communication sectors as quadrats, the random variable δ_i^+ counting the number of nodes located in s_i's communication sector Φ_i of area $\alpha r^2/2$ is

[2]Quadrats are bounded regions of any possible shape including Φ.

then a Poisson point process with parameter $n\alpha r^2/2$, and probability density function (pdf):

$$\Pr[\delta_i^+ = z] = \frac{e^{\frac{-n\alpha r^2}{2}} \left(\frac{n\alpha r^2}{2}\right)^z}{z!} \tag{3.3}$$

The probability that s_i is f_1-isolated (i.e., Φ_i is empty) is

$$\Pr[\delta_i^+ = 0] = e^{\frac{-n\alpha r^2}{2}}$$

and the probability p_f^i that s_i is f_1-connected (i.e., at least one node in Φ_i) is:

$$\Pr[\delta_i^+ \geq 1] = \sum_{z=1}^{n-1} \frac{e^{\frac{-n\alpha r^2}{2}} (\frac{n\alpha r^2}{2})^z}{z!} = 1 - e^{\frac{-n\alpha r^2}{2}}, \tag{3.4}$$

yielding the result of Lemma B.1. The derivation of Equation 3.4 employs the series approximation of the exponential function for large n and small αr^2, given below:

$$e^x = \sum_{z=0}^{\infty} \frac{x^z}{z!} = 1 + \sum_{z=1}^{\infty} \frac{x^z}{z!}.$$

b. Evaluating p_b^i

Lemma B.2 For $n \to \infty$ and $r \ll 1$, s_i is b_1-connected with probability p_b^i equal to p_f^i.

Proof of Lemma B.2 The b_1-connectivity problem is analogous to an area coverage problem, in which a point is "covered" if it lies within the area of the communication sector of any other node. Obviously, s_i is b-connected if $\Upsilon_i \in \Phi_j$ for any $j \neq i$. The proof is constructed from concepts in stochastic geometry [24], similar to the proof of area coverage derived for the general case in [36]. Consider the WOSN with n nodes as points that are uniformly located in a unit area region. The probability that any point Υ_i (which is the position of node s_i) does not fall

within an arbitrary sensor's communication sector equals $(1-\alpha r^2/2)$ where $\alpha r^2/2$ is the area of the sector. Conditioned on the number of nodes n, the probability that s_i is not covered is $(1-\alpha r^2/2)^n$ [24]. For large n and $r << 1$, this Binomial is well approximated as a Poisson so that:

$$\Pr[s_i \text{ is not covered}] = e^{\frac{-n\alpha r^2}{2}},$$

and the probability p_b^i that s_i is b-connected (i.e., it is covered) is then obtained as:

$$p_b^i = 1 - e^{\frac{-n\alpha r^2}{2}}. \tag{3.5}$$

The result of Lemma B.2 follows.

c. Evaluating $p_{b|f}^i$

Lemma B.3 For $n \to \infty$ and $\alpha r^2 \ll 1$, s_i is b_1-connected given it is f_1-connected with probability $p_{b|f}^i$ given as:

$$p_{b|f}^i = 1 - \frac{e^{\frac{-n\alpha r^2}{2}}}{1-e^{\frac{-n\alpha r^2}{2}}}\left(1-\frac{\alpha r^2}{2}\right)^{n-1}\left(e^{\left[\frac{n\alpha r^2(2\pi-\alpha)}{2\pi(2-\alpha r^2)}\right]}-1\right).$$

Proof of Lemma B.3 Assume s_i is f-connected ($\mathcal{S}_i \neq \emptyset$) so that $\delta_i^+ \geq 1$. We wish to evaluate

$$p_{b|f}^i = \Pr[\delta_i^- \geq 1 | \delta_i^+ \geq 1].$$

where $\delta_i^+ \in \mathbb{Z}[1,n]$ and $\delta_i^- \in \mathbb{Z}[0,n-1]$ represent the random variables counting the number of s_i's successors and predecessors, respectively, and $\mathbb{Z}$ is the set of integers. Following our model with independently deployed nodes assumed, to obtain $p_{b|f}^i$, we consider two disjoint cases for which s_i can attain b-connectivity given it is already f-connected:

Case 1 : The event that s_i has no bi-directional link with any of its successors, de-

noted [no bi], implying that of the $\delta_i^+ = z$ nodes in Φ_i, none are oriented to cover s_i. In this case, s_i may only be b-connected if it has established a link with at least one of the $n - z - 1$ other nodes not in Φ_i, termed *non-successor nodes*. This event is referred to as [no bi].

Case 2 : The event that s_i has at least one bi-directional link with one of its successors. That is, at least one successor is also a predecessor, (s_i also falls in the communication sector of at least one of the nodes in Φ_i) so that s_i is b-connected by any of the z successor nodes in Φ_i. This event is referred to as [at least one bi].

Due to the disjointness of case 1 and case 2, we can write:

$$\begin{aligned} p^i_{b|f} &= \Pr[\delta_i^- \geq 1 | \delta_i^+ \geq 1] \\ &= 1 - \Pr[\delta_i^- = 0 | \delta_i^+ \geq 1] \\ &= 1 - \big\{\Pr[\delta_i^- = 0 | \delta_i^+ \geq 1, \text{no bi}].\Pr[\text{no bi}]\big\} \\ &\quad - \big\{\Pr[\delta_i^- = 0 | \delta_i^+ \geq 1, \text{at least one bi}].\Pr[\text{at least one bi}]\big\} \end{aligned} \tag{3.6}$$

Observe that $\Pr[\delta_i^- = 0 | \delta_i^+ \geq 1, \text{at least one bi}] = 0$, since $\delta_i^- = 0$ contradicts the case that [at least one bi] exists, so that Equation 3.6 above simplifies as:

$$\begin{aligned} p^i_{b|f} &= 1 - \big\{\Pr[\delta_i^- = 0 | \delta_i^+ \geq 1, \text{no bi}].\Pr[\text{no bi}]\big\} \\ &= 1 - \sum_{z=1}^{n-1} \Pr[\delta_i^- = 0 | \delta_i^+ = z, \delta_i^+ \geq 1, \text{no bi}].\Pr[\text{no bi} | \delta_i^+ = z, \delta_i^+ \geq 1] \\ &\qquad \times \quad \Pr[\delta_i^+ = z | \delta_i^+ \geq 1] \end{aligned} \tag{3.7}$$

Following our model of assuming uniformly random sector orientation, the probability of a bidirectional link existing between s_i and any of its successors s_j, denoted as $\Pr[s_j \rightarrow s_i | s_i \rightarrow s_j] = \alpha/2\pi$, so that the probability that no bidirectional link exists between s_i and any of its $\delta_i^+ = z$ successors ($\delta_i^+ \geq 1$) equals $(1 - \alpha/2\pi)^z$. For independently deployed nodes, given that s_i is f-connected we have that:

$$\Pr[\text{no bi} \mid \delta_i^+ = z, \delta_i^+ \geq 1] = (1 - \frac{\alpha}{2\pi})^z, \qquad \text{for} \quad z = 1, 2, \cdots n-1. \tag{3.8}$$

Given our unit area deployment region, we have that:

$$\Pr[\delta_i^- = 0 | \delta_i^+ = z, \delta_i^+ \geq 1, \text{no bi}] = \left(1 - \frac{\alpha r^2}{2}\right)^{n-z-1}, \tag{3.9}$$

and

$$\begin{aligned} \Pr[\delta_i^+ = z | \delta_i^+ \geq 1] &= \frac{\Pr[(\delta_i^+ = z) \cap (\delta_i^+ \geq 1)]}{\Pr[\delta_i^+ \geq 1]} \\ &= \frac{(\frac{n\alpha r^2}{2})^z e^{\frac{-n\alpha r^2}{2}}}{z!} . \frac{1}{1 - e^{\frac{-n\alpha r^2}{2}}} \end{aligned} \tag{3.10}$$

where:

$$\Pr[(\delta_i^+ = z) \cap (\delta_i^+ \geq 1)] = \begin{cases} \Pr[\delta_i^+ = z] & \text{for} \quad z > 0 \\ 0 & \text{for} \quad z = 0 \end{cases}$$

Equation 3.10 employs the more accurate approximation for $\Pr(\delta_i^- = 0 | \delta_i^+ = z, \text{no bi})$ as Binomial$(\alpha r^2/2)$ for $z = 1, 2, \cdots n-1$, as the Poisson approximation is only valid for large n and small z values (see the Appendix). Substituting Equations

3.8, 3.9 and 3.10 into Equation 3.7, yields:

$$\begin{aligned} p^i_{b|f} &= 1 - \sum_{z=1}^{n-1} \left(1 - \frac{\alpha r^2}{2}\right)^{n-z-1} .(1 - \frac{\alpha}{2\pi})^z . \left[\frac{(\frac{n\alpha r^2}{2})^z e^{\frac{-n\alpha r^2}{2}}}{z!} . \frac{1}{1 - e^{\frac{-n\alpha r^2}{2}}}\right] \\ &= 1 - \frac{e^{\frac{-n\alpha r^2}{2}}}{1 - e^{\frac{-n\alpha r^2}{2}}} \left(1 - \frac{\alpha r^2}{2}\right)^{n-1} \sum_{z=1}^{n-1} \left(\frac{2\pi - \alpha}{2\pi} . \frac{2}{2 - \alpha r^2}\right)^z . \left[\frac{(\frac{n\alpha r^2}{2})^z}{z!}\right] \\ &= 1 - \frac{e^{\frac{-n\alpha r^2}{2}}}{1 - e^{\frac{-n\alpha r^2}{2}}} \left(1 - \frac{\alpha r^2}{2}\right)^{n-1} \sum_{z=1}^{n-1} \frac{\left[\frac{n\alpha r^2(2\pi-\alpha)}{2\pi(2-\alpha r^2)}\right]^z}{z!} \end{aligned} \tag{3.11}$$

Now, employing the series approximation of an exponential for large n and small αr^2, yields:

$$p^i_{b|f} = 1 - \frac{e^{\frac{-n\alpha r^2}{2}}}{1 - e^{\frac{-n\alpha r^2}{2}}} \left(1 - \frac{\alpha r^2}{2}\right)^{n-1} \left(e^{\left[\frac{n\alpha r^2(2\pi-\alpha)}{2\pi(2-\alpha r^2)}\right]} - 1\right), \tag{3.12}$$

the result of Lemma B.3.

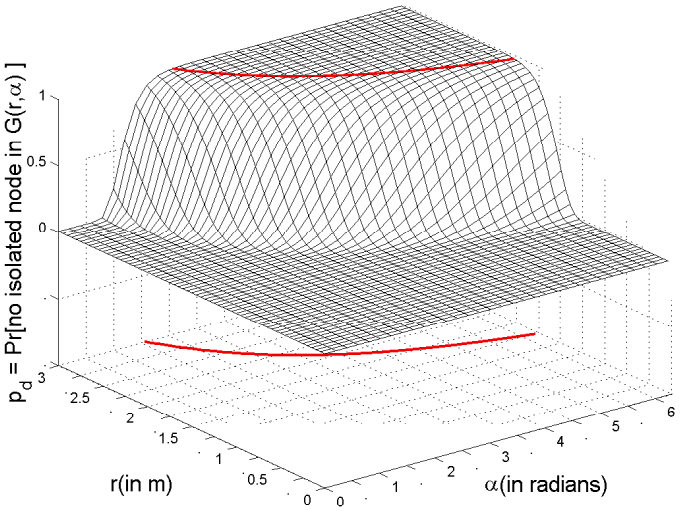
Observe that for the omnidirectional case with $\alpha = 2\pi$, $p^i_{b|f} = 1$ as expected. That is, with the RGG communication model and all links bidirectional, if a node is f-connected, then of course it is also b-connected. It is clear that $p^i_{b|f} \geq p^i_b$ due to the possibility of bidirectional links.

d. Evaluating p^i_d

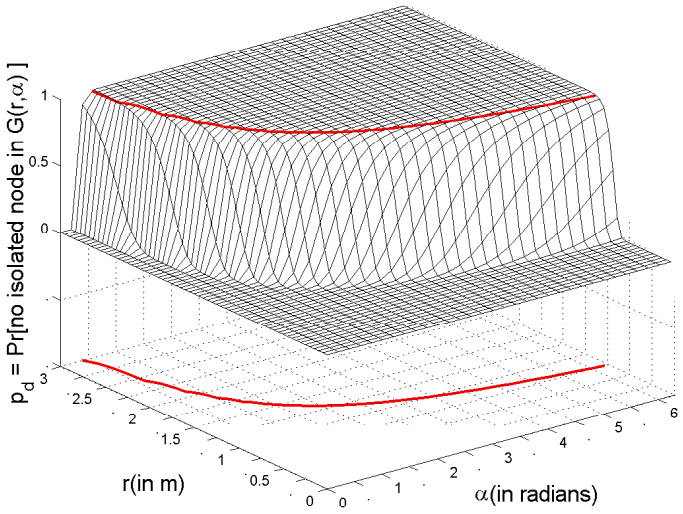
Substituting Equations 3.4 and 3.12 into Equation 3.1, and simplifying yields:

$$p^i_d = \left[1 - e^{\frac{-n\alpha r^2}{2}}\right] \left[1 - \frac{e^{\frac{-n\alpha r^2}{2}}}{1 - e^{\frac{-n\alpha r^2}{2}}} \left(1 - \frac{\alpha r^2}{2}\right)^{n-1} \left(e^{\left[\frac{n\alpha r^2(2\pi-\alpha)}{2\pi(2-\alpha r^2)}\right]} - 1\right)\right] \tag{3.13}$$

Observe that $p^i_f \geq p^i_d$ for large n and small αr^2 with equality when $\alpha = 2\pi$.

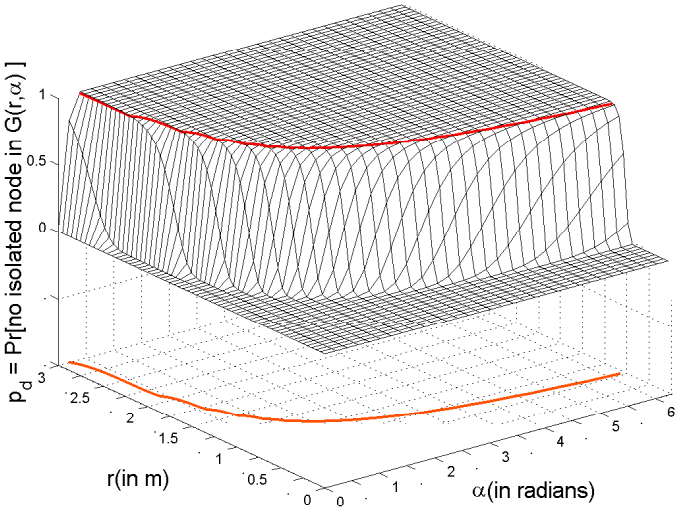


(a) $n = 100$

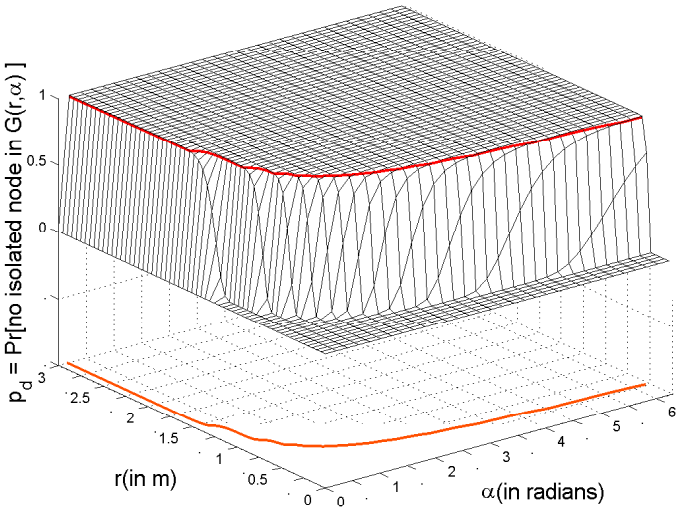


(b) $n = 500$

Fig. 12. Depicting the mesh plot of the probability p_d that no isolated node occurs in $G_n(\mathcal{S}_n, \mathcal{E})$ with varying r and α values for different node densities n. The red line indicates the (r, α) pair values for which $p_d = 0.99$.

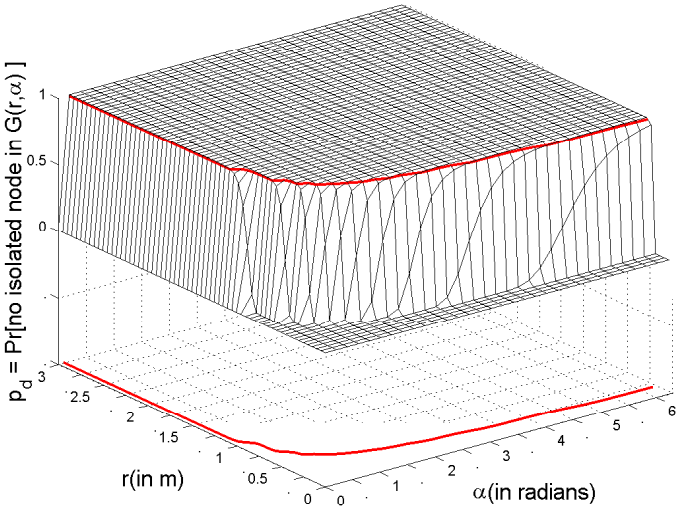


(c) $n = 1,000$

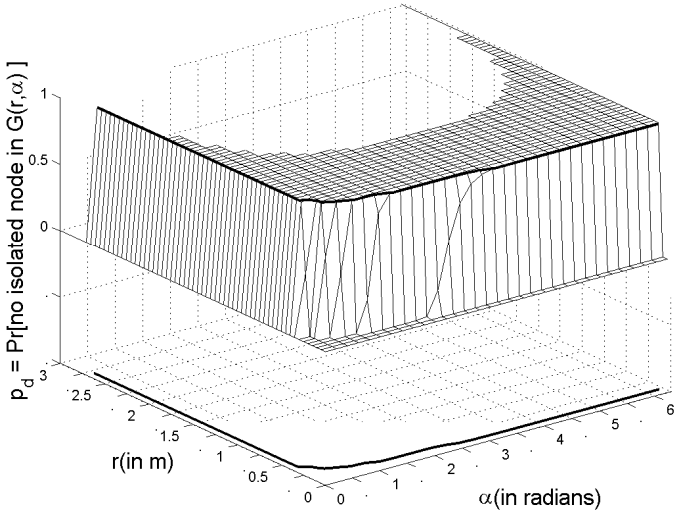


(d) $n = 5,000$

Fig. 12 continued.



(e) $n = 10,000$



(f) $n = 100,000$

Fig. 12 continued.

e. Evaluating p_d

Theorem B.4 For $n \to \infty$ and small αr^2, there is no isolated node in $G_n(\mathcal{S}_n, \mathcal{E})$ with probability p_d:

$$p_d = \left[1 - e^{\frac{-n\alpha r^2}{2}}\right]^n \left[1 - \frac{e^{\frac{-n\alpha r^2}{2}}}{1 - e^{\frac{-n\alpha r^2}{2}}} \left(1 - \frac{\alpha r^2}{2}\right)^{n-1} \left(e^{\left[\frac{n\alpha r^2(2\pi-\alpha)}{2\pi(2-\alpha r^2)}\right]} - 1\right)\right]^n \tag{3.14}$$

Proof of theorem B.4 Assuming statistical independence among events that distinct nodes are isolated, Theorem B.4 follows by computing p_d for n nodes as:

$$p_d = \begin{pmatrix} n \\ n \end{pmatrix} (p_d^i)^n (1 - p_d^i)^0 \tag{3.15}$$

where the expression for p_d^i is given in Equation 3.13. For $\alpha = 2\pi$ we note that p_d reduces to $(1 - e^{-n\pi r^2})^n$ as obtained by Bettsetter [42]. It therefore turns out that Equation 3.14 is the expression relating network parameters n, r and α with the probability p_d that no isolated node occurs for WSNs in general.

Figure 12 illustrates p_d for a range of r and α values for different n values with the (red) line on the $r - \alpha$ plane of each mesh plot indicating the (r, α)-pair values for which there is almost surely ($p_d = 0.99$) no isolated node. We observe that as node density n increases, network connectivity improves, and for a very dense network with $n = 100,000$, parameter value pairs as small as $(r = .01, \alpha = 6\pi/25)$ yield a network with almost surely no isolated node.

Example 1: (Simulation Study): We perform a simulation-based study of a WOSN to investigate the connectivity property. Employing a uniform random generator we position n WOSN nodes in a square planar region of area 1 km^2, following our deployment model. We aim to determine the minimum parameter values that achieve a WOSN in which, with high probability (> 0.99), no node is isolated. From the analytical expression of Equation 3.14, we obtain the minimum r and corresponding α

Table IV. The minimum r value for corresponding network parameter (n, α) pair values that achieve $p_d \geq 0.99$ in $G_n(\mathcal{S}_n, \mathcal{E})$.

n	$\alpha = \frac{\pi}{9}$	$\alpha = \frac{2\pi}{9}$	$\alpha = \frac{\pi}{3}$	$\alpha = \frac{\pi}{2}$	$\alpha = \frac{3\pi}{4}$	$\alpha = \pi$	$\alpha = \frac{3\pi}{2}$	$\alpha = 2\pi$
100	0.755	0.527	0.426	0.345	0.281	0.243	0.198	0.172
500	0.360	0.253	0.205	0.167	0.136	0.118	0.096	0.083
1000	0.262	0.184	0.150	0.122	0.099	0.086	0.070	0.061
5000	0.125	0.088	0.072	0.058	0.048	0.041	0.034	0.029
10000	0.091	0.064	0.052	0.042	0.035	0.030	0.025	0.021
100000	0.011	0.008	0.006	0.005	0.004	0.004	0.003	0.003

required for $p_d \geq 0.99$ with n given, as shown in Table IV.

For example, observe that for $n = 1000$ and $\alpha = 2\pi/9$, $p_d \geq 0.99$ is achieved with $r \geq 0.184$ km. If however the WOSN nodes are only capable of achieving $r = 0.09$ km for the same α, then we need at least ~ 5000 nodes, or at design time, we may choose to increase α to π in order to deploy the same $n = 1000$ nodes and obtain the same confidence for p_d. With $n = 500$ nodes and $\alpha = 2\pi/9$, $\alpha = \pi/2$ and $\alpha = \pi$ we obtain $p_d \geq 0.99$ with $r \geq 0.253$ km, $r \geq 0.167$ km and $r \geq 0.118$ km respectively. This compares with $r \geq 0.083$ km value obtained in [42] for $n = 500$ nodes in the omnidirectional network scenario.

Interestingly, we observe that for the same confidence on p_d, doubling r allows us reduce α by approximately a fourth. An interesting study beyond the scope of this work would involve comparing the practical cost (dollar, energy) of increasing r while reducing α (or vice versa) to determine the optimal WOSN node (r, α)-parameter configuration based on a given cost function.

2. Probability of No K-isolated WOSN Node

It is necessary to consider K-connectivity in the design of robust and secure networks in order to accommodate link and/or node failures or compromise. A *K-connected network* is defined as one that remains connected after the failure of any choice of $(K-1)$ nodes. To gain insight into K-connectivity for the WOSN, similar to previous analysis we first consider the probability p_{d_K} that no isolated node occurs in the network, and its relationship to the network parameters n, r, α.

Obviously, a given node s_i is K-connected (i.e., not K-isolated) with probability:

$$p^i_{d_K} = p^i_{f_K \cap b_K} = p^i_{f_K} . p^i_{b_K|f_K}, \tag{3.16}$$

where $p^i_{f_K}$ is the probability that s_i is f_K-connected, and $p^i_{b_K|f_K}$ is the probability that s_i is b_K-connected, given it is f_K-connected. The probability p_{d_K} that no K-isolated node occurs in the n-node network, assuming independence among events that distinct nodes are isolated, is then $p_{d_K} = (p^i_{d_K})^n$. We are now left to derive $p^i_{f_K}$ and $p^i_{b_K|f_K}$.

By similar arguments, we easily extend the results of Lemmas B.1 and B.2 for f_1- and b_1-connectedness to the f_K- and b_K-connected cases, respectively, and conclude that the probability $p^i_{f_K} = \Pr[\delta^+_i \geq K]$ that s_i is f_K-connected is equivalent to the probability $p^i_{b_K} = \Pr[\delta^-_i \geq K]$ that s_i is b_K-connected, given as:

$$p^i_{f_K} = \Pr[\delta^+_i \geq K] \;=\; \sum_{m=K}^{n-1} \frac{e^{\frac{-n\alpha r^2}{2}} (\frac{n\alpha r^2}{2})^m}{m!} = p^i_{b_K} \tag{3.17}$$

while

$$p^i_{b_K|f_K} = \Pr[\delta^-_i \geq K | \delta^+_i \geq K] \;=\; 1 - \Pr[\delta^-_i < K | \delta^+_i \geq K] \tag{3.18}$$

Equations 3.17 and 3.18 yield the basis for deriving p_{d_K} by following similar arguments

employed for the $K = 1$ case. As an illustration, we derive p_{d_K} for $K = 2$ in the next section.

a. Case for K = 2

From Equation 3.17 we readily obtain that:

$$p^i_{f_2} = \Pr[\delta_i^+ \geq 2] = \sum_{z=2}^{n-1} \frac{e^{\frac{-n\alpha r^2}{2}}(\frac{n\alpha r^2}{2})^z}{z!} = 1 - e^{\frac{-n\alpha r^2}{2}}\left(1 + \frac{n\alpha r^2}{2}\right) \tag{3.19}$$

Since $\Pr[\delta_i^+ \geq 2] = 1 - \Pr[\delta_i^+ = 0] - \Pr[\delta_i^+ = 1]$, where

$$\Pr[\delta_i^+ = 0] = e^{\frac{-n\alpha r^2}{2}} \quad \text{and} \quad \Pr[\delta_i^+ = 1] = \frac{n\alpha r^2}{2} e^{\frac{-n\alpha r^2}{2}}.$$

To derive $p^i_{b_2|f_2}$ we employ the following:

$$\begin{aligned}
p^i_{b_2|f_2} &= \Pr[\delta_i^- \geq 2 | \delta_i^+ \geq 2] \\
&= 1 - \Pr[\delta_i^- < 2 | \delta_i^+ \geq 2] \\
&= 1 - \Pr[\delta_i^- = 0 | \delta_i^+ \geq 2] - \Pr[\delta_i^- = 1 | \delta_i^+ \geq 2] \\
&= 1 - \Pr[\delta_i^- = 0 | \delta_i^+ \geq 2, \text{no bi}].\Pr[\text{no bi}] \\
&\quad -\Pr[\delta_i^- = 1 | \delta_i^+ \geq 2, \text{no bi}].\Pr[\text{no bi}] \\
&\quad -\Pr[\delta_i^- = 0 | \delta_i^+ \geq 2, \text{at least one bi}].\Pr[\text{at least one bi}] \\
&\quad -\Pr[\delta_i^- = 1 | \delta_i^+ \geq 2, \text{exactly one bi}].\Pr[\text{exactly one bi}] \\
&\quad -\Pr[\delta_i^- = 1 | \delta_i^+ \geq 2, \text{at least two bi}].\Pr[\text{at least two bi}]
\end{aligned} \tag{3.20}$$

But $\Pr[\delta_i^- = 0 | \delta_i^+ \geq 2, \text{at least one bi}] = \Pr[\delta_i^- = 1 | \delta_i^+ \geq 2, \text{at least two bi}] = 0$, so:

$$\begin{aligned} p^i_{b_2|f_2} &= 1 - \underbrace{\Pr[\delta_i^- = 0 | \delta_i^+ \geq 2, \text{no bi}].\Pr[\text{no bi}]}_{part1} \\ &\quad - \underbrace{\Pr[\delta_i^- = 1 | \delta_i^+ \geq 2, \text{no bi}].\Pr[\text{no bi}]}_{part2} \\ &\quad - \underbrace{\Pr[\delta_i^- = 1 | \delta_i^+ \geq 2, \text{exactly one bi}].\Pr[\text{exactly one bi}]}_{part3} \end{aligned} \tag{3.21}$$

where part 1 is:

$$\sum_{z=2}^{n-1} \Pr[\delta_i^- = 0 | \delta_i^+ = z, \delta_i^+ \geq 2, \text{no bi}].\Pr[\text{no bi} | \delta_i^+ = z, \delta_i^+ \geq 2].\Pr[\delta_i^+ = z | \delta_i^+ \geq 2],$$

part 2 is:

$$\sum_{z=2}^{n-1} \Pr[\delta_i^- = 1 | \delta_i^+ = z, \delta_i^+ \geq 2, \text{no bi}].\Pr[\text{no bi} | \delta_i^+ = z, \delta_i^+ \geq 2].\Pr[\delta_i^+ = z | \delta_i^+ \geq 2],$$

and part 3 is:

$$\sum_{z=2}^{n-1} \Pr[\delta_i^- = 1 | \delta_i^+ = z, \delta_i^+ \geq 2, \text{one bi}].\Pr[\text{one bi} | \delta_i^+ = z, \delta_i^+ \geq 2].\Pr[\delta_i^+ = z | \delta_i^+ \geq 2].$$

Now, we have that for $z = 2, 3, \cdots n-1$:

$$\Pr[\text{no bi } | \delta_i^+ = z, \delta_i^+ \geq 2] = (1 - \frac{\alpha}{2\pi})^z, \tag{3.22}$$

and

$$\Pr[\text{one bi} | \delta_i^+ = z, \delta_i^+ \geq 2] = z\frac{\alpha}{2\pi}(1 - \frac{\alpha}{2\pi})^{z-1}, \tag{3.23}$$

and

$$\Pr[\delta_i^+ = z | \delta_i^+ \geq 2] = \frac{\Pr[(\delta_i^+ = z) \cap (\delta_i^+ \geq 2)]}{\Pr[\delta_i^+ \geq 2]} = \frac{(\frac{n\alpha r^2}{2})^z e^{\frac{-n\alpha r^2}{2}}}{z! \left[1 - e^{\frac{-n\alpha r^2}{2}}(1 + \frac{n\alpha r^2}{2})\right]} \tag{3.24}$$

and

$$\Pr[\delta_i^- = 0 | \delta_i^+ = z, \delta_i^+ \geq 2, \text{no bi}] = \left(1 - \frac{\alpha r^2}{2}\right)^{n-z-1} \tag{3.25}$$

and

$$\Pr[\delta_i^- = 1 | \delta_i^+ = z, \delta_i^+ \geq 2, \text{no bi}] = (n - z - 1) \left(\frac{\alpha r^2}{2}\right) \left(1 - \frac{\alpha r^2}{2}\right)^{n-z-2} \tag{3.26}$$

and

$$\Pr[\delta_i^- = 1 | \delta_i^+ = z, \delta_i^+ \geq 2, \text{exactly one bi}] = \left(1 - \frac{\alpha r^2}{2}\right)^{n-z-1}. \tag{3.27}$$

where

$$\Pr[(\delta_i^+ = z) \cap (\delta_i^+ \geq 2)] \quad = \quad \begin{cases} \Pr[\delta_i^+ = z] & \text{for} \quad z \geq 2 \\ 0 & \text{for} \quad z = 0, 1 \end{cases}$$

and

$$\Pr[\delta_i^- = k] = \binom{n - z - 1}{k} \left(\frac{\alpha r^2}{2}\right)^k \left(1 - \frac{\alpha r^2}{2}\right)^{n-z-1-k}.$$

Substituting Equations 3.22, 3.24 and 3.25 into part 1 of Equation 3.21, we have:

Part 1:

$$\sum_{z=2}^{n-1} \Pr[\delta_i^- = 0 | \delta_i^+ = z, \delta_i^+ \geq 2, \text{no bi}].\Pr[\text{no bi} | \delta_i^+ = z, \delta_i^+ \geq 2].\Pr[\delta_i^+ = z | \delta_i^+ \geq 2]$$

$$= X \sum_{z=2}^{n-1} \frac{\left(1 - \frac{\alpha}{2\pi}\right)^z \left(1 - \frac{\alpha r^2}{2}\right)^{n-1-z} \left(\frac{n\alpha r^2}{2}\right)^z}{z!} = X \left(1 - \frac{\alpha r^2}{2}\right)^{n-1} \sum_{z=2}^{n-1} \frac{\left(\frac{n\alpha r^2(2\pi - \alpha)}{2\pi(2 - \alpha r^2)}\right)^z}{z!}$$

$$= X \left(1 - \frac{\alpha r^2}{2}\right)^{n-1} \sum_{z=2}^{n-1} \frac{Q^z}{z!} \qquad = \qquad X \left(1 - \frac{\alpha r^2}{2}\right)^{n-1} \left(e^Q - Q - 1\right)$$

where

$$X = \frac{e^{\frac{-n\alpha r^2}{2}}}{1 - (1 + \frac{n\alpha r^2}{2}) e^{\frac{-n\alpha r^2}{2}}} \qquad \text{and} \qquad Q = \left[\frac{n\alpha r^2(2\pi - \alpha)}{2\pi(2 - \alpha r^2)}\right],$$

and the series approximation of the exponential is employed assuming large n and small αr^2. Substituting Equations 3.22, 3.24 and 3.26 into part 2 of Equation 3.21, we have that:

Part 2:

$$\sum_{z=2}^{n-1} \Pr[\delta_i^- = 1 | \delta_i^+ = z, \delta_i^+ \geq 2, \text{no bi}].\Pr[\text{no bi} | \delta_i^+ = z, \delta_i^+ \geq 2].\Pr[\delta_i^+ = z | \delta_i^+ \geq 2]$$

$$= X\frac{\alpha r^2}{2} \sum_{z=2}^{n-1} (n-1-z) \frac{\left(1-\frac{\alpha}{2\pi}\right)^z \left(1-\frac{\alpha r^2}{2}\right)^{n-2-z} \left(\frac{n\alpha r^2}{2}\right)^z}{z!}$$

$$= X\frac{\alpha r^2}{2} \left(1-\frac{\alpha r^2}{2}\right)^{n-2} \sum_{z=2}^{n-1} \frac{(n-1)\left(\frac{n\alpha r^2(2\pi-\alpha)}{2\pi(2-\alpha r^2)}\right)^z}{z!} - \frac{z\left(\frac{n\alpha r^2(2\pi-\alpha)}{2\pi(2-\alpha r^2)}\right)^z}{z!}$$

$$= X\frac{\alpha r^2}{2} \left(1-\frac{\alpha r^2}{2}\right)^{n-2} \left\{(n-1)(e^Q - Q - 1) - Q\sum_{z=2}^{n-1} \frac{Q^{z-1}}{(z-1)!}\right\} \tag{3.28}$$

$$= X\frac{\alpha r^2}{2} \left(1-\frac{\alpha r^2}{2}\right)^{n-2} \left\{(n-1)(e^Q - Q - 1) - Q\sum_{y=1}^{n-2} \frac{Q^y}{y!}\right\}$$

$$= X\frac{\alpha r^2}{2} \left(1-\frac{\alpha r^2}{2}\right)^{n-2} \left\{(n-1)(e^Q - Q - 1) - Q(e^Q - 1)\right\} \tag{3.29}$$

Where we employed the change of variable $y = z - 1$ in Equation 3.28, and again, employed the series approximation for the exponential for n large and αr^2 small.

Similarly, substituting Equations 3.23, 3.24 and 3.27 into part 3 of Equation 3.21, we obtain for large n and small αr^2 that:

Part 3:

$$\begin{aligned}
&\sum_{z=2}^{n-1} \Pr[\delta_i^- = 1 | \delta_i^+ = z, \delta_i^+ \geq 2, \text{one bi}].\Pr[\text{one bi} | \delta_i^+ = z, \delta_i^+ \geq 2].\Pr[\delta_i^+ = z | \delta_i^+ \geq 2] \\
= \; & X \frac{\alpha}{2\pi} \sum_{z=2}^{n-1} \frac{z \left(1 - \frac{\alpha}{2\pi}\right)^{z-1} \left(1 - \frac{\alpha r^2}{2}\right)^{n-z-1} \left(\frac{n\alpha r^2}{2}\right)^z}{z!} \\
= \; & X \frac{n\alpha^2 r^2}{4\pi} \left(1 - \frac{\alpha r^2}{2}\right)^{n-2} \sum_{z=2}^{n-1} \frac{\left(1 - \frac{\alpha}{2\pi}\right)^{z-1} \left(\frac{2}{2-\alpha r^2}\right)^{z-1} \left(\frac{n\alpha r^2}{2}\right)^{z-1}}{(z-1)!} \\
= \; & X \frac{n\alpha^2 r^2}{4\pi} \left(1 - \frac{\alpha r^2}{2}\right)^{n-2} \sum_{z=2}^{n-1} \frac{\left(\frac{2n\alpha r^2(2\pi-\alpha)}{4\pi(2-\alpha r^2)}\right)^{z-1}}{(z-1)!} \\
= \; & X \frac{n\alpha^2 r^2}{4\pi} \left(1 - \frac{\alpha r^2}{2}\right)^{n-2} \sum_{y=1}^{n-2} \frac{\left(\frac{n\alpha r^2(2\pi-\alpha)}{2\pi(2-\alpha r^2)}\right)^{y}}{y!} \\
= \; & X \frac{n\alpha^2 r^2}{4\pi} \left(1 - \frac{\alpha r^2}{2}\right)^{n-2} \left(e^Q - 1\right)
\end{aligned}$$

Substituting expressions for parts $1, 2$ and 3 into Equation 3.21 we then obtain:

$$\begin{aligned}
p^i_{b_2|f_2} \; = \; & 1 - X(1 - \frac{\alpha r^2}{2})^{n-1} \left[e^Q - Q - 1\right] \\
& - X \left(\frac{\alpha r^2}{2}\right) \left(1 - \frac{\alpha r^2}{2}\right)^{n-2} \left[(n-1)\left(e^Q - Q - 1\right) - Q(e^Q - 1)\right] \quad (3.30) \\
& - X \frac{n\alpha^2 r^2}{4\pi} \left(1 - \frac{\alpha r^2}{2}\right)^{n-2} \left(e^Q - 1\right) \quad (3.31)
\end{aligned}$$

Observe again that $p^i_{b_2|f_2} = 1$ when $\alpha = 2\pi$, as expected. That is, for a bidirectional network, for any given node s_i, given that $\delta_i^+ \geq 2$ implies that $\delta_i^- \geq 2$ with probability one. The probability $p^i_{d_2}$ that s_i is not 2-isolated is then:

$$p^i_{d_2} = p^i_{f_2}.p^i_{b_2|f_2} \quad (3.32)$$

and the probability that no 2-isolated node occurs in the network assuming independence is then $p_{d_2} = (p^i_{d_2})^n$. Expressions for $p^i_{d_2}$ and p_{d_2} obtained by simple substi-

tutions, are omitted here as they appear repetitive. For $\alpha = 2\pi$ representing the omnidirectional case we have that:

$$p_{d_2} = \left[1 - e^{\frac{-n\alpha r^2}{2}} \left(1 + \frac{n\alpha r^2}{2}\right)\right]^n.$$

Example 2: (Simulation study of the 2*-isolation property for a directional wireless sensor network*: We consider a simulation setup similar to Example 1 with the aim of achieving an WOSN in which a.s., no 2-isolated node occurs. Table V presents the minimum r values corresponding to preselected α and n values for which $p_{d_2} \geq 0.99$. We observe that for $n = 5000$ and $\alpha = \pi/2$, $p_{d_2} \geq 0.99$ for $r \geq 0.064$ km. However, if the nodes are capable of r up to 0.14 km, then for the same α and p_{d_2} confidentiality we require only 1000 nodes. On the other hand, if our nodes are only capable of $\alpha = 2\pi/9$ and $r = 0.07$ km, then we need at least $10,000$ nodes to achieve the same p_{d_2} confidentiality. Our expression yields $r \geq 0.093$ km for the omnidirectional network scenario, with $n = 500$ as observed in [42]. Compared to the $K = 1$ case, larger values for the corresponding minimum r and α are required to achieve the same p_{d_2} confidentiality.

3. One-dimensional Case

In this section, motivated by applications in ad hoc deployments of one-dimensional (1-D) sensor networks [92] as well as for comparative purposes with similar work for omnidirectional networks, we study the node isolation property in the 1-D WOSN. For this case, we model probabilistic 1-D connectivity, incorporating the 2-D orientation property of nodes.

Consider the set $\{\mathcal{S}_n\}$ of n nodes independently and uniformly distributed on an interval $[0, x_{\max}]$ of the real line. Let $x_i \in [0, x_{\max}]$ denote node s_i's position on the

Table V. The minimum r value for corresponding network parameter (n, α) pair values that achieve $p_{d_2} \geq 0.99$ in $G_n(\mathcal{S}_n, \mathcal{E})$.

n	$\alpha = \frac{\pi}{9}$	$\alpha = \frac{2\pi}{9}$	$\alpha = \frac{\pi}{3}$	$\alpha = \frac{\pi}{2}$	$\alpha = \frac{3\pi}{4}$	$\alpha = \pi$	$\alpha = \frac{3\pi}{2}$	$\alpha = 2\pi$
100	0.829	0.585	0.477	0.388	0.317	0.274	0.224	0.194
500	0.395	0.279	0.228	0.186	0.152	0.132	0.108	0.093
1000	0.287	0.203	0.166	0.135	0.110	0.096	0.078	0.068
5000	0.136	0.096	0.079	0.064	0.053	0.046	0.037	0.032
10000	0.098	0.070	0.057	0.047	0.038	0.033	0.027	0.024
100000	0.012	0.008	0.007	0.006	0.005	0.004	0.004	0.003

interval $[0, x_{\max}]$. Each node $s_i \in \{\mathcal{S}_n\}$ for $(i = 1, 2, \cdots n)$ transmits data within an interval I_i of length r (communication range). For large n, it is reasonable to assume that the existence of a directed edge between any two nodes is independent of the existence of links between the nodes and its neighbors, and that, if one node is chosen, the other $n - 1$ nodes are still uniformly distributed on the line.

Let us denote the $p_\alpha = \alpha/2\pi$ as the probability that the edge $s_i \rightarrow s_j$ exists, so that with probability p_α, the element of the adjacency matrix $\mathcal{E}^{1D}_{ij} = 1$, if $d(x_i, x_j) \leq r$. That is, $s_i \rightarrow s_j$ with probability p_α if $d(x_i, x_j) \leq r$. We define the graph $G^{1D}_n(\mathcal{S}_n, \mathcal{E}^{1D})$ as the 1-D WOSN RSSG. Previous definitions for f_K-connectivity, f_K-isolation, b_K-connectivity and b_K-isolation for the planar 2-D WOSN graphs translate in 1-D.

We consider the parameter (r, α) assignment problem for the n-node 1-D WOSN with $K = 1$, and ask: What is the expression relating the parameters r, α and n with the probability ${}_1p_d$ that no isolated node occurs in $G^{1D}_n(\mathcal{S}_n, \mathcal{E}^{1D})$? Our goal is to evaluate the minimum r and α values, such that ${}_1p_d \geq 0.99$, similar to the study for the omnidirectional communication paradigm in section 4.2.1 of [42].

As a first step, consider for node s_i, the probability that any node falls within I_i is r/x_{max}, and the probability that s_i is f-connected (to at least one node in I_i) is then $\alpha r/2\pi x_{max}$. Let ${}_1\delta_i^+$ denote the random variable counting the number of nodes that s_i is f-connected to. Ignoring edge effects, the probability that (of the remaining $(n-1)$ nodes) s_i is f-connected to k nodes in I_i is:

$$\Pr[{}_1\delta_i^+ = k] = \binom{n-1}{k} \left(\frac{\alpha r}{2\pi x_{max}}\right)^k \left(1 - \frac{\alpha r}{2\pi x_{max}}\right)^{n-k-1} \tag{3.33}$$

Employing the Poisson approximation of the Binomial for n large, $r << x_{max}$ with the ratio n/x_{max} kept constant [93], the probability that there are k nodes in I_i is:

$$\Pr[{}_1\delta_i^+ = k] = \frac{\left(\frac{n\alpha r}{2\pi x_{max}}\right)^k}{k!} e^{\frac{-n\alpha r}{2\pi x_{max}}}, \tag{3.34}$$

and the probability that s_i is f-isolated (i.e., has no successors) is

$$\Pr[{}_1\delta_i^+ = 0] = e^{\frac{-n\alpha r}{2\pi x_{max}}},$$

so that the probability ${}_1p_f^i$ that s_i is f-connected is then:

$$\Pr[{}_1\delta_i^+ > 0] = 1 - e^{\frac{-n\alpha r}{2\pi x_{max}}} \tag{3.35}$$

By similar arguments given in Lemma B.2 for the 2-D case, we note that the probability ${}_1p_b^i$ that s_i is b-connected equals ${}_1p_f^i$. It is also easy to derive the probability ${}_1p_{b|f}^i$ that s_i is b-connected given it is f-connected as:

$${}_1p_{b|f}^i = 1 - e^{\frac{-n\alpha r}{2\pi}} \left(1 - \frac{\alpha}{2\pi}\right)^{n-2} - e^{-n\alpha r/\pi} \left(1 - \frac{\alpha}{2\pi}\right) \left[e^{\left(\frac{n\alpha r}{2\pi} - \frac{n\alpha^2 r}{4\pi^2}\right)} - 1\right] \tag{3.36}$$

Simple substitutions from Equations 3.35 and 3.36 yield the probability ${}_1p_d^i = {}_1p_f^i \cdot {}_1p_{b|f}^i$ that s_i is not isolated. Extending this result for the n-node 1-D WOSN, the probability ${}_1p_d = ({}_1p_d^i)^n$ that no isolated node occurs in $G_n^1(\mathcal{S}_n, \mathcal{E})$ is then given as:

Corollary B.5 There is no isolated node in the 1-D network $G_n^1(\mathcal{S}_n, \mathcal{E})$ with probability ${}_1p_d$ given as:

$${}_1p_d = \left[1 - e^{\frac{-n\alpha r}{2\pi}}\right]^n \left[1 - e^{\frac{-n\alpha r}{2\pi}} \left(1 - \frac{\alpha}{2\pi}\right)^{n-2} - e^{-n\alpha r/\pi} \left(\frac{\alpha}{2\pi}\right) \left(e^{\left(\frac{n\alpha r}{2\pi} - \frac{n\alpha^2 r}{4\pi^2}\right)} - 1\right)\right]^n \tag{3.37}$$

Proof of Corollary B.5 The proof follows from the above arguments and is similar to that of Theorem B.4. This is a generalized expression relating ${}_1p_d$ to n, r, α, with the case of $\alpha = 2\pi$ yielding the omnidirectional 1-D results obtained in [42].

C. Simulations and Discussion

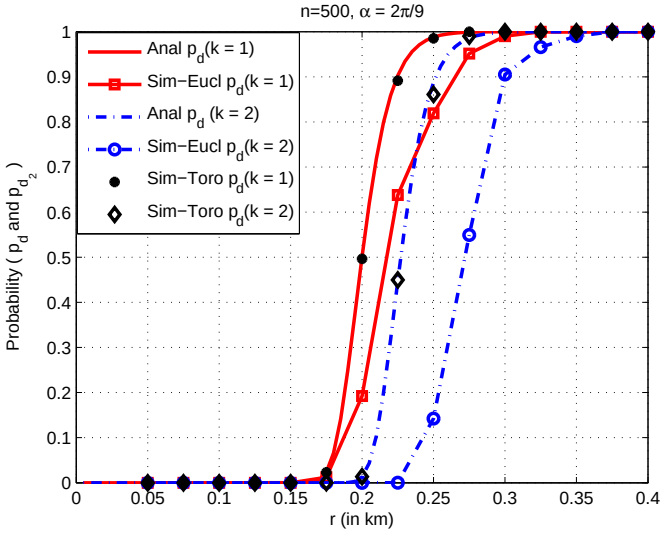
We employ simulations to empirically determine p_d (Sim), in order to compare it with analytical curves obtained for p_d, with K set to 1 and 2. The MATLAB software is used to simulate a WOSN with $n = 500$ nodes randomly positioned and oriented according to a uniform distribution in a planar square region of unit area 1 km^2. We employ six representative α values $(40^o, 90^o, 135^o, 180^o, 270^o, 360^o)$, and r ranging from 0 through 0.2 km (except for $\alpha = 40^o$ where we have used a wider range of r values from 0 through 0.5 km in order to observe salient changes in p_d). The adjacency matrix $\mathcal{E}$ of the resulting WOSN is obtained using the conventional Euclidean distance metric to determine the successors relationship of each node. Note that it is sufficient to compute successors of each node in populating $\mathcal{E}$, as predecessor relationships are derived by reversing successor links. The computations for determining the successors of a node is presented in the Appendix.

We study the node isolation property of $G_n(\mathcal{S}_n, \mathcal{E})$ by observing the neighborhood relationships reflected in $\mathcal{E}$. For each set of network parameters, our simulations are repeated 1000 times to yield an acceptable statistical confidence of the obtained results, and p_d is measured for each random network topology. We obtain an empir-

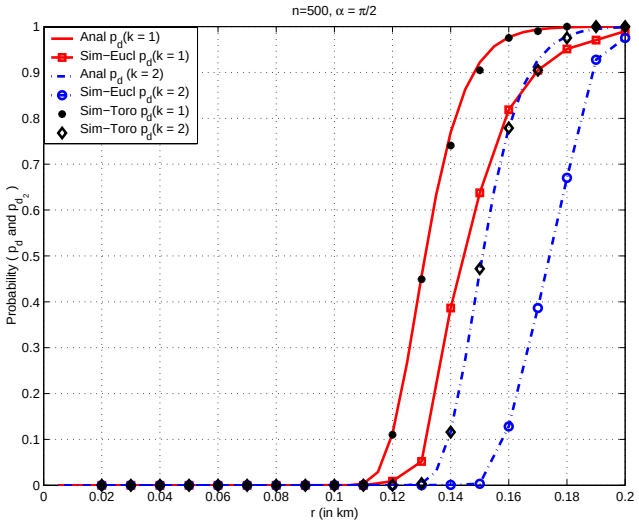
ical average of p_d by counting the number of directionally isolated nodes n_I in each simulation scenario, and compute p_d as $(1 - n_I/n)$, averaged over the 1000 random trials.

We conduct a second set of simulations in which $\mathcal{E}$ is computed using the *Toroidal* distance metric to obtain p_d, necessary to eliminate border effects. With the Toroidal metric, nodes at a border of the deployment region are modeled as being adjacent to nodes at the opposite border, creating a wrap around effect so that the flat simulation area becomes a torus. In our plots, we refer to p_d-Eucl and p_d-Toro as simulation plots obtained for p_d employing the Euclidean and Toroidal distance metrics respectively. We also conduct a third set of simulations to investigate the directional 2-isolation property (i.e., $K = 2$) of WOSNs, and derive empirical curves for p_{d_2}-Eucl and p_{d_2}-Toro to compare with analytically derived p_{d_2}.

Figure 13 depicts plots of p_d and p_{d_2}, illustrating the simulation results qualitatively following the analytical plots, with p_d-Toro almost exactly matching p_d-Anal as expected. We observe that p_d-Eucl does not exactly match up with p_d-Anal due to adverse border effects and a finite simulation region. We note that for smaller values of α the disparity between p_d-Anal and p_d-Eucl grows. This is obviously due to the fact that border effects in this case become more severe, since nodes at the boundary become isolated with a higher probability than for larger α values. Compensating for this boundary effect with p_d-Toro, we observe the desired result of an excellent match with p_d-Anal.

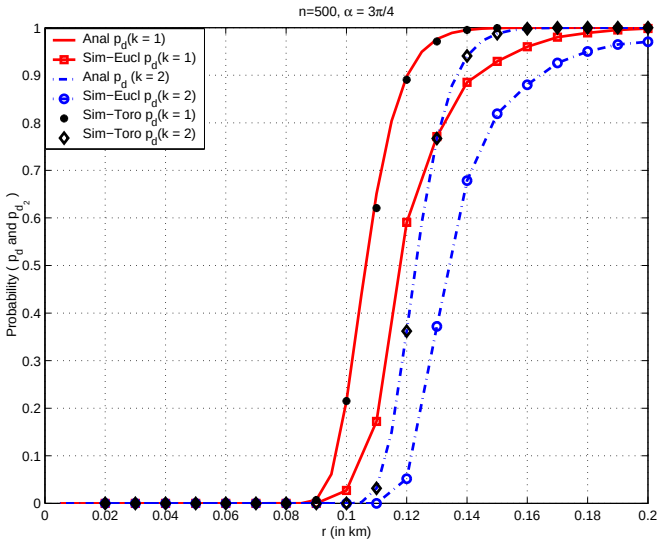


(g) $\alpha = 40$

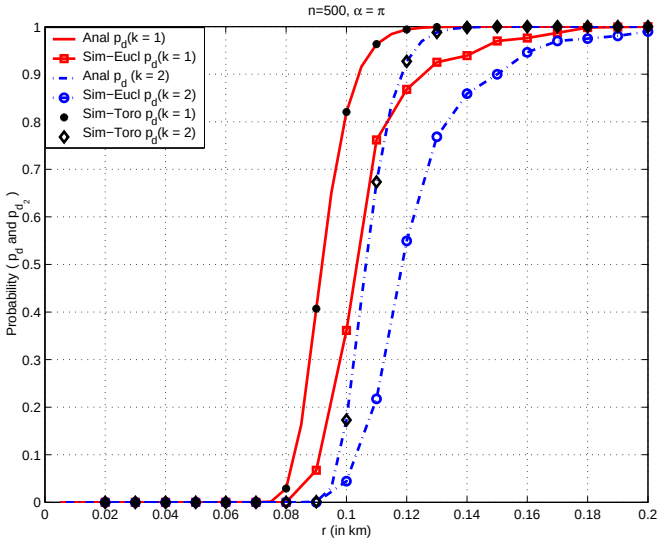


(h) $\alpha = 90$

Fig. 13. Analytical p_d (Anal) and simulation p_d for Euclidean (Sim-Eucl) and Toroidal (Sim-Toro) distance metrics for $K = 1, 2$, with varying r values, $n = 500$ and six preset α values.

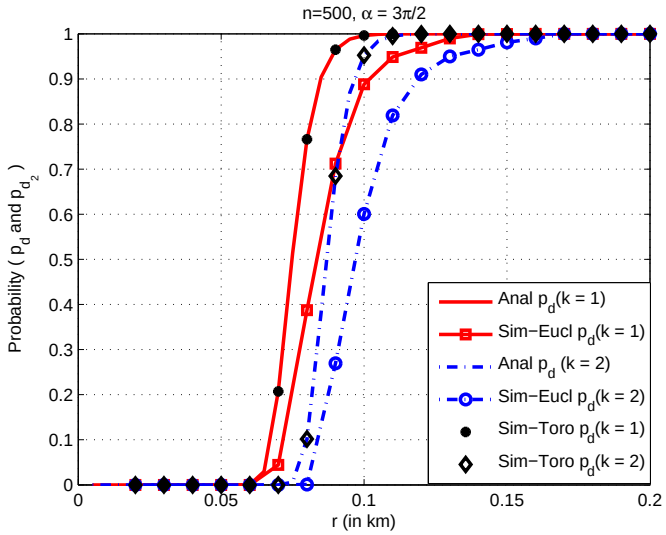


(c) $\alpha = 135$

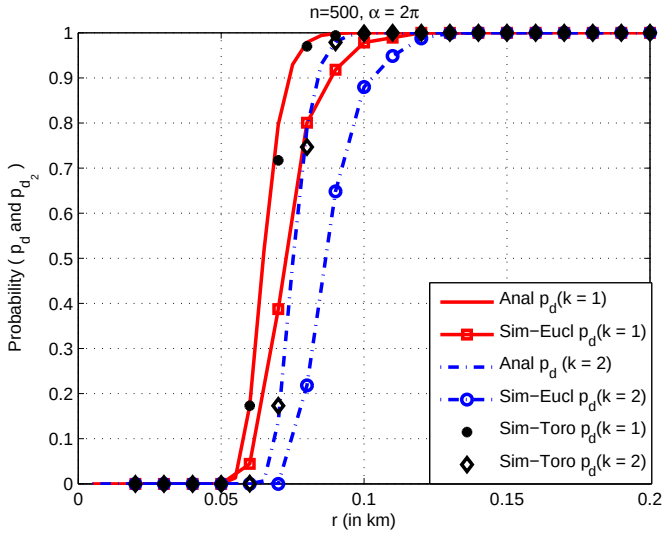


(d) $\alpha = 180$

Fig. 13 continued.

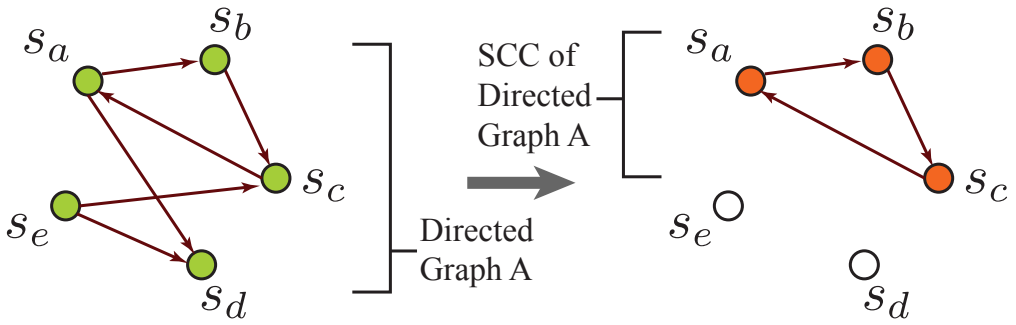


(e) $\alpha = 270$

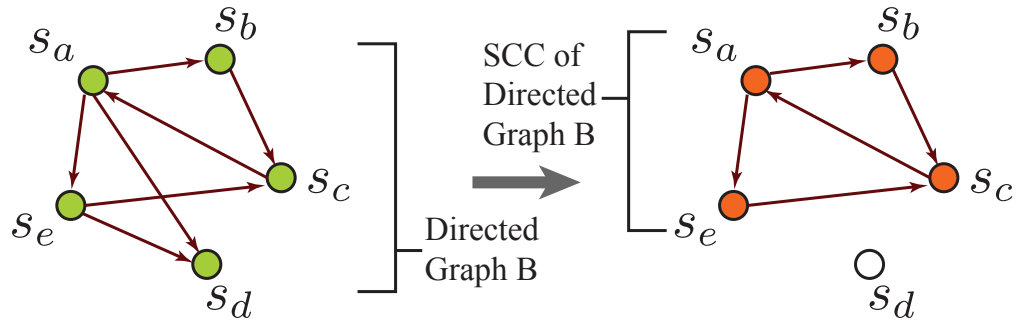


(f) $\alpha = 360$

Fig. 13 continued.



(a) For graph A, $p_c = 3/5$



(b) For graph B, $p_c = 4/5$

Fig. 14. Two examples of strong connected components (SCCs) of directed graphs.

We note that as n grows, (i.e., denser network), the analytical and simulation plots will agree more closely, due to the approximations made for $n \to \infty$ in the derivation of the analytical equations. We also observe that the p_{d_2} curves perform similarly so that as $\alpha \to 2\pi$, the simulation p_d more closely approach analytical p_d, more so for $K = 2$ than the $K = 1$ case. In both cases however, eliminating border effects results in the simulations with a high degree of match to analytical predictions.

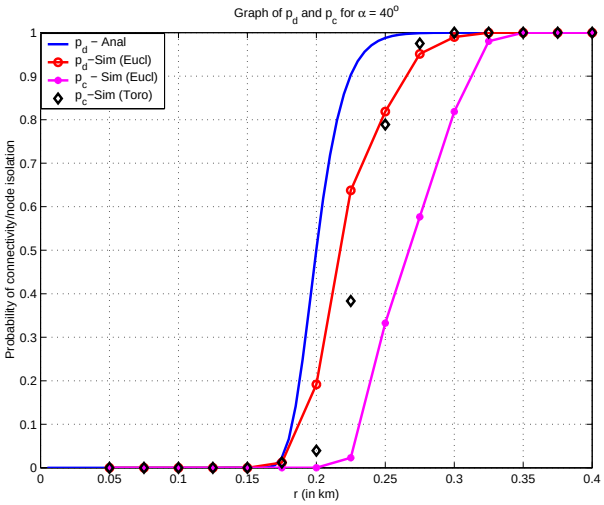
To empirically determine p_c, we obtain the number of nodes n_c in the largest *strongly connected component* (SCC) $G_n^c(\mathcal{S}_n, \mathcal{E}) \subset G_n(\mathcal{S}_n, \mathcal{E})$ as a fraction of n, where $G_n^c(\mathcal{S}_n, \mathcal{E})$ forms the largest partition of the network such that any pair of nodes in $G_n^c(\mathcal{S}_n, \mathcal{E})$ are pairwise connected. Figure 14 depicts examples of the SCC of two

5-node directed graphs A and B, with p_c equivalent to 3/5 and 4/5 respectively. We employ the well known Kosaraju's algorithm [94] which efficiently implements a depth-first-search (DFS) algorithm [95] to determine $G_n^c(\mathcal{S}_n, \mathcal{E})$ in our simulations. Kosaraju's algorithm uses the fact that the transpose graph[3] of a directed graph has exactly the same SCC as the original graph.

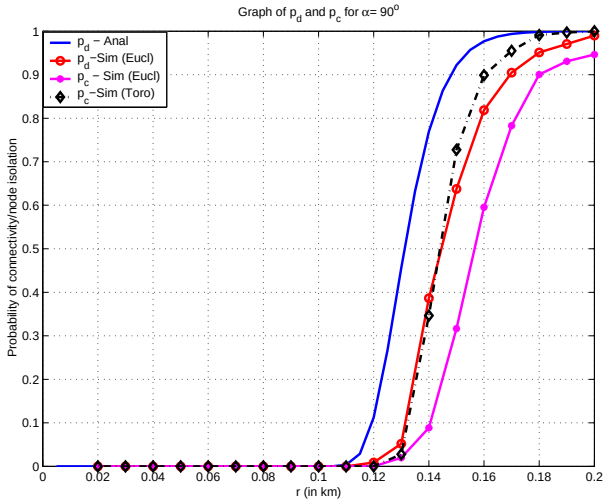
Similar to the MATLAB simulation scenario used to study node isolation in Section C, we generate an n-node random topology of $G_n(\mathcal{S}_n, \mathcal{E})$ over a square region of unit area 1 km^2. For $n = 500$, six representative α values and r varying, we repeat the simulations 1000 times to yield an acceptable confidence of obtain results. We measure empirical values for p_c as the ratio n_c/n for each trial, averaged over the 1000 random topologies, where n_c is the number of nodes in $G_n^c(\mathcal{S}_n, \mathcal{E})$ obtained using Kosaraju's algorithm. Because Kosaraju's algorithm is $O(|\mathcal{E}|n \log n)$, extensive simulation time is required to determine p_c especially for large r and α values for which $\mathcal{E}$ is dense, even with the use of Texas A & M's supercomputing facilities [96].

Figure 15 compares plots of empirically derived p_c (using both a Euclidean and a Toroidal distance metric), with p_d-Anal and p_d-Sim, for pre-selected α values. We observe that for large probability values, the property that $p_c = p_d$ holds, when Toroidal distance metric is used to compensate for boundary effects. This implies that for probabilities larger than about 0.95, parameter values obtained for the curve of p_d serve as a good approximation for attaining the same p_c confidence.

[3]The transpose graph is the same graph with the direction of every edge reversed.

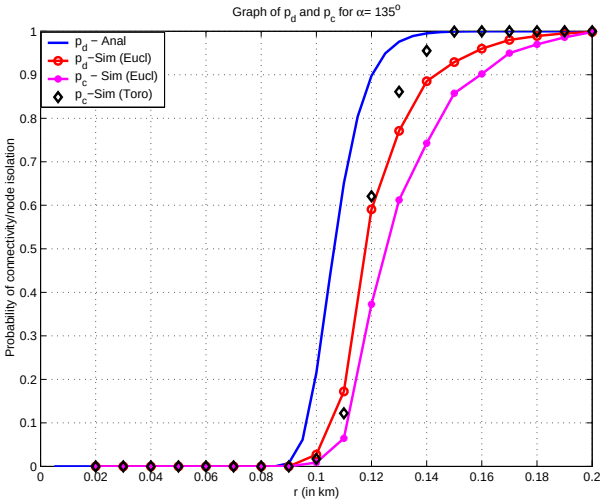


(a) $\alpha = 40^o$

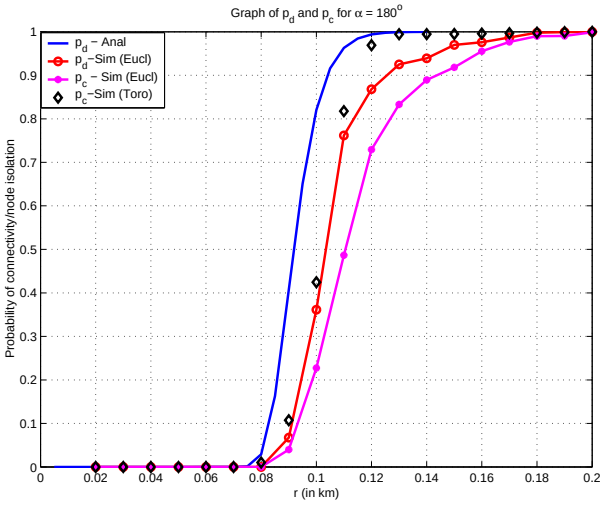


(b) $\alpha = 90^o$

Fig. 15. Comparing the probability p_c that the network is connected to the probability p_d that there is no isolated network node (simulated and analytical).

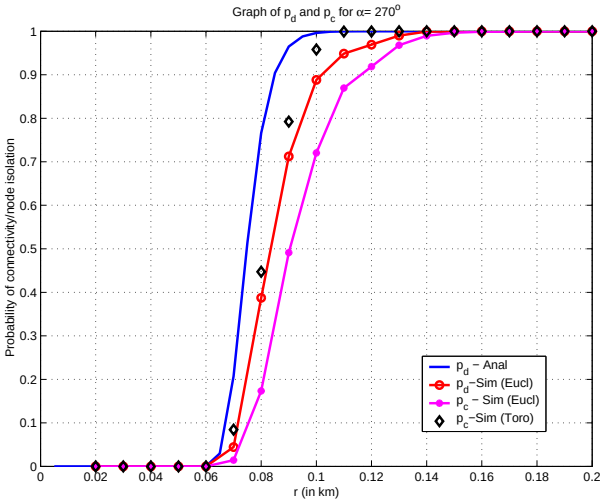


(c) $\alpha = 135^o$

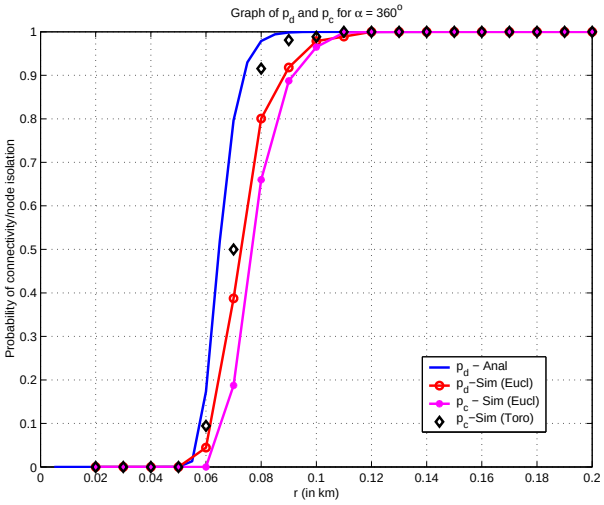


(d) $\alpha = 180^o$

Fig. 15 continued.



(e) $\alpha = 270^o$



(f) $\alpha = 360^o$

Fig. 15 continued.

In a real world application, this would be especially true with very dense networks and large deployment regions that minimize the boundary effects. It is noteworthy that our results are consistent with the conclusions of [42]. That is, for directional networks, it is also true that p_d is a tight upper bound for p_c for $n \to \infty$ and probabilities close to one. However, we observe that this result is even more so, as α increases. That is, as $\alpha \to 2\pi$, p_c does a much better job at approaching p_d, especially for large probability values close to 1.

Another interesting phenomenon observed for p_d and p_c is the 'phase transition' property typically observed for random graphs [29], in which p_c transitions rapidly from 0 (i.e., network is disconnected with probability 1) to 1 (i.e., network is connected with probability 1). This property gets stronger as $\alpha \to 2\pi$. For example, for $\alpha = 40^o, 180^o$ and 360^o, while $p_c = 0$ for $r = 0.20, 0.08$ and 0.06 km respectively, $p_c = 1$ for $r = 0.35, 0.18$ and 0.12 km respectively. That is, for $\alpha = 40^o, 180^o$ and 360^o, the 'phase transition' spans a distance of $0.15, 0.10$ and 0.06 km respectively. Our results lead us to state the following:

Proposition C.1 For n WOSN nodes randomly distributed and oriented on the planar unit area square according to a uniform distribution, let r_c and r_d denote, the minimum r at which the network graph $G_n(\mathcal{S}_n, \mathcal{E})$ is connected and attains no isolated node, respectively. Then*:*

$$Pr[r_c = r_d] \to 1 \quad as \quad n \to \infty \quad and \quad \alpha \to 2\pi$$

D. Impact of Hierarchy and Clustering on Connectivity

The traffic pattern in the naturally hierarchical WOSN consisting mainly of base station-to-nodes or nodes-to-base station traffic [97]. Consider a cluster-based WOSN with a fraction of the nodes acting as cluster heads (CHs) that send and receive data

directly to and from the base station, respectively, on behalf of other nodes. In terms of hierarchy, the base station forms the highest layer, the CHs constitute the middle layer, while the other remaining nodes form the lowest layer of the network. A higher class of CH nodes, perhaps equipped with more energy and communication resources may also be envisioned in a heterogenous sensor network architecture. Clustered sensor networks have been vastly studied in the literature with regard to improving energy [53, 97], power and topology control, scalability, load balancing, data aggregation, fault tolerance and routing efficiency [98, 99].

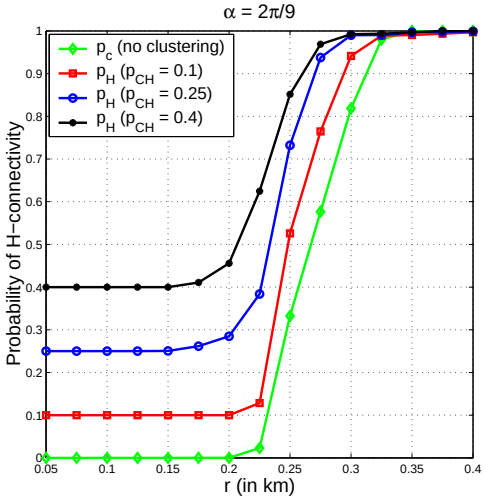
Let us define the *hierarchical connectivity* (H-connectivity) property of the WOSN as the connectivity of the **supergraph** $G_n^s(\mathcal{S}_n, \mathcal{E}^s) \supseteq G_n(\mathcal{S}_n, \mathcal{E})$ formed by adding edges [19] between all pairs of nodes in $\mathcal{CH}$. In this model, the CHs act as *articulation nodes* such that with high probability $\mathcal{CH}$ forms a *cut set* for the SCC of $G_n^s(\mathcal{S}_n, \mathcal{E}^s)$. That is, the removal of the set $\mathcal{CH}$ results in the likely disconnection of $G_n^s(\mathcal{S}_n, \mathcal{E}^s)$. H-connectivity implies that all nodes in the network can communicate (send and receive) with the base station, conforming to the desired traffic pattern of sensor networks.

Within this context, the question we raise is, what is the impact of p_{CH} on the H-connectivity property of $G_n(\mathcal{S}_n, \mathcal{E})$? More specifically, how can we choose p_{CH} such that with a given probability p_H, the network is H-connected. The answer to this question is crucial in determining the fraction of 'special' nodes that must be manufactured and deployed as CHs during design phase, to achieve a desired p_H. In fact, p_{CH} is an additional tunable network parameter to enable a more flexible network design.

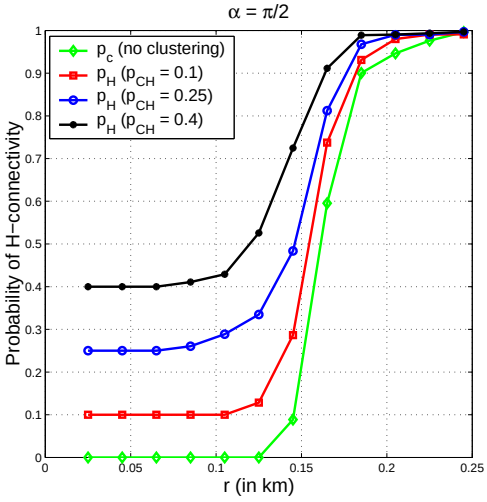
We empirically evaluate the effect of clustering on H-connectivity. Similar to previous simulations, 1000 random topologies of a 500-node network are generated and evaluated to yield acceptable confidence on obtained empirical results. In this

scenario, nodes are designated as CHs with probability p_{CH} set to three representative values of $10\%, 25\%$, and 40%, and the adjacency matrix of $G_n^s(\mathcal{S}_n, \mathcal{E}^s)$ is obtained by updating $\mathcal{E}$ to reflect the additional links between all CHs. We compute p_H as the ratio of the number of nodes in the SCC of $G_n^s(\mathcal{S}_n, \mathcal{E}^s)$ to n, and obtain empirical values for p_H as the average across the 1000 trials.

Figure 16 depicts plots of p_H compared to p_c for the different P_{CH} values. We observe that for all α values clustering remarkably improves network connectivity. For example, for $\alpha = 40^o$, we observe that $p_c = 0.33$ for $r = 0.25$ while $p_H = 0.52, 0.72$ and 0.85 respectively with corresponding p_{CH} values of $10\%, 25\%$, and 40%. Consider for example, a WOSN deployed within a unit area (1km $\times$1km) planar region. If the network owner can only afford to deploy a limited number of nodes, say 500 nodes, each node possessing a communication radius r and angle α of 0.15m and 90^o respectively, he is only guaranteed a connectivity of about 20% of nodes. If however, 25% of nodes are equipped to function as cluster heads, the connectivity of the network improves to 60%. Further if 40% of nodes are designated as cluster heads, the network connectedness of almost 80% can be guaranteed. (See Figure 16(b)). Practical cost considerations determine the tradeoff between enhancing a node's capability to become a cluster head versus deploying several more of the ordinary nodes.

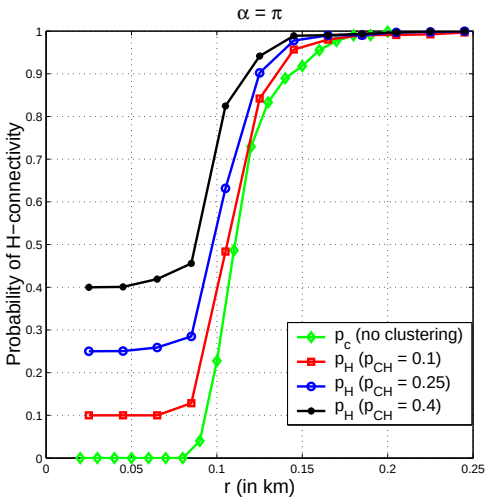


(a) $\alpha = 40^o$

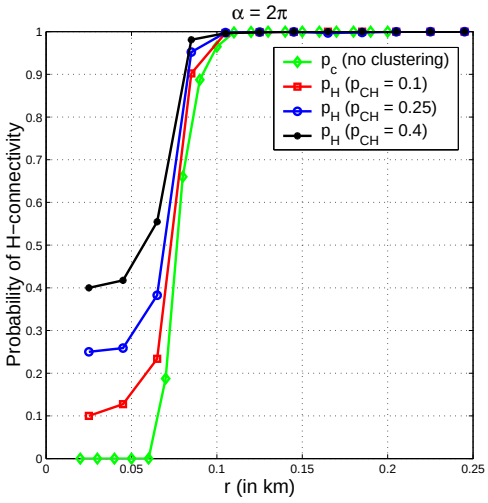


(b) $\alpha = 90^o$

Fig. 16. Plots of p_{hc} compared to p_c for varying p_{CH}.



(c) $\alpha = 180^o$



(d) $\alpha = 360^o$

Fig. 16 continued.

E. Connectivity Analysis in a Fading Channel Model

In FSO communication, absorption or obscuration of the beam by the atmosphere, adverse weather conditions such as fog, snow, heavy rain, or optical turbulence due to temperature and pressure variations, can be important to channel performance.

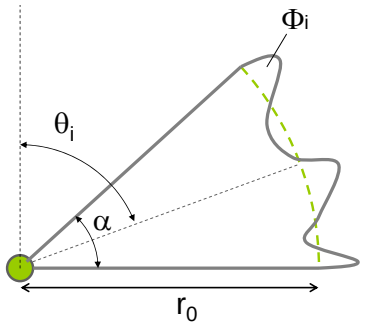


Fig. 17. An example of the region of transmission of a WOSN node in a fading channel.

Due to the impact of ambient light on FSO, and its susceptibility to atmospheric turbulence (especially fog) and obscuration, it is imperative that we model *fading* channel links as a result of these factors that cause degradation to the WOSN's connectivity [26]. For example, due to fading effects that result in random values of r_0 at various points (and therefore random $A(\Phi_i)$ value), the boundary of the region of transmission (RoT) for the WOSN node is an irregular shape as illustrated in Figure 17 instead of a simple sector as with the no fading case.

It is well known [100] that in a WOSN fading environment, the compound signal attenuation H is comprised of two main components: a *deterministic path loss component* h_l due to atmospheric attenuation from atmospheric absorption or obscuration of the beam, and by adverse weather conditions such as fog, snow, heavy rain; and a *stochastic path loss component* h_a due to atmospheric optical turbulence from temperature and pressure variations. The stochastic path loss for the FSO signal has been

characterized by a *log-normal* probability density function (pdf) for *weak turbulence* and a *K-distribution* for *strong turbulence*[101, 102]. The effects of a third geometric spread and pointing errors component is negligible for broad beam FSO, and will therefore be ignored in this dissertation. We assume a non-ergodic channel with stationary link characteristics implying that the time scales of the fading processes are far larger than bit interval, so that time varying behaviors may be ignored.

This model represents a communication channel in which r_0 and hence *link probability* $\Pr[s_i \rightarrow s_j]$ is modeled as a random variable (r.v.) instead of the simple monotone step function $\Pr[s_i \rightarrow s_j] = \mathbf{1}_{\Delta_{ij} \leq r_0,\ |\Theta_i - \Psi_{ij}^T| \leq \frac{\alpha}{2}}$, employed where there is no consideration for fading [9, 23], where $\Delta_{ij} = \sqrt{d(x_i, x_j)^2 + d(y_i, y_j)^2}$ is the Euclidean distance between s_i and s_j, and $\Psi_{ij}^T = \min\left[|\Theta_i - \Psi_{ij}|, |\Theta_i + 2\pi - \Psi_{ij}|, |\Theta_i - 2\pi - \Psi_{ij}|\right]$ represents the angular difference between the direction of s_i and the position of s_j, with $\Psi_{ij} = \arccos d(y_j, y_i)/\Delta_{ij}$ as depicted in Figure 18.

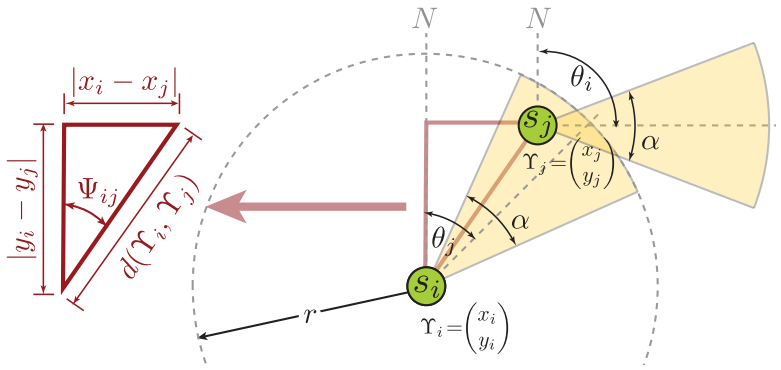


Fig. 18. Geometric illustration for $s_i \rightarrow s_j$ if $d(s_i, s_j) \leq r$ and $|\Theta_i - \Psi_{ij}^T| \leq \frac{\alpha}{2}$ based on a simple monotone function.

In the WOSN fading channel with attenuation H_{ij} on the link $s_i \rightarrow s_j$, given r_o, Δ_{ij} and $\Psi_{ij} \leq \alpha/2$, we determine that $s_i \rightarrow s_j$ exists if H_{ij} is less than a given threshold attenuation H_t which is a function of r_0 - the maximum distance granting a link in the absence of fading. Recall that H_{ij} is formulated as $H_{ij} = P_t(s_i)/P_r(s_j)$,

where $P_t(s_i)$ and $P_r(s_j)$ are transmit and receive power at s_i and s_j respectively. The question we address in this section is: given a fading environment, what is the probability p_c that the WOSN is connected in terms of the physical layer variables of n, r and α? To answer this question, we determine the closed form expression for an analytical expression for p_d within a fading channel, and the impact of fading on p_c.

1. Fading Channel Statistical Model

The combined effects of direct absorption and scattering of the FSO signal by air molecules, solid or liquid particles (e.g., fog) suspended in the air is described by a single path-dependent attenuation coefficient σ, so that h_l is given by the Beer-Lambert law:

$$h_l(s_i, s_j) = \exp\left(-\sigma\delta_{ij}\right)$$

where σ depends on the size and distribution of particles and the wavelength λ of the laser. For the stochastic component, h_a has been shown to have a log-normal pdf for weak turbulence (Rytov variance $\sigma_R^2 < 0.3$) given as:

$$f_{h_a}(h_a) = \frac{1}{2h_a\sigma_X\sqrt{2\pi}} \exp\left(\frac{(\ln h_a + 2\sigma_X^2)^2}{8\sigma_X^2}\right)$$

and a K-distribution for strong turbulence given as:

$$f_{h_a}(h_a) = \frac{2\beta^{\frac{\beta+1}{2}}}{\Gamma(\beta)}(h_a)^{\frac{\beta-1}{2}} K_{\beta-1}\left(2\sqrt{\beta h_a}\right) \quad \text{for} \quad h_a > 0$$

where $\sigma_X^2 \approx \sigma_R^2/4$ is the variance of the log-amplitude of the optical intensity, (assuming atmospheric channels near the ground < 18.5m), $K_\beta(.)$ is the modified Bessel function of the second kind of order β, and β is a channel parameter related to the effective number of discrete scatters [26]. Table VI summarizes sample parameter values associated with two weather conditions for weak and strong turbulence. We

Table VI. Adverse Weather Parameters Affecting The FSO signal.

Condition	Visibility	σ_R^2	σ
Clear & strong turbulence	10	1	0.44
Light fog & weak turbulence	0.5	0.1	20

implemented $K_\beta(\xi)$ in MATLAB utilizing the $\mathsf{besselk}(\beta, \xi)$ function, and point out the strong inverse correlation between turbulence strength σ_R^2 and attenuation σ.

The compound attenuation acting on link $s_i \rightarrow s_j$ is given as $H_{ij} = h_l \times h_a$, and we obtain:

$$\begin{aligned}
\Pr[H_{ij} \leq H_t | \Delta_{ij}, \Psi_{ij} < \frac{\alpha}{2}] &= \int_{-\infty}^{H_t/h_l} f_{h_a}(h_a) dh_a \\
&= \int_{-\infty}^{H_t \frac{\exp(\sigma \Delta_{ij})}{r_o}} \frac{1}{2h_a \sigma_X \sqrt{2\pi}} \exp\left(\frac{(\ln h_a + 2\sigma_X^2)^2}{8\sigma_X^2}\right) dh_a \\
&= \frac{1}{2}\left[1 - \text{erfc}\left(\frac{\ln[H_t \frac{\exp(\sigma \Delta_{ij})}{r_o}] + 2\sigma_X^2}{2\sqrt{2}\sigma_X}\right)\right] \qquad (3.38)
\end{aligned}$$

for *weak turbulence*, and

$$= \frac{2(\beta)^{\frac{\beta+1}{2}}}{\Gamma(\beta)} \int_{-\infty}^{H_t \exp(\frac{\sigma \Delta_{ij}}{r_0})} (h_a)^{\frac{\beta-1}{2}} K_{\beta-1}\left(2\sqrt{\beta h_a}\right) dh_a \qquad (3.39)$$

for *strong turbulence*, where we compute the integral of Equation 3.39 using efficient numerical techniques and the quadl function in MATLAB. The threshold attenuation value is obtained as $H_t = \exp(-\sigma r_0)$ [42]. Figure 19 depicts the link probability over Δ_{ij}/r_0 for the two weather conditions represented in Table VI. For the case of no fading ($\sigma = 0$), we observe the sharp transition at the critical r_0 value that yields a threshold. For example, in clear weather with strong turbulence, there is still a link probability of almost 10% at a distance of $1.8r_0$ while for light fog and

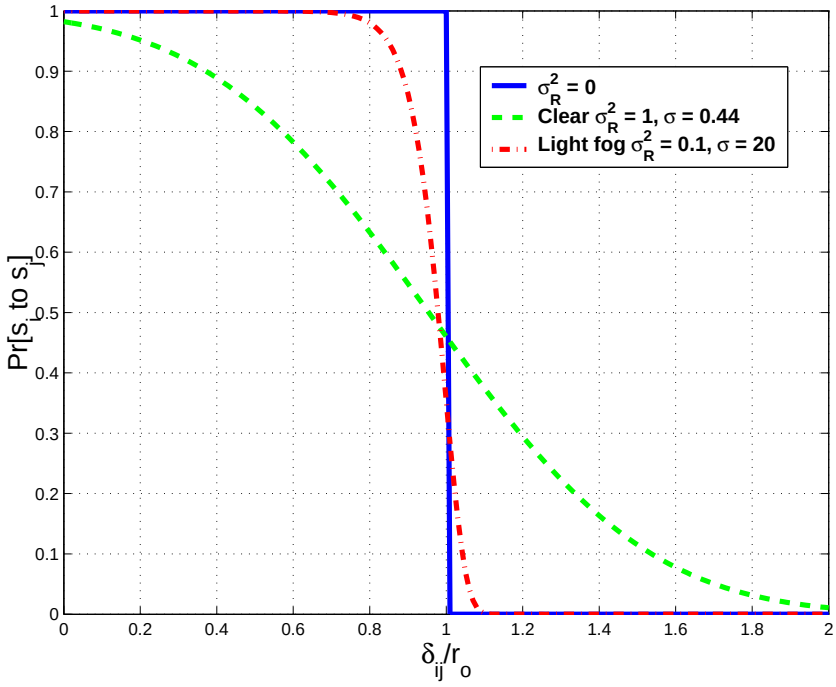


Fig. 19. Link probability for the two weather conditions given in Table VI.

weak turbulence, the probability of a link degrades to 0% at a distance of $1.1r_0$. It is obvious that the FSO signal is degraded by fog to a higher degree than by strong optical turbulence.

We now determine an analytical expression p_d for the WOSN in a fading channel, and compare it to empirically determined p_c to determine the tightness of the bound and the effect of fading for various α values.

Consider the probability $p^i_{f\cap b}$ that a randomly selected node s_i is isolated, which is equivalent to the probability that s_i is both *f-isolated* (i.e., $\mathcal{S}_i = \emptyset$) and *b-isolated* (i.e., $\mathcal{P}_i = \emptyset$), so that we can write: $p^i_{f\cap b} = p^i_f \times p^i_{b|f}$, where p^i_f is the probability that a node is f-isolated and $p^i_{b|f}$ is the probability that a node is b-isolated conditioned on the fact that it is f-isolated. Our next step is to determine $p^i_{f\cap b}$ by evaluating p^i_f and $p^i_{b|f}$, where $p^i_f = \Pr[\delta^+_i = 0]$ is obtained by considering as previously stated that

the r.v. δ_i^+ follows a Poisson$\sim n\mathrm{E}(A_{\Phi_i})$ pdf, where E(.) is the expectation function, so that,

$$\Pr[\delta_i^+ = z] = \frac{e^{-n\mathrm{E}(A_{\Phi_i})}\left(n\mathrm{E}(A_{\Phi_i})\right)^z}{z!} \tag{3.40}$$

upon which we obtain $p_f^i = e^{-n\mathrm{E}(A_{\Phi_i})}$. We next derive:

$$\begin{aligned} p_{b|f}^i &= \Pr[\delta_i^- = 0 | \delta_i^+ = 0] \\ &= \sum_{k=1}^{n-1} \Pr[\delta_i^- = 0 | \delta_i^+ = 0, k = K].\Pr[k = K] \end{aligned} \tag{3.41}$$

where k denotes the r.v. counting the number of nodes within $\mathbb{B}(\Upsilon_i, r_0) \setminus \Phi_i$. Observe that $k \sim$ Poisson $\left(n(\pi r_0^2 - \mathrm{E}(A_{\Phi_i}))\right)$ and $\Pr[\delta_i^- = 0 | \delta_i^+ = 0, k = K] = (1 - \mathrm{E}(A_{\Phi_i}))^K$, so that:

$$\begin{aligned} p_{b|f}^i &= e^{-nr^2(\pi - \frac{\alpha}{2})} \sum_{k=0}^{n-1} \frac{\left[(nr^2\pi - n\mathrm{E}(A_{\Phi_i}))(1 - \mathrm{E}(A_{\Phi_i}))\right]^k}{k!} \\ &= e^{-n(\pi r^2 - \mathrm{E}(A_{\Phi_i}))}.e^{n(r^2\pi - \mathrm{E}(A_{\Phi_i}))(1 - \mathrm{E}(A_{\Phi_i}))} \\ &= e^{-n(\pi r^2 - \mathrm{E}(A_{\Phi_i})).\mathrm{E}(A_{\Phi_i}))} \end{aligned} \tag{3.42}$$

By simple substitution, we have that:

$$\begin{aligned} p_{f\cap b}^i &= e^{-n\mathrm{E}(A_{\Phi_i})}.e^{-n(\pi r^2 - \mathrm{E}(A_{\Phi_i})).\mathrm{E}(A_{\Phi_i}))} \\ &= e^{-n\mathbb{E}(A_\Phi)\left[1 \,+\, \pi r_o^2 - \mathbb{E}(A_\Phi)\right]} \end{aligned} \tag{3.43}$$

Given our assumption that the isolation of individual nodes are independent events for large n, the conditional probability p_d that there is no isolated node in $G_n(r, \alpha)$ given n is:

$$p_d = (1 - p_{f\cap b}^i)^n \tag{3.44}$$

$$= \left(1 - e^{-n\mathbb{E}(A_\Phi)\left[1 \,+\, \pi r_o^2 - \mathbb{E}(A_\Phi)\right]}\right)^n \tag{3.45}$$

We need to evaluate $n\mathbb{E}(A_\Phi)$ which is the expected number of nodes within a given node's RoT, where $\mathbb{E}(A_\Phi)$ is computed by integrating $\Pr[H \leq H_t|\Delta, \phi]$ over the entire system plane:

$$\begin{aligned} \mathbb{E}(A_\Phi) &= \int_0^\alpha \int_0^\infty \Pr[H \leq H_t|\Delta, \phi] \ \Delta \ d\phi \ d\Delta \\ &= \alpha \int_0^\infty \Pr[H \leq H_t|\Delta] \ \Delta \ d\Delta \end{aligned} \tag{3.46}$$

Equation 3.46 is computed by plugging in equations 3.38 and 3.39 and employing numerical means to solve $\mathbb{E}(A_\Phi)$ for the weak and strong turbulence cases, respectively.

2. Numerical Results and Observations

In order to validate our analytical results, we perform a number of computer-based simulations in MATLAB for p_d and p_c under the two (weak and strong turbulence) fading channel conditions using parameter values reflected in Table VI, as well as the no fading condition. We compare our simulation results with curves obtained with our analytical derivations of Equation 3.44, for similar conditions. With α set to three representative values of $2\pi/9, \pi/2$, and π for a chosen $H_t = 40$dB (implying a given r_0), we randomly place a given number of nodes n in a unit area region according to a Uniform distribution. For each node pair (s_i, s_j), given the absolute angular difference from s_i to s_j is less than $\alpha/2$, we compute link probability from Equation 3.38 and 3.39 for the fading channel, and determine that with this probability, link $s_i \rightarrow s_j$ exists. Once all nodes have established links according to the channel and transmission parameters, we check the topology for any isolated node and test the connectivity of the network. We employ Monte Carlo methods, repeating our experiments 500 times, and estimate p_d and p_c as the percentage of topologies with no isolated node and the percentage of connected topologies, respectively. We repeat the

process with varying n values.

Our results, presented in Figures 20 (a) - (c), clearly indicate that network connectivity degradation due to fading worsens as α increases on one hand, while it improves with no fading. This trade off implies that careful design consideration must be given in the choice of the optimal α that ensure connected minimum density network in a fading channel. For example with $\alpha = 2\pi/9, \pi/2, \pi$, without fading, $n = 170, 80, 50$ yields analytical $p_d = .99$, whereas $n = 300, 230, 240$ is required for the same p_d under strong turbulence, respectively. Additionally, we observe that the simulation curves of p_d and p_c qualitatively follow their corresponding analytical curves, but lag them quantitatively, due to boundary effects [42] which are not compensated for. The negligible difference between p_d and p_c for probabilities close to one suggests it suffices to compute the minimum n that achieves $p_d \geq .99$, as a tight lower bound for the n required to achieve a corresponding p_c.

3. Summary of Insights

We now summarize the insights gained from our analysis and simulation results as compared to the $\alpha = 2\pi$ case as follows:

1. A linear change in r produces a much more significant impact on p_d than a corresponding linear change in α.

2. As in the $\alpha = 2\pi$ case, there is a critical value of r above which the network will almost surely have no isolated nodes. This natural trend is preserved even for directional networks that do not follow the RGG model. However, we observe that the "phase transition" nature of the plots are not as strong for smaller α values.

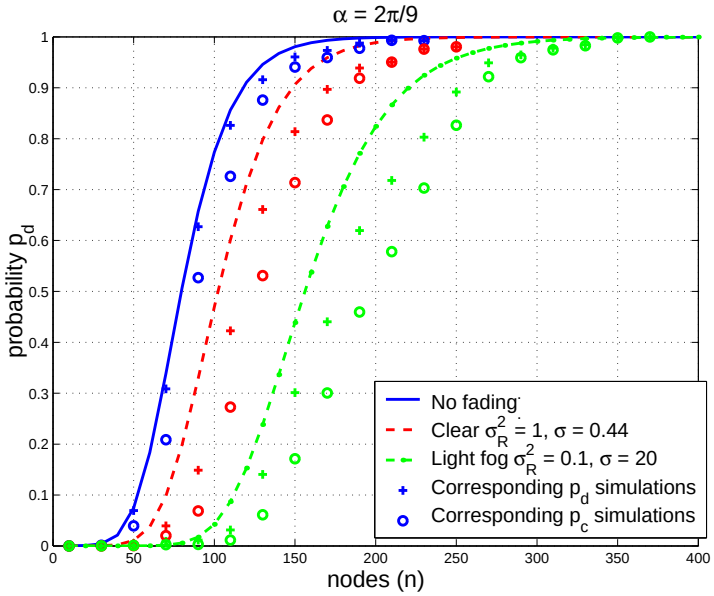
3. Node isolation has been one of the major hurdles for broadband directional

networks and the conservative results derived in this paper demonstrate the potential for connectivity in such networks providing further support for emerging hybrid RF/FSO systems.

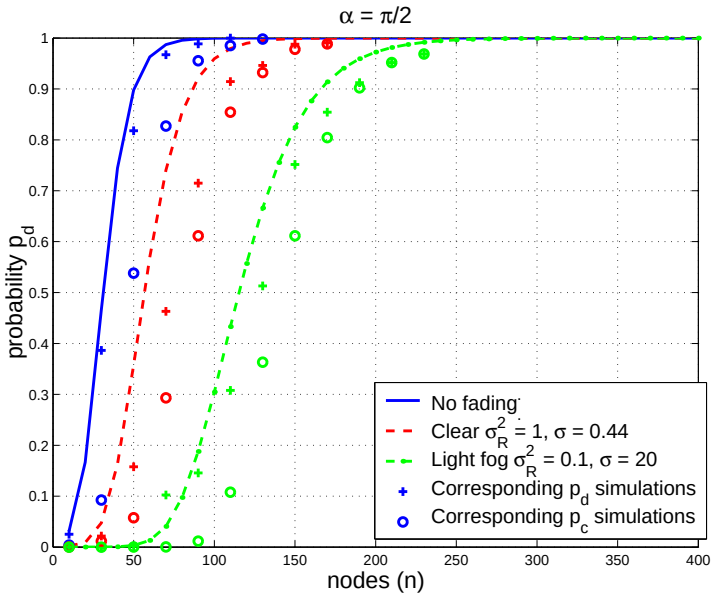
4. For K-connectivity of a network, as K grows, it is projected that significantly larger values of r will be required to maintain connectivity for lower values of α. For sensor networks in which it is possible that a fraction of nodes may die or be corrupted, such performance motivates even more the need for a hybrid or clustered heterogenous paradigm.

5. The importance of considering fading in a given deployment environment for the WOSNs cannot be over emphasized, as it can greatly impact on the network connectivity, and hence the choice of physical layer parameter values. In particular, when fading effects are considered in WOSNs, n rather than r turns out to be the most sensitive network parameter for connectivity in the network.

The next chapter is concerned with the introduction of the secure integrated routing and localization scheme for the WOSN, assuming the network satisfies connectivity requirements developed in this chapter.

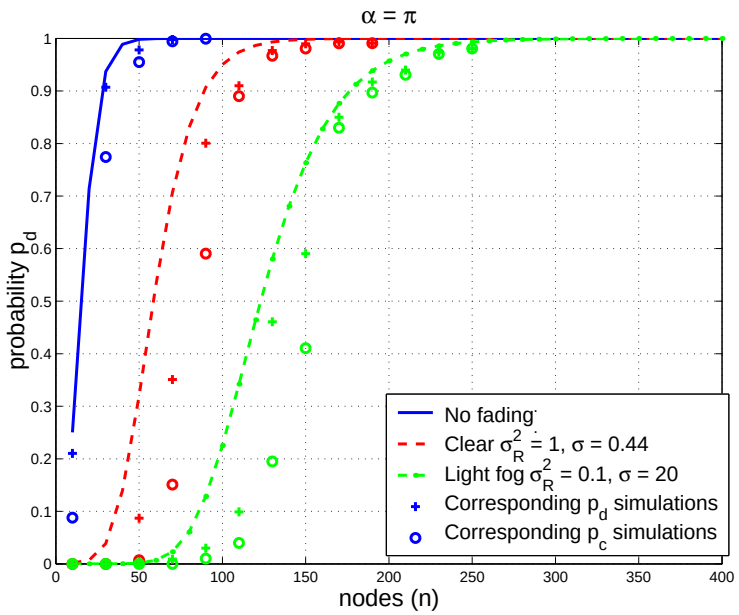


(a) $\alpha = 2\pi/9$



(b) $\alpha = \pi/2$

Fig. 20. Comparing simulation results for p_d and p_c with analytical values for various α and fading conditions, with $H_t = 40$dB.



(a) $\alpha = \pi$

Fig. 20 continued.

CHAPTER IV

SIRLoS: SECURE INTEGRATED ROUTING AND LOCALIZATION SCHEME

A. Introduction

It is vital to consider security objectives at the onset of the design phase for network layer protocols such as routing, clustering and localization, as previously stated in Chapter II. In the WOSN, the non-reversibility of paths further complicates route setup. Due to the lack of bi-directionality in most of the WOSNs' links, a node cannot immediately discover its complete neighborhood. This is because knowledge of a node's *successors* cannot be gained simply by listening to the channel, and the exchange of link layer acknowledgements proves non-trivial, creating huge overhead. As a result, common neighborhood discovery mechanisms based on reverse path forwarding, such as topology broadcast [53], and range-free localization schemes which work well for omnidirectional networks, cannot be exploited for WOSNs. Similarly, protocols that have simply been optimized to accommodate a limited number of directional network links are hugely inefficient and wasteful in WOSNs.

In the WOSN, opportunities exist for an attacker to exploit loopholes in security assumptions and attack counter-measures that have been proffered and designed specifically for omnidirectional networks. Therefore, it is imperative that for WOSNs, novel, bottom up security-aware routing and localization paradigms be designed, and corresponding attacks and countermeasures which may be relevant in traditional omnidirectional networks be re-evaluated [27].

In this chapter, we introduce SIRLoS, a novel lightweight *secure integrated routing and localization scheme* for WOSNs. SIRLoS does not employ range estimation methods, time synchronization or expensive localization hardware. Instead SIRLoS ex-

ploits a hierarchical cluster-based organization of the network to offer a lightweight security services based on symmetric cryptography; a novel circuit-based neighborhood discovery and routing approach; and a simple location estimation algorithm based on topology control.

The security objectives of the SIRLoS protocol includes providing per hop and broadcast authentication, assuring nodes and the base station of the origin of the routing beacon. SIRLoS also guarantees that routing and location information are protected against outsider eavesdropping and unauthorized manipulation, thus providing data confidentiality, integrity and freshness for beacons. We employ one-way key chains, individual and network wide symmetric keys, individual node passwords and cluster head specific nonce values[1] to defend against unauthorized participation, spoofing, altering or replaying route signals. For security against insider attacks on routing in WOSNs, we submit to the prudence and practicality of leveraging the resources of the trusted and powerful base station. The use of a base station anchored circuit-based paradigm provides a lower overhead alternative for neighborhood discover compared to prior routing protocols [9] which have been offered for the WOSN.

In this chapter, we describe the various aspects of SIRLoS, demonstrate the security advantages due to link directionality, and provide performance, security and attack evaluations and countermeasures to demonstrate the potential benefits of SIRLoS compared to other routing schemes for WOSN applications. Through this investigation, we demonstrate some fundamental insights in this emerging field, which include:

1. security and neighborhood discovery in WOSNs is more challenging compared to the traditional omnidirectional networks, due to an added orientation constraint

[1]A nonce is a randomly generated bitstream used to achieve data freshness.

which necessitates a mechanism for efficient discovery of successors;

2. by employing routing beacons which originate at the trusted and powerful base station, propagate through the network and terminate at the base station, we show that directionality provides various advantages that may be leveraged for enhanced security in WOSNs;

3. an emerging research area which involves securing the network layer of WOSNs is a rich field of study which encompasses problems such as connectivity analysis, secure localization, intrusion detections, topology control and secure data aggregation, and novel attacks relevant to this architecture. This opens up several directions for novel research in WOSNs.

B. SIRLoS: Secure Integrated Routing and Localization Scheme

SIRLoS is a two-phase, restricted flooding mechanism that entails a centralized circuit-based protocol anchored at the base station. SIRLoS is aimed at enabling network nodes to discover *uplink* routes for data forwarding to, and a *downlink* routes for data receiving from the base station respectively. In summarizing the protocol, the base station initiates neighborhood discovery by flooding cluster head-distinct circuit discovery beacons (CDBs) into the network via all the cluster heads. The beacons act as agents that traverse the network, gathering routing data (such as sequence of nodes encountered) as they propagate. That is, nodes append their unique information to any new CDB encountered after they record data from those beacons into their routing tables, before rebroadcasting the beacon to its successors.

A CDB is terminated whenever it expires (a concept we will explain in the next section) or it first reaches an exit cluster head, that then returns the beacon to the base station, thus completing a BS-circuit. The base station, having gathered all the

returned CDBs, employs the location, connectivity and security data extracted from the returned beacons to reconstruct the global network topology, and then update the routing tables of each node. The base station also acts at the umpire to ensure that security and trust are not breached.

We piggyback a simple, light weight and coarse localization scheme to further leverage the bandwidth utilized for neighborhood discovery in SIRLoS. The centroid method localization algorithm enables nodes to coarsely estimate their locations based on the location estimate of predecessors as well as the orientation information which is included in the CDBs they propagate. A light weight topology control mechanism is suggested to provide refined location estimate with improved performance to the centroid only methods [74].

In formulating the neighborhood discovery mechanism of SIRLoS, as commonly required for sensor networks, our objective is to be efficient in terms of minimizing routing overhead such as storage, computation and communication, preventing fabrication or alteration of routing signals, preventing routing loops, as well as incorporating scalability for large networks. In contrast to omnidirectional sensor networks, there is naturally a heavier routing overhead in WOSNs which justifies leveraging the centralized nature of the base station. By shifting more of the processing to the base station, it is possible to make the protocol lightweight at the node's end. We consider three secure routing phases:

1. **Neighborhood discovery**: initiated by the base station soon after network deployment, and employing a beacon flooding mechanism, the goal of this phase is to efficiently and securely obtain a global view of the network topology. In contrast to many omnidirectional network neighborhood discovery mechanisms, this phase is terminated by the base station.

2. **Dynamic route establishment**: leveraging the base station, this phase is initiated by individual nodes on a per need basis after neighborhood discovery. This is similar to some well known protocols for omnidirectional networks such as SNEP [31] which also employs the help of the base station for pairwise key establishment. In this case, the base station provides routing updates.

3. **Route maintenance**: is initiated by nodes and provides a mechanism for discovering malfunctioning paths by exploiting multi-path routing and low rate acknowledgement packets.

We employ the following notations to describe our security protocols: $A|B$ denotes concatenation of message A with message B if both proceed from the same node and $A||B$ if A and B are from different nodes, while $\mathbb{E}_K[M], \mathbb{D}_K[M]$ and $MAC_K\{M\}$ denote the encryption, decryption and message authentication code (MAC) of message M with key K respectively. We assume all encryptions employ a symmetric 64-bit key RC5 scheme. The $\oplus$ notation denotes the XOR function which we have chosen to use because as it does not expand byte overhead of the algorithm and is easily undone at the base station. We assume that time t is broken into a number of slots, and the network is synchronized employing the algorithm proposed in [9].

1. Efficient Neighborhood Discovery

a. Off-line Key Setup

The first stage of SIRLoS is off-line key generation and setup performed prior to network deployment. A μ-TESLA mechanism [31] is leveraged for BS broadcast authentication. Briefly described, the BS pre-computes and stores a length-E one-way *key chain* $\{K_e\}$ for $e = 0 \cdots E$, by successively applying a known one-way hash function $\mathcal{F}$ to a randomly generated initial key K_E, so that $K_e = \mathcal{F}(K_{e+1})$ where

$e = 0, 1, \cdots E-1$ indexes a particular broadcast era, and E is large enough to span the network's lifetime. The last key of the chain K_0, known as the *commitment*, is preloaded into each node. Due to the nature of $\mathcal{F}$, future keys cannot be computed from previous keys. However, it is trivial to verify that a key K_e once revealed was derived from a previous key, by simply applying $\mathcal{F}$ to K_e $(e-1)$ times, denoted $\mathcal{F}^{e-1}(K_e)$, and verifying that the result equals K_0. After deployment, keys in $\{K_e\}$ are revealed to nodes by the BS in the reverse order from which they were generated, yielding an efficient, simple and lightweight mechanism for BS authentication.

b. Challenge and Respond Protocol

After deployment, each CH, say $s_x^* \in \mathcal{CH}$, indicates its readiness to begin neighborhood discovery by sending a READY signal to the BS within a specified time period. The base station responds by generating a unique nonce η_t^x at the start time $t = 0$ for s_x, and initiating the *challenge-and-respond protocol* (CRP) [31] to authenticate s_x^* employing K_x and PW_x. The CRP also provides a simple *range and angular* estimation mechanism for determining Υ_x. If s_x^* passes the challenge, the BS sends it a *circuit discovery beacon* (CDB) containing its position Υ_x, marked with η_t^x and encrypted with K_N for onward flooding. The exchange is:

$$BS \rightarrow s_x^* : \mathbb{E}_{K_x}[\eta_t^x]$$

$$s_x^* \rightarrow BS : \mathbb{E}_{K_x}[PW_x \oplus \eta_t^x]$$

$$BS \rightarrow s_x^* : [\mathbb{E}_{K_N}[\underbrace{\mid HT = 0 \mid e = 1 \mid K_1 \mid \eta_t^x \mid \Upsilon_x \mid ... \mid}_{CDB}]$$

where HT is a variable that counts the *number of hops traveled* by the CDB and is thus incremented at every intermediate node. The base station sends individual CDBs to all cluster heads at the same time $t = t_0$. We assume that $t_0 = 0$.

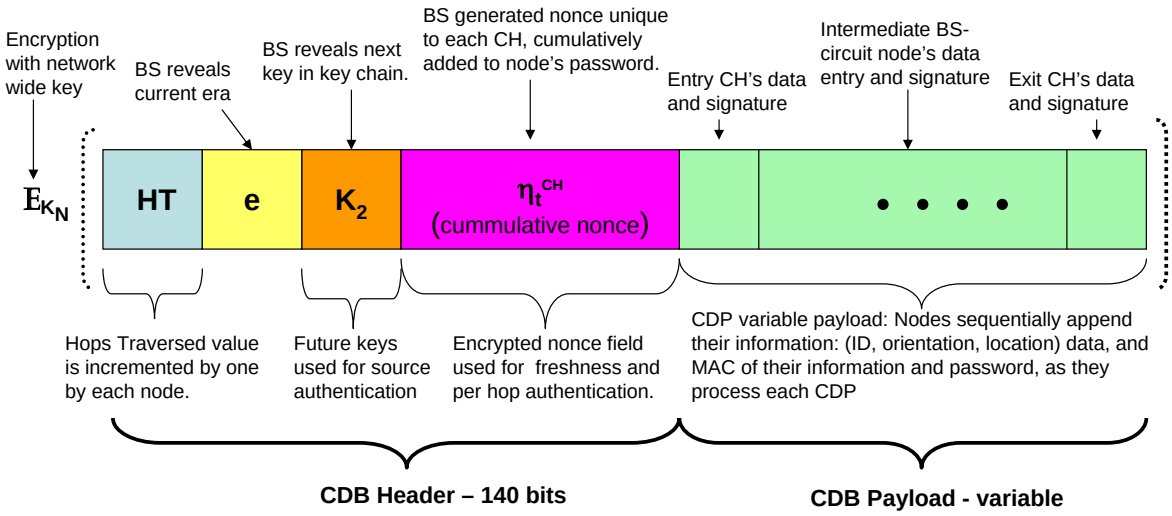


Fig. 21. Illustrating the format and various fields of a CDB packet.

c. Format of the CDB

The CDB consists of a 140-bit header[2] and a variable payload into which each node s_i encountering the CDB inserts a 160-bit entry consisting of its 32-bit information vector (8-bit name, 16-bit position and 8-bit orientation values) and a 128-bit HMAC-MD5 signature computed as $MAC_{K_i}\{I(s_i)|PW_i\}$. The header consists of a 4-bit field for HT, an 8-bit field to hold e, and two 64-bit fields for revealing K_e and the rolling nonce values, respectively. Each node s_x that encounters the CDB also increments HT by one, and xor's its password to the rolling nonce. Figure 21 depicts the format and the various fields of a CDB packet, with their associated functions. Consider for example, the CDB packet in the first era at time step $t = 2$ after the beacon has traversed two nodes s_x^* and s_y as:

$$[\, HT = 2 \,|\, e = 1 \,|\, K_2 \,|\, \eta_{t+2}^x \,||\, I(s_x) \,|\, MAC_{K_x}\{I(s_x)\,|PW_x\} \,||\, I(s_y) \,|\, MAC_{K_y}\{I(s_y)\,|PW_y\}\,],$$

[2]The size of the header should scale up with increasing numbers of nodes, size of observation area.

where $\eta^x_{t+2} = \eta^x_{t+1} \oplus PW_y$ and $\eta_{t+1} = \eta^x_t \oplus PW_x$.

The CDB carries a progressively higher overhead in contrast to beacons in omnidirectional networks and/or void of security inputs, where the 128-bit MAC entry per node encountered is not required. This higher communication overhead which depends on δ, and p_{CH} requires higher bandwidth capacity provided by the FSO medium, and is partially offset by pushing more of the computation to the base station.

d. Hot Potato Node Processing of the CDB

Each node s_i (including cluster heads) maintains a *predecessor routing table* PRT(s_i) into which it makes entries of the information vector of each of its predecessors along with the chronologically organized IDs of nodes on the corresponding downlink and an associated *cost value* C_d, which is equivalent to the HT value of the CDB at the time it arrives at s_i. We denote as C_{d_0} the HT value of the very first CDB a node receives. Upon receipt of the very first CDB from a predecessor s_h at time step $t_0 + C_{d_0}$, s_i decrypts the packet and performs some security and hop count checks within one time step, and immediately passes the CDB to its successors. We name this phase of routing the initial CDB as each node the *hot potato routing phase*. The checks performed by the node before passing the initial CDB are as follows:

1. Validation of the source of the packet by checking that $\mathcal{F}^{e-1}(K_e) = K_0$;

2. Verification that s_i has not previously seen this CDB or that s_i's data is not embedded in the current CDB's payload, thereby avoiding routing loops.

If $s_i \notin \mathcal{CH}$, it estimates its location Υ^{est}_i based on the location of its predecessors included in the payload of CDB's it receives, by employing the location estimation algorithm described in section 2. If $s_i \in \mathcal{CH}$, it simply obtains its accurate coordinates

from the CDP received from the BS as previously noted above. It then performs a subsequent *range-and-orientation constraint* (ROC) test to verify that:

$$d(\Upsilon_h, \Upsilon_i^{est}) \leq r \quad \text{and} \quad |\Theta_i - \Psi_{hi}| \leq \frac{\alpha}{2},$$

where $d(a, b)$ is the Euclidean distance between points a and b, and

$$\Psi_{hi} = \arccos \frac{d(y_h^e, y_i)}{d(\Upsilon_h, \Upsilon_i^e)}$$

ensures that $\Upsilon_i \in \Phi_h$. The ROC test provides a geometric constraint on the network graph which is exploited as a security check, and provides protection against routing attacks such as wormholes.

If this CDB is the very first one encountered by the node at time $t_0 + C_{d_0}$ the node engages the hot potato routing strategy. Essentially, it processes and forwards the CDB within one time step, otherwise if this is not the first CDB it receives, it caches the CDB in its buffer and waits to perform the *restricted and compounded flooding* phase described in subsection f. Observe that a node may receive more than one CDB's at $t_0 + C_{d_0}$, in which case it randomly selects only one of the CDB's to forward in the hot potato phase and caches the other CDBs for compounded flooding. We have made the reasonable assumptions that one time step Δt is sufficiently long to accommodate a CDB's reception, processing and re-transmission, and that a node can receive a CDB while transmitting another CDB in the same time step.

Before forwarding its initial CDB, s_i verifies that $C_{d_0} \leq \delta$ (i.e., the CDB has not expired), where δ is the maximum number of hops a CDB is allowed, and represents the diameter of the network[3]. As previously stated δ is predetermined by the base station and known to nodes prior to deployment. If $C_{d_0} \leq \delta$, the node increments

[3]Number of links in the shortest path between the furthest pair of nodes.

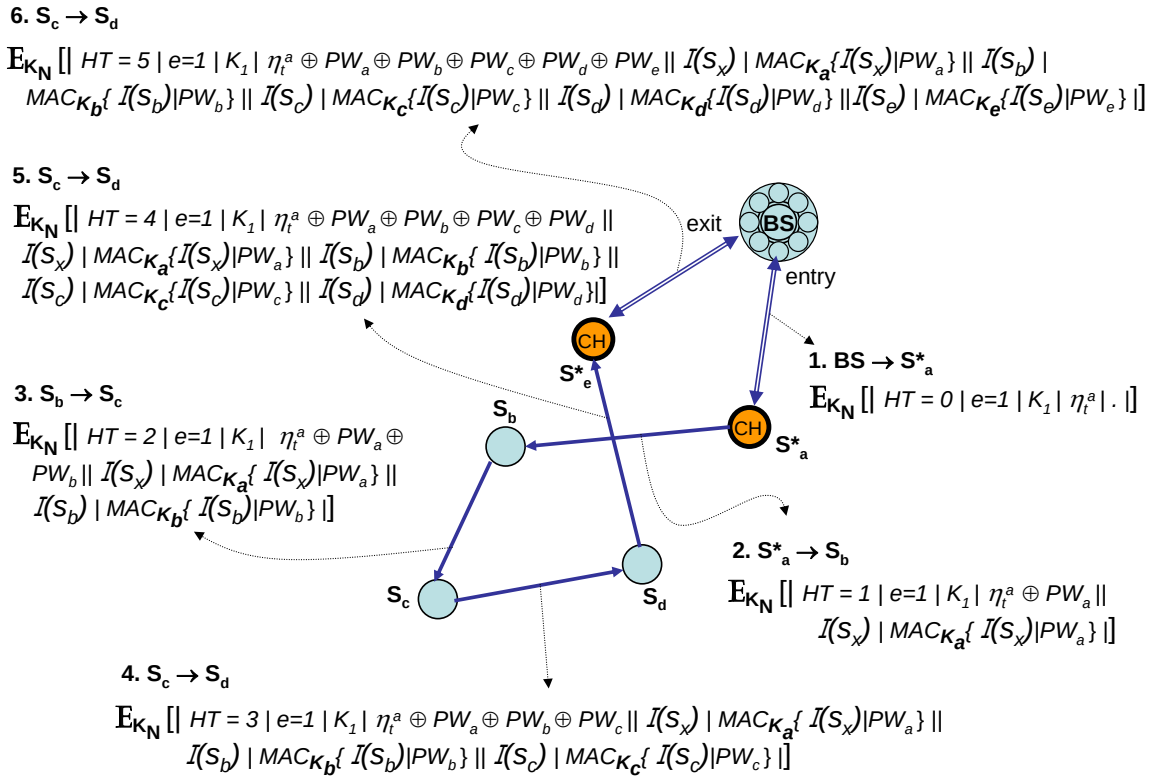


Fig. 22. Illustrating the information gathering and processing within a CDB as it traverses a BS-circuit during neighborhood discovery.

the HT field by one, updates the current nonce $\eta^*_{t_0+C_{d_0}}$ in the packet as $\eta^*_{t_0+C_{d_0}+1} = PW_x \oplus \eta^*_{t_0+C_{d_0}}$, appends its data $[I(s_i) \mid MAC_{K_x}\{I(s_x)|PW_x\}]$ to the CDB's payload, re-encrypts the new CDB with K_N, and then re-broadcasts the updated CDB to its successors at time step $t_0 + C_{d_0} + 1$.

The route discovery task of a CDB with $1 < HT \leq \delta$ is terminated when it encounters a cluster head, who completes the BS-circuit by returning the packet to the base station. A CDB is discarded if $HT > \delta$ or if it fails any of the security checks. The information gathering and processing of a CDB as it traverses a typical BS-circuit during neighborhood discovery (assuming it is the first packet that all nodes on the BS-circuit encounter) is illustrated in Figure 22. Before concluding this phase, within

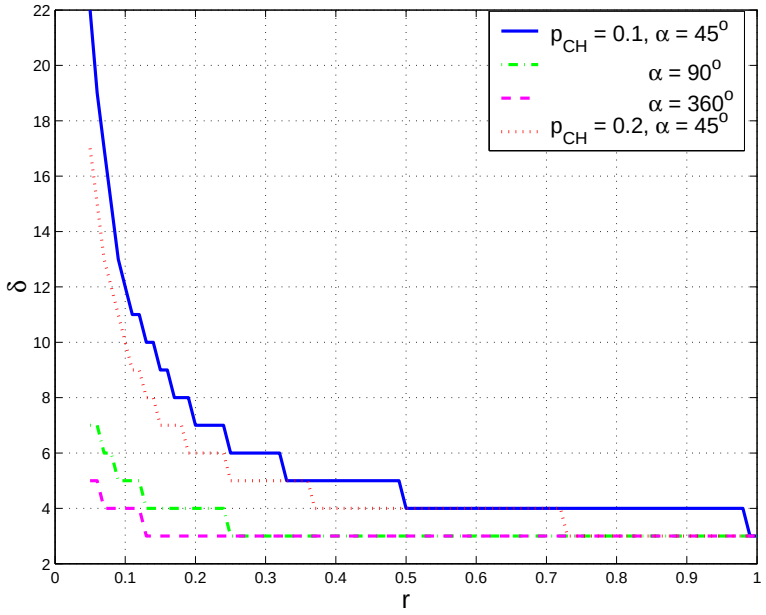


Fig. 23. Values for δ for $n = 500$ depend on r, α and p_{CH}.

$\tau < \Delta t$ seconds after transmitting the initial CDB, each node s_i broadcasts a low-bit hello packet (HELLO_i) within a communication sector $-\alpha/2 + \Theta_i \leq \varphi_i^1 \leq +\alpha/2 + \Theta_i$ of radius $r' < r$, discussed in the next subsection.

e. Determining δ

It is easy to imagine that the network diameter δ, which bounds the maximum BS-circuit length, ought to increase with n and decrease with p_{CH}, α and r. Through simulations and trying various formulas, we find that δ is sufficiently determined as:

$$\delta = \left\lceil \frac{-\log(p_{CH}) \log(n)}{8\alpha r} \right\rceil$$

While we have not employed a methodical derivation of this formula, we find that it closely reflects the maximum depth of a directed $\lceil np_{CH} \rceil$-root node forest [25] built on $G_n(\mathcal{S}_n, \mathcal{E})$, controlled by r and α (radians) which guarantees that 99% of nodes

are reached by SIRLoS. Figure 23 shows the values of δ for various parameter values. For example, $\delta = 12$ for $p_{CH} = 0.1$ and $\alpha = 45^o$, while it is 10 for the same α and $p_{CH} = 0.2$. For the omni directional network, δ represents the maximum depth of the forest the reaches all nodes. Observe also that when $p_{CH} = 1$, implying that every node is a cluster head, then $\delta = 0$.

f. Restricted and Compounded Flooding

After re-broadcasting the initially received CDB of cost C_0 as described in section d, a node waits and listens to the channel for a period of $\delta - C_0$. This wait enables the node to receive CDBs from its other predecessors as these beacons may not have reached it at time $t = C_0$ when it received, processed and forwarded the initial CDB. A node time stamps each CDB arriving after $t = C_0$ and caches the packet until the assigned wait period, expires (at time step $t = \delta$). The node then concatenates all the CDBs it has received during this time, into one *compound circuit discovery beacon* (C^2DB), and forwards this C^2DB to its successors following a simple schedule of transmission.

Only nodes that received CDBs or C^2DBs after the hot potato phase of SIRLoS may consider transmitting to its successors during the next time step, according to the scheduling algorithm described in subsection g below. All other nodes continue to listen for beacons in the channel. Any node that has received and buffered one or more CDBs or more than one C^2DB during its waiting phase, schedules the aggregated packet for transmission with probability 1. This is because the CDBs within the network at this time contain new information on the network topology that has not yet reached the base station. On the other hand, if only one C^2DB is received from a predecessor, it is processed and scheduled for rebroadcast with a probability of $p_r = 2/n\alpha r^2$. Otherwise, the C^2DB is dropped. The value of p_r is the reciprocal

of $n\alpha r^2/2$, which represents the expected number of neighbors of a node [4], thereby ensuring that the network is not flooded with each node's C^{2}DB. Similar to the CDB, the transmission of the C^{2}DB is terminated when it encounters a cluster head, or if its HT value exceeds δ.

g. Schedule of Transmission

At time step $t = \delta + 1$ only nodes that have a packet scheduled for rebroadcast will perform the following schedule of transmission algorithm (SA) described in Table VII, where the phase i is initialized to 1:

Table VII. Schedule of transmission algorithm *SA(i)*.

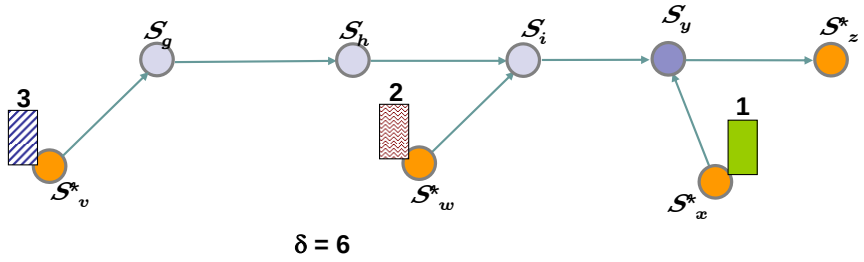
a) ORANGE: transmit with probability $p_s = \frac{\delta - C_0}{\delta}$;
b) GREEN: for $i > 1$, transmit with probability 1 if did not transmit in $i - 1$;
c) RED: wait and listen for $\delta - (C_0 + i)$ time steps;
d) i ++, repeat SA$(i++)$.

The SA is a stochastic algorithm that mimics the pattern of traffic light scheduling somewhat, by slowing down travel and bunching up packets during the orange and red steps, and then moving them onto the next intersection with the green step. Observe that the scheduling algorithm is only executed by nodes that have a buffered packet waiting to be rebroadcast at $t > C_0$. Figure 24(a) illustrates a sample 13-node network, and the associated schedule of transmissions for three packets originating at different cluster heads within the network is depicted in Figure 24(b). We have assumed that at $t = \delta = 6$ time steps, and observe that C_0 is one for both s_i and s_y.

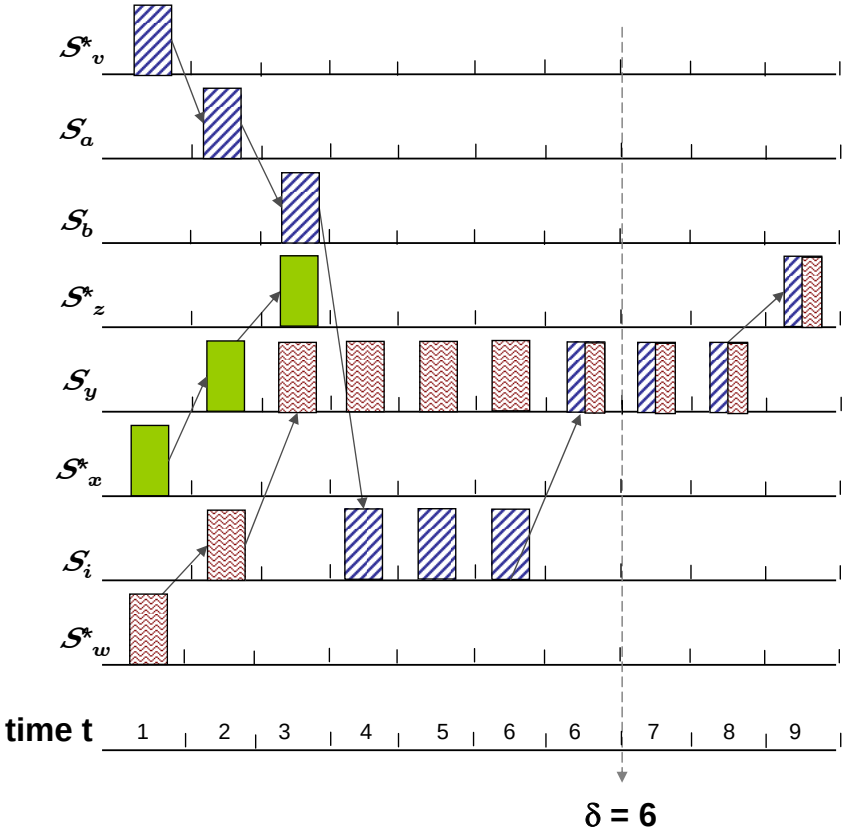
[4]The average out degree of $G_n(\mathcal{S}_n, \mathcal{E})$.

After a wait of $\delta - C_0$ we observe that s_i makes the decision (with probability 5/6) to transmit while s_y waits for an additional $\delta - C_0 - 1$ and then transmits as proposed by the scheduling algorithm. In this case, it requires 10 time steps to complete the transmission of the packets within the network.

Obviously the schedule of transmission observed for s_i and s_y in the example above may have been reversed, leading to larger overall delays. For example, at $t = \delta$, if s_i had chosen (with probability 1/6) to wait for 4 time steps, and s_y had chosen to transmit (which occurs with probability 5/6), and then to wait for 3 time steps at $t = 10$, then the overall delay in the network would increase to 13. From this example, it is obvious that the maximum possible delay incurred by the SIRLoS algorithm in the network of diameter d is determined as $\delta(\delta - 1)$. This delay is observed in the worse case scenario in which each node along a BS-circuit of length δ is within one downlink hop from a cluster head, and chooses to wait for $\delta - 1$ time steps during its initial round of the scheduling algorithm. The node furthermost from the exit cluster head receives an additional packet in the second time step. Recall that we have assumed time synchronization within the WOSNs, employing the methods proposed and explored in [9].



(a) Sample 10 node network.



(b) Time line of packet transmission.

Fig. 24. Illustrating the transmission of various packets within a sample network.

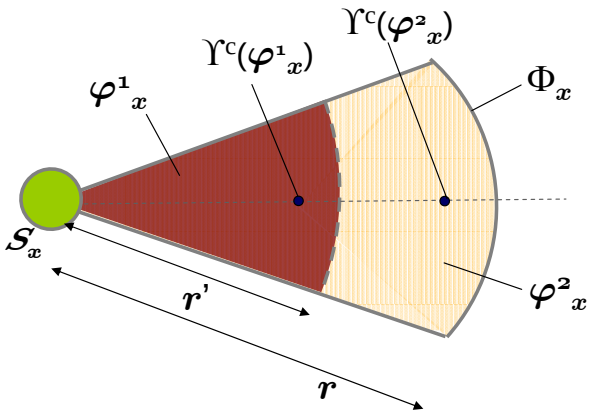


Fig. 25. The centroid of the two regions φ_x^1 and φ_x^2 that comprise the communication sector Φ_x of node s_x. The sector-based communication provides more localized estimation of the node position and the additional HELLO-phase provides even finer granularity.

2. Location Estimation

The reception of a CDB provides a node s_i with knowledge that it lies within the communication sector ϕ_i of the predecessor that forwarded the CDB. To provide finer granularity to location estimation, we employ the following procedure. After τ seconds of receiving a CDB from s_i, s_j may determine that its location Υ_j lies either within the sector $\varphi_i^1 \in \Phi_i$ if it received HELLO$_i$, or otherwise within the circular segment $\varphi_i^2 \in \Phi_i$ as depicted in Figure 25, and then estimates its location Υ_j^{est} as the *centroid* of the corresponding region. The centroid is known to be the *least square error solution* [91] given that s_j falls with equal probability at any point within Φ_i. We consider location estimation in the two possible cases.

Case 1: Node s_j concludes that $\Upsilon_j \in \varphi_i^1$ and determines Υ_j^{est} as the centroid $\Upsilon^c(\varphi_i^1)$ of the sector φ_i^1 given by the well known formula for the centroid of a sector:

$$\Upsilon_j^{est} = \begin{pmatrix} x_i \\ y_i \end{pmatrix} + \left| \frac{2r' \sin(\alpha)}{3\alpha} \right| \begin{pmatrix} \sin(\theta_i) \\ \cos(\theta_i) \end{pmatrix} \tag{4.1}$$

where $|.|$ denotes absolute value, and $r' = r/\sqrt{2}$ is determined to be the optimal radius of φ_1 such that $A(\varphi_1) = A(\varphi_2)$, implying it is equally likely that s_j falls within either part.

Case 2: Node s_j concludes that $\Upsilon_j \in \varphi_i^2$ and determines Υ_j^{est} as the centroid $\Upsilon^c(\varphi_i^2)$ of the sector segment φ_i^2:

$$\Upsilon_j^{est} = \begin{pmatrix} x_i \\ y_i \end{pmatrix} + \left| \frac{2r\sin(\alpha)}{3\alpha} \right| \left(\frac{2\sqrt{2}-1}{\sqrt{2}} \right) \begin{pmatrix} \sin(\theta_i) \\ \cos(\theta_i) \end{pmatrix}, \tag{4.2}$$

Equation 4.2 is easily derived by employing the formula for the centroid $\binom{x^c(\Lambda)}{y^c(\Lambda)}$ of an M-part composite shape Λ given as:

$$\begin{pmatrix} x^c(\Lambda) \\ y^c(\Lambda) \end{pmatrix} = \frac{\sum_{j=1}^{M} A(\lambda_j) \binom{x^c(\lambda_j)}{y^c(\lambda_j)}}{\sum A(\lambda_j)},$$

where $A(\lambda_j)$ and $\binom{x^c(\lambda_j)}{y^c(\lambda_j)}$ represent the area and centroid of the j^{th} individual part of Λ, respectively. With Φ composed of two parts φ^1 and φ^2 as depicted in Figure 25, it is easy to rearrange the equation above to yield:

$$\begin{pmatrix} x^c(\varphi^2) \\ y^c(\varphi^2) \end{pmatrix} = \frac{A(\Phi) \binom{x^c(\Phi)}{y^c(\Phi)} - A(\varphi^1) \binom{x^c(\varphi^1)}{y^c(\varphi^1)}}{A(\varphi^2)}$$

Substituting $A(\varphi^1) = A(\varphi^2)$, yields $\Upsilon^c(\varphi^2) = 2\Upsilon^c(\Phi) - \Upsilon^c(\varphi^1)$, where the formulae for the centroids $\Upsilon^c(\Phi)$ and $\Upsilon^c(\varphi^1)$ of sectors of radius r and r' respectively may be derived from Equation 4.1, easily yielding the expression of Equation 4.2.

If s_y hears $m > 1$ predecessors at time step $t \geq C_0$, it estimates its location as the average of the centroid's of the m regions within which it falls, given as $\Upsilon_j^{est} = \frac{1}{m} \sum_{q=1}^{m} \Upsilon^c(\varphi_i^q)$. Similarly, it continues to refine its location estimate with each CDB or HELLO packet it receives from a new predecessor. In this case, Υ_j^{est} does not represent the centroid of the overlapping region of the m sectors, but instead the midpoint of the centroids of the communication sectors of predecessors, which is

simply a location within the sectors overlap region. For our method, nodes are not required to perform range estimation or angle-of-arrival measurements, keeping both computational and communication overhead low. Our simple and computationally efficient mechanism for location estimation does not require complex search algorithms to determine the boundaries of the irregular shaped overlap region, or grid score tables to find the centroid of the resulting overlap region as was proposed in [91]. While our simple localization scheme does not perform as well as other hardware based and computationally intensive schemes such as [91], it serves well as a good first estimate of the locations of node, which may be further employed as the initializing seed for other more complex localization algorithms. For example, with the scheme proposed in [91], our estimate may be employed to determine the boundaries of a more conservative grided search region, rather than what has been proposed.

While the centroid-based scheme proposed in [91] yields the least square error estimate of a node's location, we justify our approach due to the minimum delay and computation incurred as it is integrated with the neighborhood discovery scheme. Our scheme also differs from well known triangulation methods in which each node must wait to receive beacons from three known-location predecessors to determine its location. The authors of [9] have proposed a localization scheme for WOSNs based on triangulation, in which they show that the scheme converges asymptotically, that is as network density increases to infinity.

3. Secure Base Station Network Topology Reconstruction

The BS is able to reconstruct and estimate $G_n(\mathcal{S}_n, \mathcal{E}')$ of $G_n(\mathcal{S}_n, \mathcal{E})$ from the BS-circuits and individual node information available in returned CDBs and C^{2}DBs. First, it validates each CDB (or parsed CDB contained in a C^{2}DB) received (as discussed below), and then constructs an adjacency matrix $\mathcal{E}'$ by assuming that a

subsequent node in a CDB's chronologically organized payload entry is a successor of the previous node. That is, if s_j's entry follows that of s_i, the BS assumes $s_i \rightarrow s_j$ and hence $\mathcal{E}'_{ij} = 1$. The BS also records (or compares with existing records) the information vector of each node represented in each received and validated CDB.

To validate a CDB, the BS performs the following security checks:

1. verifies that HT equals the number of appended sections in the payload;
2. verifies the claimed identity and per hop entry of each node s_i with an input in the payload, by ensuring that its computed $MAC_{K_i}\{I(s_i) \mid PW_i\}$ is equivalent to the signature entry of the node;
3. performs the ROC test for each link represented in the payload;
4. verifies that the final cumulative path nonce η^*_{t+h} included in the CDB for each h-length path, say $s* _1 \rightarrow s_2 \rightarrow \cdots \rightarrow s_h$, equals $\eta^1_t \oplus PW_1 \oplus PW_2 \oplus \cdots \oplus PW_h$.

If any of the four security checks fail, or the BS observes any discrepancy in the entries of any CDB, that CDB is discarded, and intrusion detection mechanisms initiated on the suspicious routes.

4. Updating Nodes Routing Tables

From $\mathcal{E}'$, the BS constructs both the predecessor routing table PRT(s_i) and the successor routing table SRT(s_i) for each node s_i. Similar to PRT(s_i), each of s_i's authentic successor's information vector, associated uplink and path cost is entered into SRT(s_i). The BS unicasts the encrypted routing tables $\mathbb{E}_{K_i}[\text{RT}(s_i)] = \mathbb{E}_{K_i}[\text{PRT}(s_i)|\text{SRT}(s_i)]$ to s_i, who upon receipt, compares the PRT from the BS with its self-registered PRT. Any discrepancy observed in entries triggers suspicion and deletion of the corresponding circuit from PRT(s_i) and a report to the BS. Figure illustrates a sample 12-node

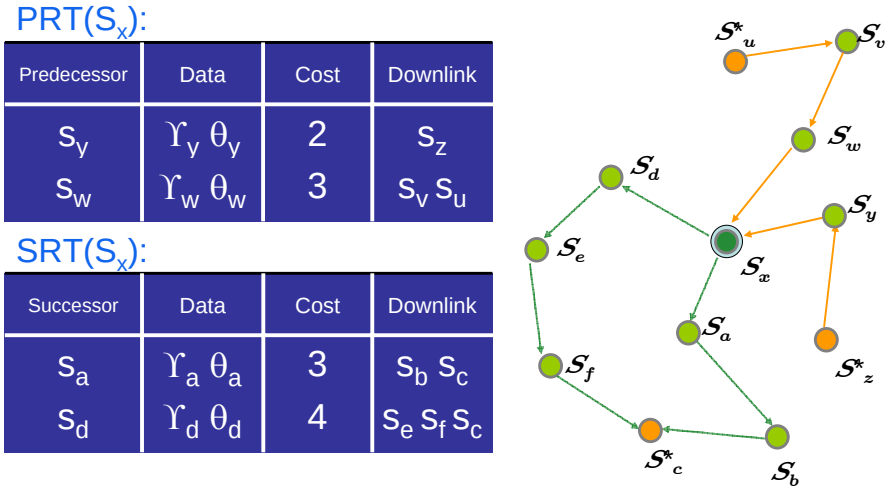


Fig. 26. A sample network with the corresponding predecessor and successor routing tables PRT(s_i), SRT(s_i) for node s_i.

network and the corresponding PRT and SRT for node s_i. Observe that the size of the routing tables is dependent on the expected number of predecessors and successors which is $n\alpha r^2/2$. Nodes that receive valid routing tables conclude the neighborhood discovery phase by sending an acknowledgement (ACK) to the BS. The BS queries nodes from which it has not received an ACK within a stipulated time frame. Each node employs the minimum cost route in its SRT to transmit its sensor data to the base station by fixing its laser in the direction of the appropriate successor. Figure 26 illustrates a sample network with the corresponding predecessor and successor routing tables PRT(s_i), SRT(s_i) for node s_i. The optimal downlink and uplink paths is seen to be via nodes s_y and s_a respectively.

5. Dynamic Route Setup

Dynamic route establishment for the WOSN entails a node, say s_i, seeking a secure and efficient route to any node s_j as needed, by leveraging the BS [31]: s_i sends an

encrypted route request RREQ(s_j) for s_j to the BS, who responds by sending s_i the minimum cost path for $s_i \rightsquigarrow s_j$, and sending s_j the minimum cost RETURN link for $s_j \rightsquigarrow s_i$, encrypted with K_i and K_j respectively. The BS also includes a unique pairwise key K_{ij}^e to enable s_i and s_j establish a secure communication for a session.

6. Route Maintenance

Route Maintenance for SIRLoS aims to discover malfunctioning, dead or subverted nodes along BS-circuits, and is achieved by leveraging the naturally occurring path diversity in the network; each node is with high probability, contained in more than one disjoint BS-circuit, and hence can exploit multiple uplink paths to the base station in order to alert the network of possible malicious behavior. The expected number of unique uplinks and downlinks to the base station is equivalent to the expected number of successors and predecessors respectively. Route maintenance is initiated if a node does not receive updates to their routing tables from the base station.

A node floods route maintenance request (RMReq) towards the base station via all its successors uplink paths by scanning its laser. A RMReq is signed and encrypted with a nodes individual key. Once a base station receives and authenticates a RMReq, he initiates route maintenance by querying each downlink path to the affected node by requesting multi-path 'multi-cast' returns of his route maintenance query (RM-Query) packet, similar to flooding. Each node encountering the RMQuery appends its signature along with its information vector and time stamp on the RMQuery so the packet accumulates chronological BS-circuit information. Validated circuits whose RMQuery packets return to the base station are marked as functional. Since flooding is robust, this process will easily discover non cooperative nodes in a given BS-circuit.

Time stamping a RMQuery may also be employed by the base station to detect nodes that are running malicious code using mechanisms similarly utilized for

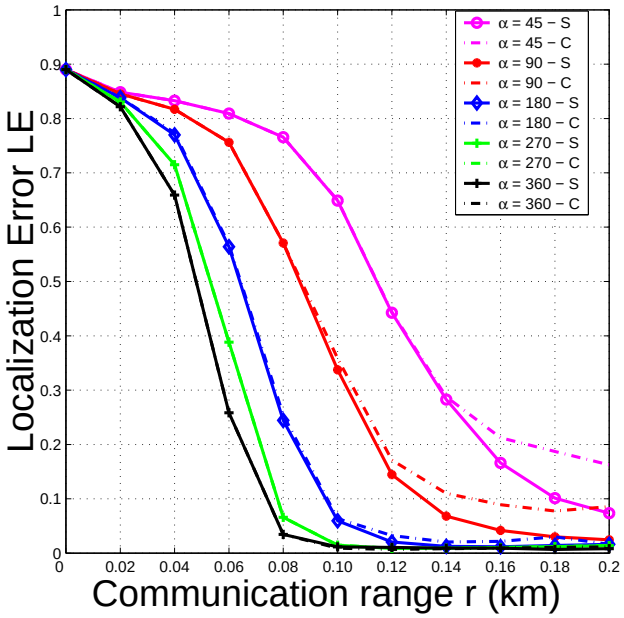


Fig. 27. Simulation results for localization error versus r with $p_{CH} = 0.1$.

remote entity verification. Aimed at exposing malicious nodes that attempt to avoid detection by correctly processing RMQuery and similar intrusion detection packets, the underlying assumption is that, additional time is required for a malicious node to reload authentic code in memory in order to correctly process a RMQuery, resulting in a time delay that is longer than normal, thereby exposing the fraudulent node.

C. Performance Evaluation

We employ MATLAB simulations and analysis to study performance metrics of SIRLoS. With α, p_{CH} and r preset, $n = 300$ nodes are randomly positioned and oriented in a planar square region of unit area 1 km^2 according to a uniform distribution. As predecessor relationships are derived by reversing successor links, it suffices to populate $\mathcal{E}$ by determining successor relationships only, using the ROC test between each node and every other node. We employ Monte Carlo mechanisms, repeating each

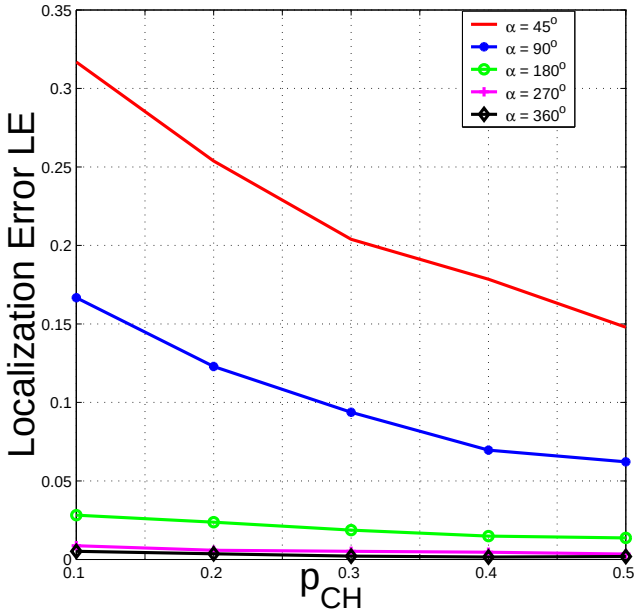


Fig. 28. Simulation results for localization error versus p_{CH} with $r = 0.1$ km.

simulation scenario 1000 times, and averaging the results over all the trials to yield an acceptable statistical confidence of obtained results. We study three important metrics of performance for SIRLoS, including localization error, average hop count and end-to-end delay of the routing mechanism in the network.

1. Localization Error

With p_{CH} set to 0.1, and r varying from 0 through 0.2 km, we run SIRLoS and compute the localization error LE $= \sum_{i=1}^{n} \sqrt{(x_i - x_i^c)^2 + (y_i - y_i^c)^2}/n$ as the mean squared error between the correct and estimated position vectors (initialized to zero) of $\mathcal{S}_n$. Figure 27 illustrates plots of LE versus r for SIRLoS denoted "S" which performs better, compared with the centroid only [91] method (positions are estimated as the average centroid of the sectors of predecessors) denoted "C", as r increases and α decreases. Observe that as $r \to 0$, LE $\to (1 - p_{CH})$ (in this case 0.9), since

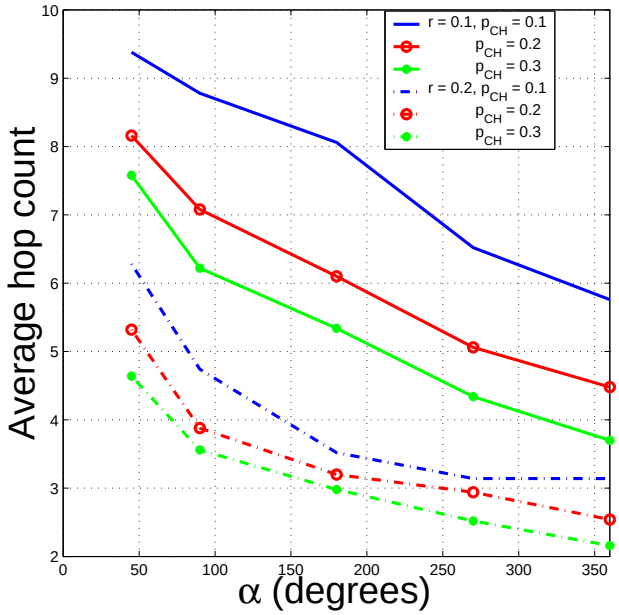


Fig. 29. Simulation results for average hop count versus α.

the network is almost surely disconnected at small r values and CHs are the only nodes that determine their positions (accurately) from the BS. Another interesting observation is the 'phase transition' property [19], (LE transitions rapidly from a maximum to minimum value) which gets more dramatic as $\alpha \rightarrow 2\pi$. As expected, LE improves for larger α and r, as a greater number of predecessors are available for location estimation. In a second experiment, we vary p_{CH} from 0.1 through 0.5 and measure LE for various α, with $r = 0.1$ km. Figure 28 illustrates plots of LE decreasing with increasing p_{CH} and α.

2. Average Hop Count

To study the communication overhead of SIRLoS, we observe average hop count $\overline{HT}$, (computed by averaging HT values of CDB's received by the BS) versus α with r set to 0.1 and 0.2, and corresponding p_{CH} of $0.1, 0.2$ and 0.3, $n = 500$. We observe from

Figure 29, that increasing r yields greater improvements in $\overline{HT}$ than a corresponding increase in p_{CH}, showing it more beneficial to focus resources on increasing r and α rather than p_{CH}.

3. End-to-End Delay Analysis

The hot potato phase of SIRLoS incurs a delay of δ while we previously showed the worst case delay for the compounded flooding phase to be $\delta(\delta - 1)$, so that the worst case end-to-end delay for SIRLoS is δ^2. For comparison, we have simulated the SIRLoS and measure the end-to-end delay compared to the simple-bro/simple-gather scheme proposed for neighborhood discovery in [9]. In this paper, the authors proposed three network algorithms for WOSNs, including a localization algorithm based on trilateration, and two separate neighborhood discovery schemes: the *simple-broadcast* for downlink discovery and the *simple-gather* algorithm for uplink discovery. While the algorithms are three separate schemes, we have integrated the localization scheme with the simple-broadcast algorithm in order to achieve the best case delay performance for comparison with our scheme. Figure 30 depicts the average delay for neighborhood discovery in terms of number of time steps or iterations required for SIRLoS compared with the simple-bro/simple-gather scheme, as the network diameter value δ is varied. From the plots, we observe that SIRLoS always outperforms the simple-bro/simple-gather scheme, in the worse case by about 30% and in the best case by more than 100% for the δ values we have observed. The reason for this superior performance is obvious, since the two neighborhood discovery algorithms proposed in simple-bro/simple-gather must be executed serially (i.e. they cannot be executed concurrently since the simple-gather is dependent on the accurate execution of the simple-broadcast within four time steps). In contrast, SIRLoS integrates both steps of downlink and uplink discovery into one efficient BS-circuit discovery.

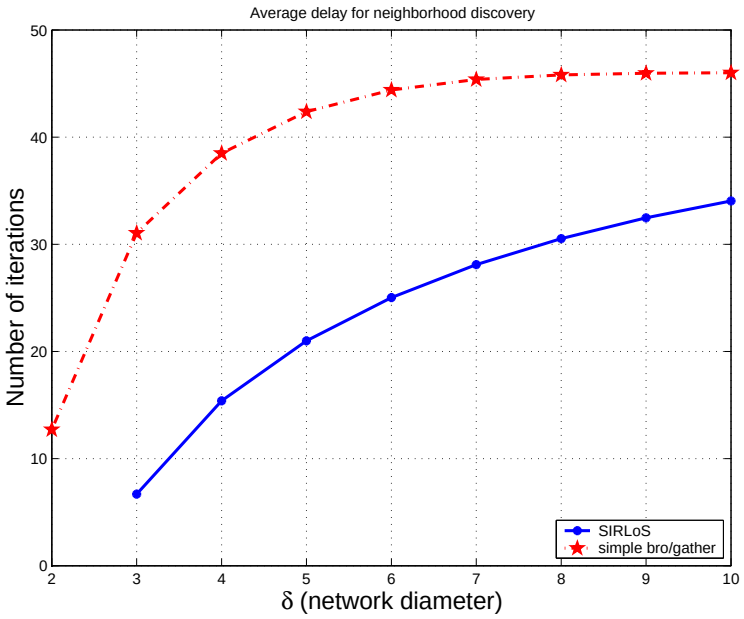


Fig. 30. Simulation results for average delay required for neighborhood discovery versus network diameter δ.

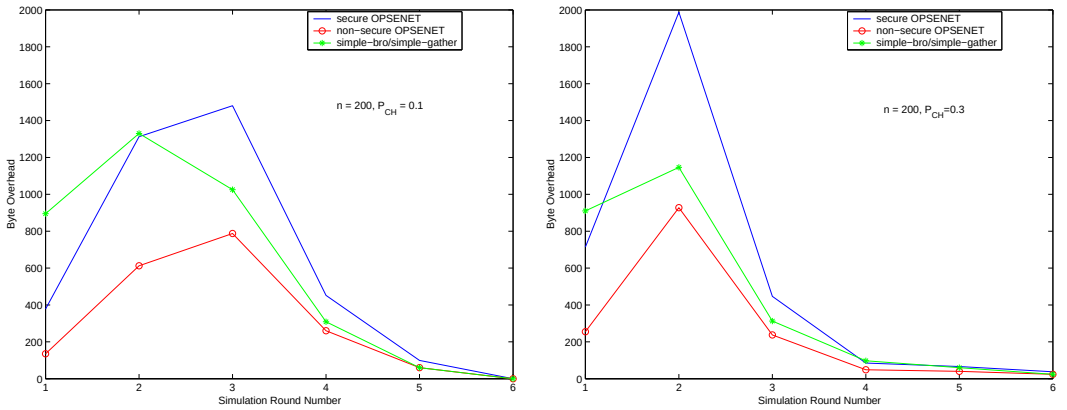
Analytical proofs of the convergence of the two neighborhood discovery algorithms are based on asymptotic assumptions for $n \to \infty$. As we found through our simulations, this assumption unfortunately has practical impacts especially on the localization scheme for real WOSNs with limited n and small p_{CH}, as it is sometimes the case that there are no nodes in the first time step that receive CDBs from three or more cluster heads in order to estimate their locations. In comparing SIRLoS to the proposed neighborhood discovery in [9], we observe that simple-broadcast algorithm executes within four iterations, while the simple-gather executes within $\delta(\delta-1)$ time steps completed by 4 of simple-broadcast time steps for each execution of the simple-gather, as described in the paper. Therefore the total best case end-to-end delay for the `simple-gather/simple-broadcast` is $\delta(\delta-1+4)+4 = \delta(\delta+3)+4$ time steps. Furthermore, the algorithms of [9] have not considered security in their design.

4. Byte Overhead

Another performance metric is the byte overhead (the overall number of bytes) generated by the protocols, which may be used to evaluate, in part, the energy requirements of the protocols. The following parameter values were utilized: 64 bit key length, 8 bits for the nonce and passwords, the HT field is $\lceil \log \delta \rceil$ bits, while a nodes ID and position coordinates are each represented with $\lceil \log n \rceil$ bits. The algorithms complete execution within 6 time steps, with the SIRLoS' paradigm of integrating the broadcasting and gathering steps into one circuit-based step hugely reducing overhead. The security functionality of SIRLoS does result in additional overhead, which quickly dies down in time.

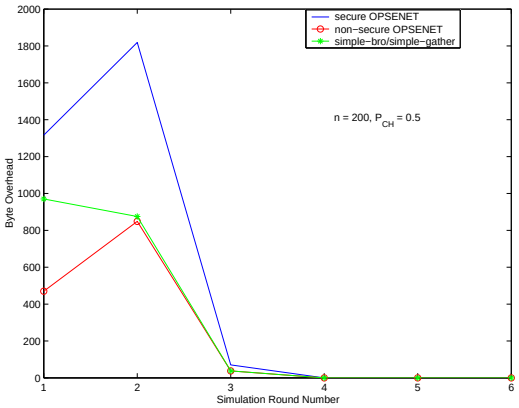
Figures 31 (a) - (d) show comparative plots of byte overhead versus number of rounds of simulation for the two algorithms, for a network size of $n = 200$, while varying P_{CH} as $0.1, 0.3, 0.5$, and 0.7, respectively. Obviously, the non-secure SIRLoS always performs better than the other two algorithms as the CDB in this case is not required to accumulate signatures of per hop nodes. For fewer CHs, security-aware SIRLoS starts out with a lower byte overhead than the `simple-gather/simple-broadcast`, but soon performs worse as the number of rounds and/or P_{CH} increases.

For all the protocols, byte overhead ramps up to a maximum value, and then rapidly declines to zero (i.e. no other packets are being transmitted for the neighborhood discovery). This phenomenon is explained by considering that initial broadcast of the CDB explodes exponentially. However, as the network becomes saturated with the CDB, and executes the restricted and compounded flooding, the number of CDBs or C^2DBs being sent dips steeply. With increasing P_{CH} all the algorithms converge faster as shorter length BS-circuits are observed.

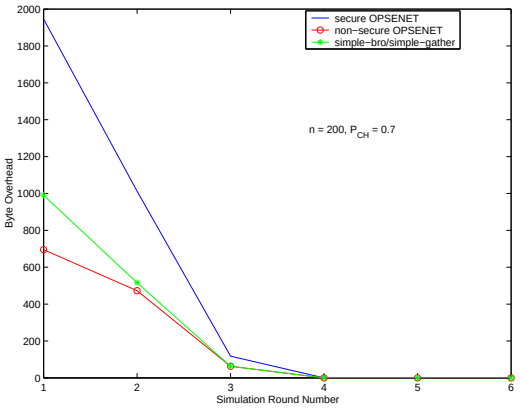


(a) $p_{CH} = 0.1$

(b) $p_{CH} = 0.3$



(c) $p_{CH} = 0.5$



(d) $p_{CH} = 0.7$

Fig. 31. A comparative plot of byte overhead versus number of rounds of simulation for SIRLoS, non-secure SIRLoS and simple-bro/simple-gather algorithm, for $n = 200$ nodes.

D. Security Analysis

In this section, we discuss the security features of the cryptographic primitives employed to mitigate insider and outsider attacks in our algorithm. We earlier classified attacks as insider and outsider attacks. Following convention, we further classify routing attacks into two categories; those that target the routing packets, and those that target the underlying routing protocols. In [11] a further distinction is made between node class and laptop-class attacks which we will not consider here.

One of the fundamental discoveries of this dissertation is that directionality of links may be exploited for security gains. This is due mainly to the fact that the probability that an independently deployed malicious node will exist in both the uplink and downlink paths of a legitimate node, is negligible. Certainly, this probability grows with the number of colluding and distributed attackers, however as we will see this probability is strongly dependent on the value of α. Indeed, we show that as $\alpha \rightarrow 0$, so does this probability. In contrast to the omnidirectional networks, the added degree of diversity due to directionality in multi-hop routing makes it more difficult for a malicious node to control both the forward beacon flow, and the paths followed by their acknowledgement packets. Any attempt at this will easily alert intrusion detection mechanisms at the base station.

The routing security objectives for WOSNs include message confidentiality, integrity, availability, freshness, authenticity, robustness to DDoS attacks (i.e., localizing the effect of a compromised node), described below:

- *Message confidentiality* ensures that a message enroute from source to destination is kept secret from intermediate router nodes for whom the data is not intended. This is often achieved by encrypting the message using an energy efficient and low complexity algorithm such as TEA or RC5 with a key known

only to the source-destination node pair.

- *Integrity* ensures that a message cannot be arbitrarily modified enroute to the destination. Three cryptographic primitives - HMAC, digital signatures and one way HMAC key chains - are widely used for this purpose. For WSNs, digital signatures requiring public key encryption is often too complex. On the other hand, HMAC while efficient and affordable requires pairwise keys, and the lightweight one-way MAC key chain enabling one authenticator to be verified by a large number of receivers is suitable for broadcast message authentication.

- *Authentication*, achieved using a signature or a message authentication code (MAC), enables the destination node to verify that the message was actually sent from the supposed sender and not an imposter.

- *Data Freshness* often achieved with a nonce and/or time stamp, ensures that an original authentic message cannot be stored and then replayed at a later time to confuse the network.

- *Tolerance to node capture* so that there is a gradual degradation of security with node compromise meaning that even if a node is compromised, the attacker cannot use extracted cryptographic information to compromise other parts of the WOSN;

- *Secure scalability* so that nodes may securely join the network without impacting the underlying routing scheme.

In general, *preventive* measures eliminate the opportunity for DoS attacks by ensuring that fabricated routing signals cannot not be injected into the network, routing messages may not be maliciously altered, loops may not be formed, and routes cannot

be maliciously redirected. Several other measures are aim at early *attack detection* and robust *recovery mechanisms*. Interestingly, routing attacks in WSNs have also been classified in terms of *routing packet attacks* versus *routing algorithm attacks* itself. Routing packet attacks such as selective packet dropping, spoofing, altering or replaying routing information targets route information exchanged between nodes in order to create loops, attract or repel network traffic, extend or shorten routes, generate false error messages, increase end-to-end latency, waste network resources or create a denial of service (DoS). Altering and spoofing routing packets requires insider participation, while the replay attack can be easily achieved by an outsider. In the following sections, we describe opportunities for, and counter measures to possible security breaches to SIRLoS.

1. Per Hop Authentication and Routing Beacons Alteration

The problem of per hop authentication requires that the base station should be able to authenticate the participation of every node claimed in each BS-circuit. The rolling nonce along with individual node's signatures with their passwords and individual keys, provides per node authentication while preventing the malicious alteration of the CDB. In essence, the one-time nonce (different for each entry cluster head) is cumulatively signed by every node which encounters it. This distinguishing node-dependence feature strengthens the cryptographic property of our algorithm, somewhat similar in notion to the data-dependent structure that is the mainstay of the RC5 encryption algorithm. SIRLoS exploits this dependence on descendants, and link directionality to enhance security (i.e., the CDB will more likely encounter the base station before it returns to a given node a second time).

Since each node updates a unique nonce with its password, the cumulative value depends on several unknown entries. Consequently, it is impossible for a subverted in-

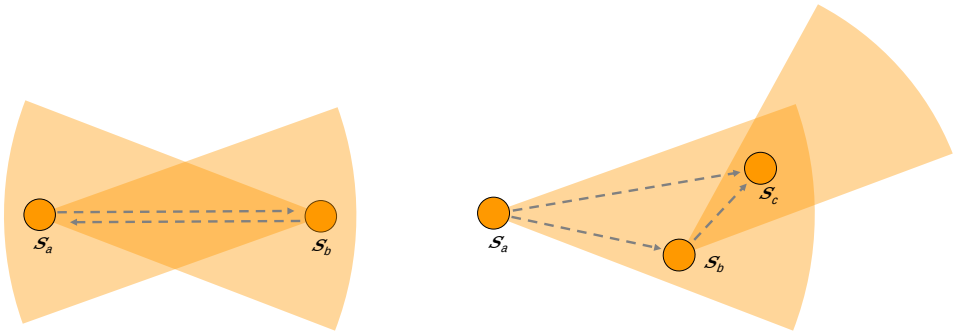
sider node who encounters a CDB to successfully alter routing information. Consider for example, two possible cases:

- A malicious node hopes to disrupt routing by deleting the data entry of prior nodes from the CDB's payload, and reducing the HT value appropriately. In this case, it is non-trivial to modify the accumulated nonce value in a way to extract the passwords of the nodes the attacker hopes to annihilate from the link, since he cannot decipher a previous node's password or the original nonce from the BS. Hence the final nonce will not verify at the base station, resulting in the discarding of the CDB.

- A malicious node hopes to forge a non existent route by making false node information entries into the CDB's payload. In this case, he is unable to correctly update the nonce or sign the MAC signatures of false entries as the passwords and individual keys of uncompromised nodes are unknown to it.

a. Problem Case I

In the two attacks enumerated above, an attacker χ_A say, may succeed in fooling its *descendants* (nodes along its uplinks) into making erroneous entries into their PRTs. This is because a CDB does not get verified until it is returned to the base station, prior to which nodes have already made entries that might be inaccurate into their PRTs. However, this falsehood is detected by the base station when the CDB reaches it, and is detected by the descendant nodes after they receive updated PRTs, secured with their individual keys from the base station. Each node compares the PRT received from the base station with the one it recorded during neighborhood discovery. An aggressive response assumes any inconsistency in PRT entries is due to a malicious attack. Such entries are deleted from the PRT, and reported to the base



(a) Bi-directional link (b) Three node insider link

Fig. 32. Depicting the two scenarios in which a vulnerability exists in the security of the neighborhood discovery scheme.

station thereby serving to initiate intrusion detection on the given BS-circuit.

b. Problem Case II

There are two scenarios under which a vulnerability exists in the security of SIRLoS' neighborhood discovery scheme as follows:

1. A bidirectional link $s_a \leftrightarrows s_b$ say as depicted in Figure 32(a), occurs.

2. A three node insider link occurs such that say, $s_a \leftrightarrows s_b$, $s_a \leftrightarrows s_c$, and $s_b \leftrightarrows s_c$ as depicted in Figure 32(b).

For the first scenario in which a bi-directional link occurs, the first node, say s_a, who receives the CDB would be able to decipher the successor s_b's secret password by storing the updated cumulative nonce $\eta_t^* \oplus PW_a$ when he first sees the CDB it at time step t, and then XORing it with the updated nonce $\eta_{t+2}^* = \eta_t^* \oplus PW_a \oplus PW_b$ it receives from s_b via the bidirectional link at time step $t+2$, when the CDB returns to it. That is, $PW_b = \eta_t^* \oplus PW_a \oplus \eta_t^* \oplus PW_a \oplus PW_b$. This problem case which occurs in part due to our choice of employing the simple bitwise $\oplus$ operation for updating the nonce,

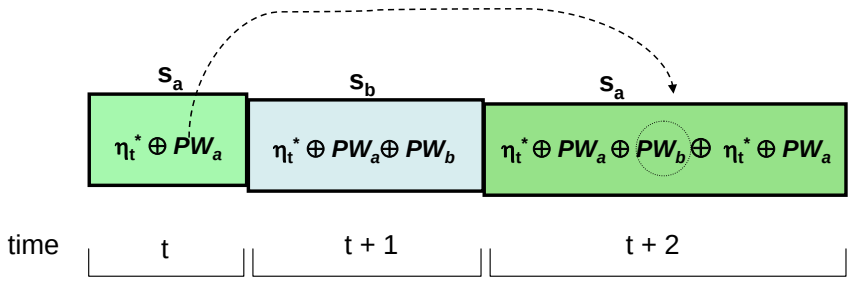


Fig. 33. Illustrating the bidirectionality vulnerability problem scenario.

is illustrated in Figure 33. To address this "bidirectionality vulnerability", we again leverage the security benefits due to directionality, by proving that the probability that this problem case occurs decreases as $\alpha \to 0$.

Let us consider the probability $(1 - \Pr[0 \leftrightarrows])$ that any given node s_a has at least one bidirectional link with a successor (i.e., 1 minus probability $\Pr[0 \leftrightarrows]$ that the node has no bidirectional link), and let Z_a be the random variable (r.v.) counting the number of s_a's successors. Recall that we previously defined p_a as the probability that a malicious node χ_A may compromise any authentic network node. We would like to determine the probability $p_{\chi_A}(> 0 \leftrightarrows)$ that a malicious node χ_A may compromises s_a which has at least one bidirectional link, as follows:

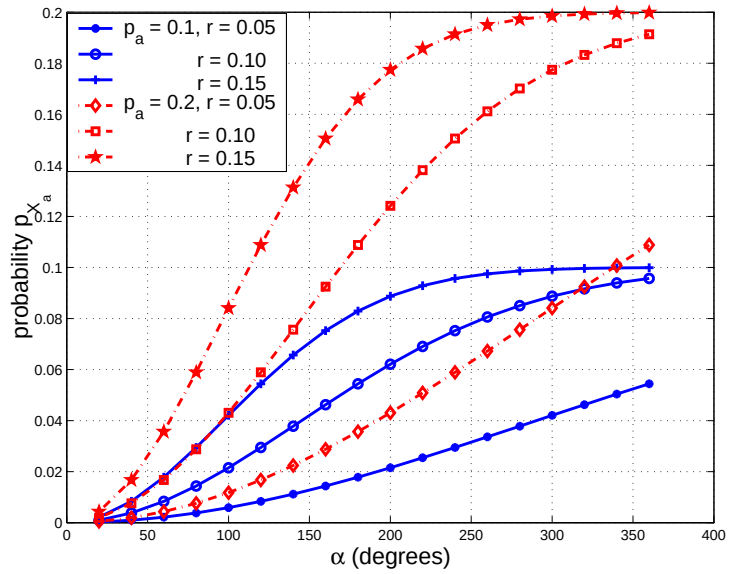
$$\begin{aligned}
p_{\chi_A}(> 0 \leftrightarrows) &= p_a \sum_{z=0}^{n-1} (1 - \Pr[0 \leftrightarrows | Z_a = z]) \times \Pr[Z_a = z] \\
&= p_a \sum_{z=0}^{n-1} \left(1 - (1 - \frac{\alpha}{2\pi})^z\right) \frac{e^{\frac{-n\alpha r^2}{2}} \left(\frac{n\alpha r^2}{2}\right)^z}{z!} \\
&= p_a \left(1 - e^{\frac{-n\alpha r^2}{2}} \sum_{z=0}^{n-1} \frac{\left(\frac{n\alpha r^2}{2}(1 - \frac{\alpha}{2\pi})\right)^z}{z!}\right) \\
&= p_a \left(1 - e^{\frac{-n\alpha r^2}{2}} e^{\frac{n\alpha r^2}{2}(1-\frac{\alpha}{2\pi})}\right) \qquad \text{for} \quad n \to \infty \\
&= p_a \left(1 - e^{\frac{-n\alpha^2 r^2}{4\pi}}\right) \qquad (4.3)
\end{aligned}$$

where as previously discussed in Chapter III, it is known that Z_a follows a Poisson distribution of parameter $n\alpha r^2/2$, with $\alpha r^2/2$ as Φ_a's area.

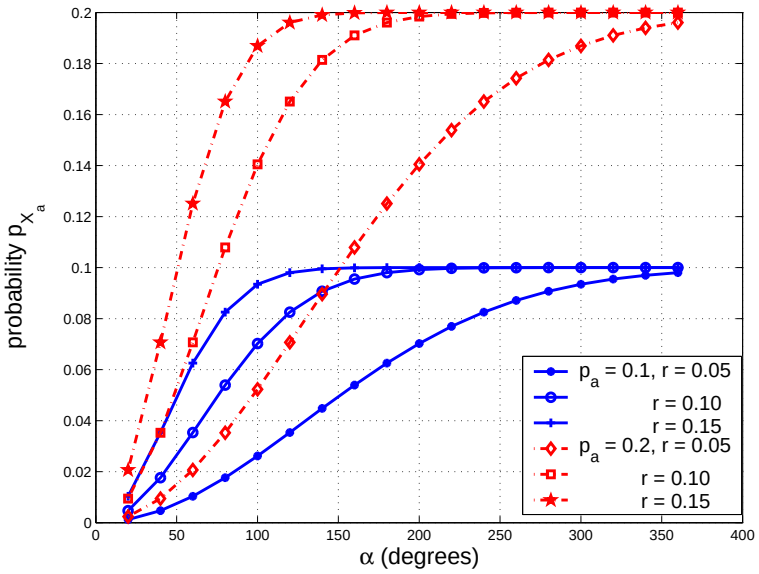
We observe from Equation 4.3 that as $\alpha \to 0$, then $p_{\chi_A}(> 0 \leftrightarrows) \to 0$. However as $\alpha \to 2\pi$ which represents the RGG model [19], we see that $p_{\chi_A}(> 0 \leftrightarrows) \to p_a(1-e^{-nr^2})$. In this case, it is obvious that directionality does not exist and therefore is no longer be exploited for any security gain as $p_{\chi_A}(> 0 \leftrightarrows)$ rapidly approaches p_a. In Figure 34 (a) and (b), we illustrate the relationship between α and $p_{\chi_A}(> 0 \leftrightarrows)$ for various r and p_a values with n set to 100 and 500 respectively. This graph reflects the relationship between α and the probability that any given node will have at least one bidirectional link.

As expected, the probability that any given node will have a bidirectional link goes to one as $\alpha \to 2\pi$, so that $p_{\chi_A}(> 0 \leftrightarrows)$ is upper bounded by p_a. It is interesting to note the trade off between an increase in r and an increase in p_a as $n \to \infty$. For example, for $n = 500$ with $\alpha \approx 140^o$ yields the same $p_{\chi_A}(> 0 \leftrightarrows)$ for parameter pair values $(p_a = 0.1, r = 0.10)$ as for $(p_a = 0.2, r = 0.05)$, while for $\alpha = 150^o$ the $p_{\chi_A}(> 0 \leftrightarrows)$ is the same for parameter pair values $(p_a = 0.1, r = 0.15)$ as for $(p_a = 0.2, r = 0.05)$. Corresponding values of α for similar conditions with $n = 100$ are 320^o and 340^o.

We further observe that, even if χ_A successfully deciphers PW_b, without knowledge of K_b, it can only succeed in dropping s_b's entry from the CDB, which may be acceptable as $s_a \leftrightarrows s_b$ represents an unwanted loop. Without the additional knowledge of s_b's individual key K_b for signing the MAC, an attacker cannot masquerade as the other node, nor can he compromise data confidentiality.



(a) n = 100



(b) n = 500

Fig. 34. Probability $p_{\chi_A}(> 0 \leftrightarrows)$ versus α for various r and p_a values.

As $\alpha \rightarrow 2\pi$, the network tends to the traditional omnidirectional model, and directionality may no longer be exploited in the security primitives. This becomes more of the case in which most links are bidirectional with only a small fraction of directional links, for which several secure routing schemes have been proposed. An interesting problem involves analyzing the critical value of α at which this transition occurs for various parameter values. For example, as observed in Figure 34 (b), for $r = 0.15$ the critical α is 140^o, while it is 200^o for $r = 0.10$. This critical α value provides a transition point at which previously proposed omnidirectional based routing schemes are preferred over circuit-based directional routing for WOSNs. That is, for example, with r set to 0.15, if $\alpha < 140^o$, then SIRLoS may be leveraged, otherwise, if $\alpha > 140^o$, a smarter approach is to consider traditional omni-directional routing schemes which have been modified to accommodate a limited number of directional links.

In the three-node insider link scenario, the final node on the link, s_c can decipher the insider node s_b's secret password as it (as well as s_b) would receive a CDB from s_a at time step t, while at time step $t + 1$, it would receive the same CDB from s_b with its nonce value now updated by PW_b. That is, s_c can easily decipher $PW_b = \eta_t^* \oplus \eta_{t+1}^* = \eta_t^* \oplus \eta_t^* \oplus PW_b$. To analyze this scenario, we evaluate the probability that a three-node insider link occurs as follows:

- Case 1: When $\alpha \leq \pi/3$ the three-node insider link vulnerability reduces to a case similar to the bi-directional link vulnerability, since we observe that the probability $\Pr[s_b \rightarrow s_c | s_a \rightarrow s_b]$ that $s_b \rightarrow s_c$ exists, given that $s_a \rightarrow s_b$ exists is $\alpha/2\pi$. This is true because at $\alpha = \pi/3$ the largest inscribed triangle within Φ_a is an equilateral triangle with side length r. This implies that the length of the longest chord the lies within Φ_a is r, so that $d(\Upsilon_b, \Upsilon_c) \leq r$ and

$\Pr[s_b \rightarrow s_c] = \alpha/2\pi$. If we denote as Z_a be the random variable (r.v.) counting the number of s_a's successors, the probability that s_c may be covered by at least one of the nodes in Φ_a, and s_c may be compromised by a malicious node χ_A is given as:

$$\begin{aligned}
p_{\chi_A}(>0 \twoheadrightarrow) &= p_a \sum_{z=1}^{n-2}(1 - \Pr[0 \twoheadrightarrow | Z_a = z]) \times \Pr[Z_a = z] \\
&= p_a \sum_{z=1}^{n-2} \left(1 - (1 - \frac{\alpha}{2\pi})^{z-1}\right) \frac{e^{\frac{-n\alpha r^2}{2}} \left(\frac{n\alpha r^2}{2}\right)^z}{z!} \qquad \text{for} \quad z > 1 \\
&= p_a \left(1 - \frac{e^{\frac{-n\alpha r^2}{2}}}{1 - \frac{\alpha}{2\pi}} \sum_{z=1}^{n-2} \frac{\left(\frac{n\alpha r^2}{2}(1 - \frac{\alpha}{2\pi})\right)^z}{z!}\right) \\
&= p_a \left(1 - \frac{e^{\frac{-n\alpha r^2}{2}}}{1 - \frac{\alpha}{2\pi}} \left[e^{\frac{n\alpha r^2}{2}(1 - \frac{\alpha}{2\pi})} - 1\right]\right) \qquad \text{for} \quad n \rightarrow \infty \\
&= p_a \left(1 - \frac{e^{\frac{-n\alpha^2 r^2}{4\pi}} + e^{\frac{n\alpha r^2}{2}}}{1 - \frac{\alpha}{2\pi}}\right) \qquad (4.4)
\end{aligned}$$

- Case 2: When $\alpha > \pi/3$ the probability $\Pr[s_b \rightarrow s_c | s_a \rightarrow s_b]$ that $s_b \rightarrow s_c$ exists, given that $s_a \rightarrow s_b$ exists is obtained as the product of the probability that two nodes in Φ_a are within a distance r, given as $r^2/2\,(\alpha - \pi/3)$, and the probability that given the former condition, $\Upsilon_b \in \Phi_c$ given as $\alpha/2\pi$. By the same arguments employed in Equation 4.4, we derive $p_{\chi_A}(>0 \twoheadrightarrow)$ as follows:

$$\begin{aligned}
p_{\chi_A}(>0 \twoheadrightarrow) &= p_a \sum_{z=1}^{n-2} \left(1 - (1 - \frac{\alpha r^2}{4\pi}(\alpha - \frac{\pi}{3}))^{z-1}\right) \frac{e^{\frac{-n\alpha r^2}{2}} \left(\frac{n\alpha r^2}{2}\right)^z}{z!} \qquad \text{for} \quad z > 1 \\
&= p_a \left(1 - \frac{e^{\frac{-n\alpha r^2}{2}}}{1 - \frac{\alpha r^2(3\alpha - \pi)}{12\pi}} \sum_{z=1}^{n-1} \frac{\left(\frac{n\alpha r^2}{2}(1 - \frac{\alpha r^2(3\alpha - \pi)}{12\pi})\right)^z}{z!}\right) \\
&= p_a \left(1 - \frac{e^{\frac{-n\alpha r^2}{2}}}{1 - \frac{\alpha r^2(3\alpha - \pi)}{12\pi}} \left[e^{\frac{n\alpha r^2}{2}(1 - \frac{\alpha r^2(3\alpha - \pi)}{12\pi})} - 1\right]\right) \qquad \text{for} \quad n \rightarrow \infty
\end{aligned}$$

By a similar analysis for the bidirectional vulnerability case, we observe that the threat due to both the bidirectional and three-node insider vulnerability is enhanced as α increases, and solutions to mitigate this problem must be further explored. One possibility is for the base station to periodically and randomly update the passwords of nodes after the neighborhood discovery phase. The success of this scheme is based on the assumption that in the early period after deployment, the probability that malicious nodes have been deployed to compromise authentic network nodes tends to zero. These password updates may be done along with the unicasting of individual node's routing table for uplink updates in the final phase of SIRLoS.

2. Broadcast Authentication and Spoofed Routing Beacons

The goal of broadcast authentication is to ensure that only the base station can initiate neighborhood discovery. The secure challenge-and-respond protocol employing individual keys and passwords of cluster heads prevents alien nodes from initiating, spoofing or fabricating any route discovery communication with the network. The one-way key chain provides broadcast authentication, as only the base station knows future keys used to authenticate routing signals, so that no other entity can reveal this key to a cluster head.

Traditionally, for omnidirectional networks, a malicious (insider or outsider) node attempting to initiate routing beacons for network discovery aims to fool nodes into believing he is the base station. If successful, he can gain control of the network as nodes route their data back to him by the principle of reverse path routing. Due to the non reversibility of routes, this spoofing attack does not directly apply for WOSNs. That is, nodes in a WOSN do not route data back in the direction from which they first received the routing beacon, but forward it along the directed path until it inadvertently reaches an exit cluster head.

Rather, an equivalent attack for CDB spoofing involves a malicious node attempting to establish communication with exit cluster heads, so that routing beacons end up with it. As previously stated, the challenge-and-respond protocol mitigates against this attack, i.e., cluster heads do not communicate with unauthenticated partners. Also, this attack is mute due to the fact that cluster heads do not necessarily advertise their role in order to attract traffic, (i.e., nodes do not advertently forward data to a cluster head). In the WOSN, a node choosing to be a cluster head does not attract any more traffic to itself than it would normally receive.

Note that a future key, once revealed in the CDB by the base station appears exposed. An insider attacker who has seen this key may attempt to use this information in a sophisticated attack. However, due to directionality and because all BS-circuits must eventually be validated by the base station, an independent attacker does not benefit from this knowledge.

3. Beacon Freshness and Correlation-based Cryptanalysis

We may employ a time stamp leash on each CDB to bound the BS-circuit discovery process. The base station allows sufficient time less than the maximum delay t_{max} within which all CBDs must either return to it or expire. Any CDB which returns after t_{max} (i.e., has been out too long) is suspected of malicious activity, and thus discarded. This step is important as it is conceivable that given sufficient time, a malicious node may succeed in cracking the security of the scheme. Consider for example, the case where an attacker wants to alter the CDB, make the route appear shorter, and confuse the routing function by removing information input sections of some of its ancestors from the payload. Given enough time, the attacker can employ sophisticated measures including for example, colluding with other nodes to sniff the nonce values at various stages of different BS-circuits. Cryptanalysis on these nonce

may reveal the passwords of various nodes, depending on the correlation between the nodes in the different BS-circuits sniffed. Note that the use of entry cluster head-dependent nonce greatly strengthens our scheme against such correlation-based cryptanalysis.

The freshness of the CDBs is assured with the use of a fresh nonce and a new future key (i.e., the next key in the key chain) for each era that dynamic route discovery or neighborhood re-discovery is initiated, required for example in case of topology changes in the network. Suspected malicious nodes are isolated by excluding them from network re-keying. That is, the base station sends an updated K_N to only the unsuspected network participants. Note that time synchronization and storing/queuing of routing beacons is not required for our protocol.

4. Unauthorized Alien Node Participation and Traffic Analysis

The cryptographic primitives employed in SIRLoS provides confidentiality and ensures that unauthorized alien nodes cannot participate in route establishment. Aliens do not possess K_N and hence cannot decrypt or update routing signals. Encrypting the CDBs also mitigates against attacks based on traffic analysis. It is noteworthy that passively observing the geographic direction of routed packets from a single vantage point in a WOSN exposes little about the location of the base station or cluster head.

E. Attack Analysis

In this section, we discuss routing attacks [11] in the context of WOSNs for SIRLoS, and particularly focus on a novel attack aimed at circumventing and undermining the security advantage due to path diversity and link directionality in WOSNs, as well as

on the wormhole attack.

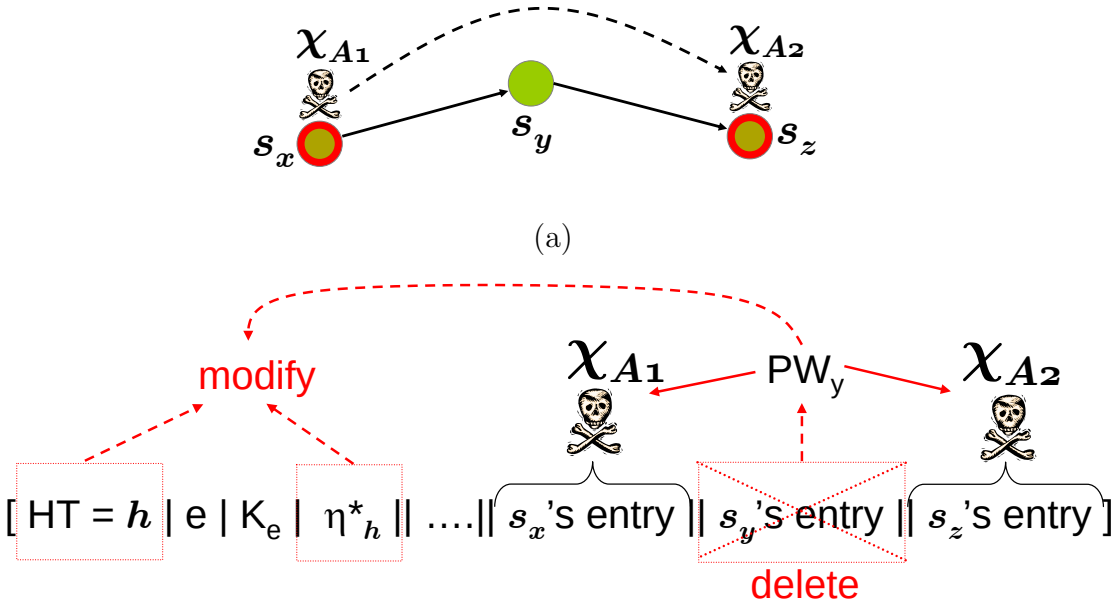


Fig. 35. BS-circuit collusion attack.

1. BS-Circuit Collusion Attack

We introduce a novel attack for the WOSN termed the *BS-circuit collusion attack* in which insider nodes collude to place themselves both at the downlink and uplink of a target node s_y, thereby breaking the authenticity of the represented BS-circuit, as depicted in Figure 35 (a). The motivation for this wormhole-type [77] insider attack is to disrupt routing by deciphering PW_y, as similarly described in problem case II, and then successfully dropping s_y's entry from any CDB, as illustrated in Figure 35 (b). For tractability, we only consider here the case with two colluding invaders χ_{A1} and χ_{A2} attempting a 2-hop attack targeting s_x and s_z, both 1-hop from/to node s_y, respectively, with the aim to decipher PW_y. We state the collusion attacker's

problem by asking: Given that χ_{A1} has successfully invaded s_y's predecessor s_x, what is χ_{A2}'s probability p_{ca} of invading a second node s_z that is one of s_y'successors?

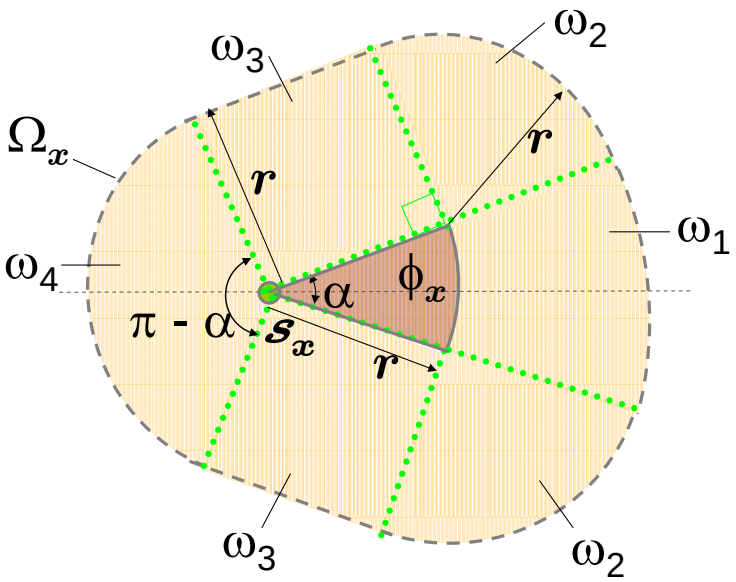
We determine the search region Ω_x where χ_{A2} attempts an invasion to be the *locus* of points at a fixed distance r from Φ_x, delineated by the dotted line around the shaded region in Figures 36 (a) and (b) for $\alpha < \pi$ and $\alpha \geq \pi$ respectively. The probability p_{ca} of χ_{A2} invading node $s_z \in \Phi_y$ given $s_y \in \Phi_x$ is:

$$\begin{aligned} p_{ca} &= p_a \sum_{z=0}^{n-1} (1 - \Pr[s_z \notin \Phi_y | s_z \in \Omega_x \mid Z_y = z]).\Pr[Z_y = z] \\ &= p_a \sum_{z=0}^{n-1} \left(1 - (1 - \frac{A(\Phi_y)}{A(\Omega_x)})^z\right) \frac{e^{\frac{-n\alpha r^2}{2}} \left(\frac{n\alpha r^2}{2}\right)^z}{z!} \\ &= p_a \left(1 - e^{-\frac{n\alpha r^2 A(\Phi_y)}{2A(\Omega_x)}}\right) \quad \text{for} \quad n \to \infty, \end{aligned} \tag{4.5}$$

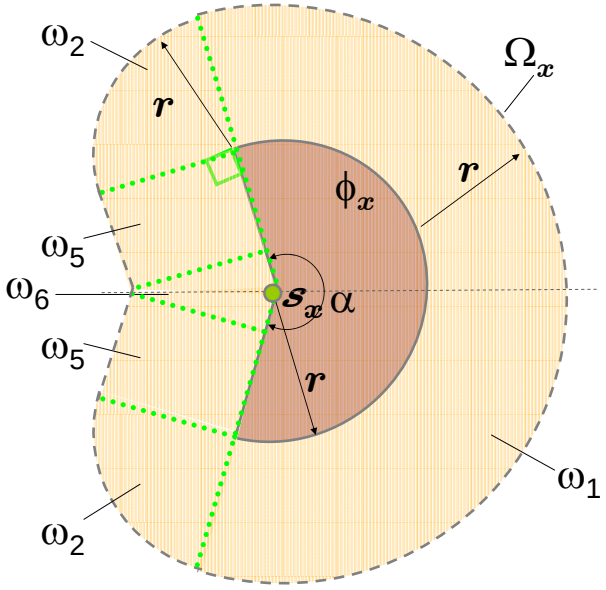
where $A(\lambda)$ is the area of λ. Simplifying steps in Equation 4.5 follow similar steps in Equation 4.3 and $A(\Omega_k)$ is obtained as:

$$\begin{aligned} A(\Omega_k) &= \sum_{i \in \Omega_x} A(\omega_i) \\ &= r^2 \left[2 + \alpha + \pi\right] \qquad \text{for} \quad \alpha < \pi \qquad (4.6) \\ &= r^2 \left[4 + 3\alpha + \pi - \frac{2}{\tan\left(\frac{2\pi - \alpha}{2}\right)}\right] \quad \text{for} \quad \alpha \geq \pi \qquad (4.7) \end{aligned}$$

which is derived as the sum of the (lightly shaded) areas of the six regular-shaped partitions of the composite shape Ω_x as depicted in Figure 36.



(a) $\alpha < \pi$



(b) $\alpha \geq \pi$

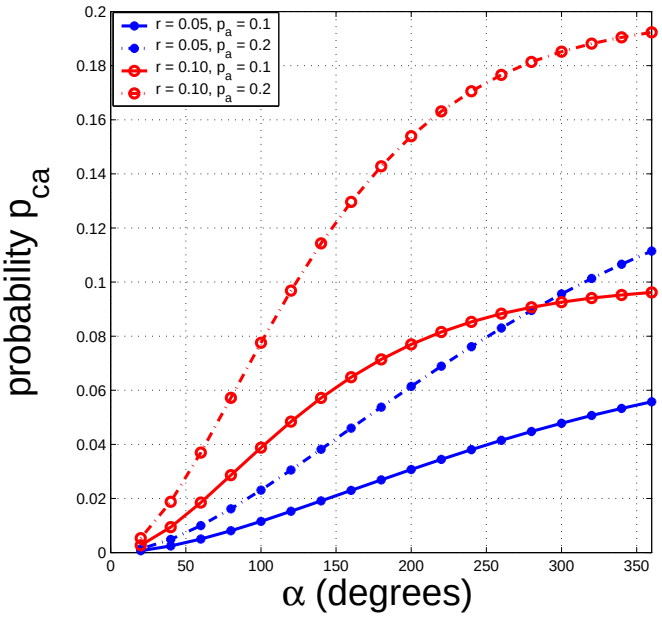
Fig. 36. Depicting the region of possibility where s_x's successor falls.

We have determined the areas of the partitions of Ω_x shown in Figure 36 as:

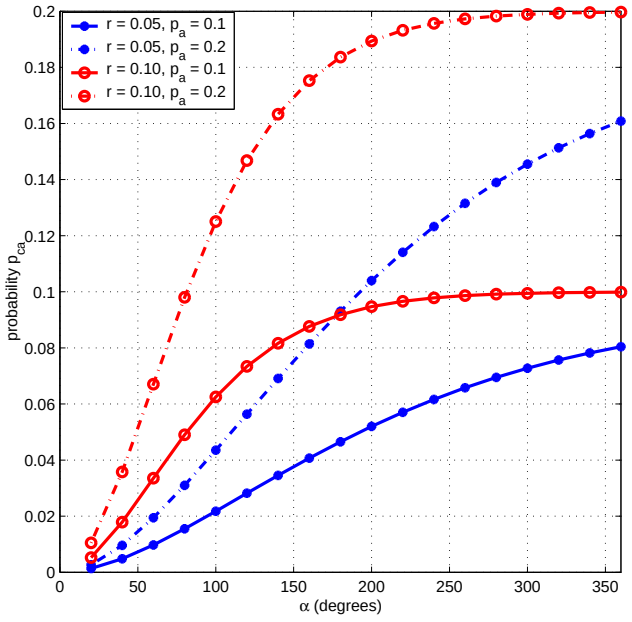
$$\begin{aligned}
A(\omega_1) &= \frac{\alpha(2r)^2}{2} - \frac{\alpha r^2}{2} = \frac{3\alpha r^2}{2} \\
A(\omega_2) &= \frac{\pi r^2}{4} \\
A(\omega_3) &= r^2 \\
A(\omega_4) &= \frac{(\pi - \alpha) r^2}{2} \\
A(\omega_5) &= r^2 \left[1 - \frac{1}{\tan\left(\frac{2\pi - \alpha}{2}\right)} \right] \\
A(\omega_6) &= \frac{r^2}{\tan\left(\frac{2\pi - \alpha}{2}\right)}
\end{aligned}$$

so that, for $\alpha < \pi$, $A(\Omega_k) = A(\omega_1) + 2A(\omega_2) + 2A(\omega_3) + A(\omega_4)$, and for $\alpha \geq \pi$, $A(\Omega_k) = A(\omega_1) + 2A(\omega_2) + 2A(\omega_5) + A(\omega_6)$, where simplifying easily yields the results of Equations 4.6 and 4.7 respectively.

In Figure 37 we show graphs of p_{ca} versus α (from Equation 4.5) for $r = 0.05,\ 0.1$, and $p_a = 0.1,\ 0.2$ with $n = 500$ and 1000. In essence, the graph describes the vulnerability of an individual node to collusion attack with α going from 0 for WOSNs to 2π for the omni-directional network. It is clear that the probability p_{ca} of successfully launching a BS-circuit collision attack increases with the increase in n, r, and α. Furthermore, we also observe that a linear increase in r produces a more significant impact on p_{ca} compared with a corresponding increase in either n or α further verifying r as a highly sensitive parameter for security. For example, in Figure 37 (a), for a given α, say 100^o, with $p_a = 0.1$, we observe that $p_{ca} = 0.012$ for $r = 0.1$. Doubling r to 0.2 results in almost a quadrupling of p_{ca} to 0.04. However doubling α to 200^o yields $p_{ca} = 0.032$ which is less than what is achieved by doubling r. Doubling n from 500 to 1000 for the same parameter values, say $\alpha = 100^o$, $r = 0.1$, $p_a = 0.1$ results in p_{ca} merely increasing from 0.04 to 0.061 as shown in Figures 37 (a) and (b).



(a) $n = 500$



(b) $n = 1000$.

Fig. 37. Illustrating the vulnerability to collusion attack with p_{ca} versus α.

In summary, we note that r is a high sensitivity parameter which directly impacts connectivity while it has an inverse relationship to the security of the WOSN with regards to its vulnerability to the impact of BS-circuit collusion attacks and other similar attacks. We have also characterized the relationship that demonstrates the benefit of directionality for security in WOSNs, as the probability and impact of a successful BS-circuit collision attack diminishes as α is reduced, as expected. That is, directionality provides clear advantages for security in ad hoc neioghborhood discovery and routing for WOSNs.

2. Wormhole Attack

A particularly devastating outsider attack, the *wormhole attack*, was introduced in [88], and has been widely studied for omnidirectional sensor networks [11, 90]. The aim of this attack is to disrupt neighborhood discovery and routing in the network. Conventionally, the attacker establishes a low metric route between two locations W_1 and W_2 say, in the network through which he tunnels packets recorded at one end W_1 say, of the wormhole to the other end W_2 where he replays them in a timely manner. Recently, two models of the wormhole attack for directional sensor networks have been identified [91], namely the long range and the short range wormholes.

A wormhole is a powerful attack that disrupts neighborhood discovery and routing in the network by establishing a low-metric link between two network locations. The attacker records beacons at one end of the link (typically closer to the base station), tunnels them via the wormhole to a colluding node who *replays* the beacon in a timely manner at the other link's end. The tunnel may be established in several ways, such as a low latency out-of-band channel (e.g., wired link) or high powered wireless transmission. A tunneled beacon arrives with a much better routing metric (e.g., faster or lower hop count) than it would if it had followed the normal multi hop

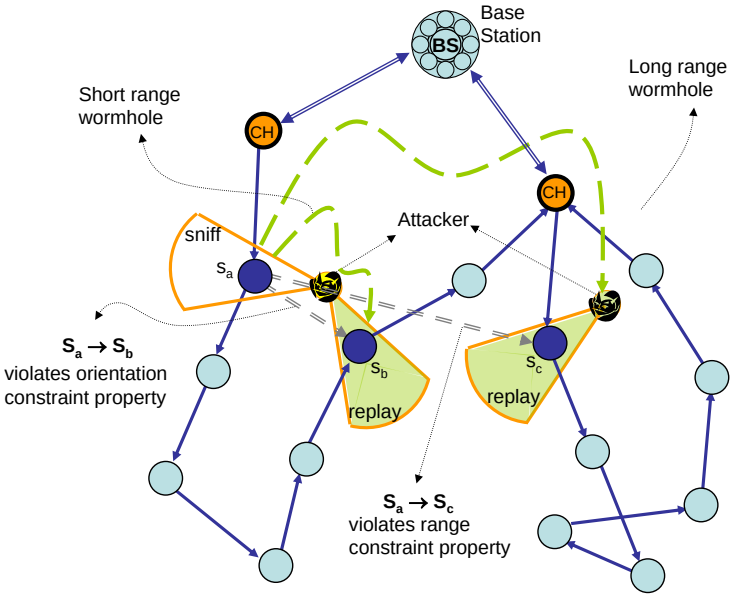


Fig. 38. Illustrating a short range and long range wormhole attack in a WOSN, which violates geometric connectivity using the range-and-orientation constraint test.

route, thereby fooling nodes in the neighborhood of the tunneled packet by creating an illusion that they have a direct (one-hop) route via the wormhole, to nodes in the neighborhood from which the packet was tunneled.

The nature of this attack makes it particularly debilitating because it may be effectively deployed as an outsider attack, even if the network provides confidentiality, integrity and broadcast/per hop authentication based on cryptographic primitives. Once the wormhole is established, the attacker then follows up with other malicious acts such as a sinkhole (selectively dropping packets), modifying and forwarding packets, or denial of service attacks. When launched prior to topology discovery, wormholes falsify the network's connectivity graph and thereby introduce erroneous or nonexistent routes that can be very difficult to recover from.

In a WOSN, a wormhole can violate either the range or the orientation constraint with either a long range wormhole of tunnel distance much greater than r, or a short

range wormhole in which packets from the original sector are replayed in a different sector within the same disc (see Figure 38 for illustration). The short range wormhole does not require specialized hardware for low latency or high powered transmissions by the attacker.

(a) Long Range Wormhole Attack: For tunnel distances much longer than r, the CDB arrives with a lower HT value than if it followed the normal route, thereby fooling nodes that receive P_W into believing they have a one-hop route (via the wormhole) to nodes in the neighborhood from which P_W was tunneled. Each node s_a performs the *range constraint test* to detect this attack as follows:

$$\text{if} \;\; d(\Upsilon_a^{est}, \Upsilon_q^{est}) > r \quad \forall s_q \in \mathcal{S}_a \quad \Rightarrow \quad \text{attack present} \tag{4.8}$$

(b) Short Range Wormhole Attack: For tunnel distances $\leq r$ the CDB arrives at W_2 with an orientation value Θ_b of the predecessor s_b that differs by more than $\alpha/2$ from the accurate orientation. To detect this attack each node s_a performs the *orientation constraint test* as follows:

$$\text{if} \;\; \Theta_a - \Psi_{ab}^T \geq \frac{\alpha}{2} \geq \Theta_a + \Psi_{ab}^T \quad \forall s_a \in \mathcal{S}_a \quad \Rightarrow \quad \text{attack absent} \tag{4.9}$$

where $\Psi_{ab}^T = \min\left[|\Theta_a - \Psi_{ab}|, |\Theta_a + 2\pi - \Psi_{ab}|, |\Theta_a - 2\pi - \Psi_{ab}|\right]$ represents the angular difference between the direction of s_b and the position of s_a, with $\Psi_{ab} = \arccos d(y_a, y_b)/\Delta_{ab}$.

For both models, the location and orientation information included in the CDB enables the ROC test in SIRLoS, and serves to mitigate this attack. That is, a wormhole is detected if this geometric connectivity test fails, similar to the method proposed in [77]. It is conceivable that a desperate attacker may attempt to modify the location or orientation information of a predecessor's entry to corroborate its

wormhole attack, as this information is in the clear. However, the base station with its global view of the network topology and connectivity, is able to detect this attack since the MAC containing the authentic location and orientation entry will fail to verify. In this dissertation, we have not considered the effects that localization error will have on the accuracy of detection for the wormhole attacks, but have included it for future work.

The conventional wormhole attack exploits the structure of reverse path routing in which link bi-directionality and reverse path routing are assumed, and the uplink and downlink paths are symmetric involving the same nodes. This does not hold for the WOSN, thereby invalidating its effect; specifically, because a downlink path of SIRLoS is different than its uplink path, a wormhole has limited effect in suggesting an attractive reverse route.

3. Other Common Routing Attacks

In this section, we consider common routing attacks in the WOSN scenario; similar routing attack analysis for traditional RF sensor networks have been performed in [43], [56], and [57]. We analyze the following well-known types of DoS attacks that affect SIRLoS, which we argue are the most significant for routing in sensor networks because of their inherent nature to disrupt information flow in cooperative networks. The development of additional attacks targeting the directional framework is a topic of ongoing research.

a. Type I: Sinkhole Attacks

A sinkhole involves a malicious node striving to illegally attract traffic through itself by giving other nodes the impression that a high quality route exists through it to the base station. Once this is accomplished, the corrupt node can then launch selective

forwarding, spoofing, packet altering, or eavesdropping. Two well known sinkhole attack include the wormhole attack previously discussed, and the sybil attack.

- Sybil Attacks: In keeping with its namesake, the popular 1970s book Sybil on multiple personality disorder, in a Sybil attack [44] a single node presents multiple (false) identities for the purpose of confusing the routing scheme and leading to a possible sinkhole. A parallel attack involves identity fabrication or theft. In SIRLoS, a malicious node may not fabricate or steal any other identity different from its own since the protocol requires each node to sign a MAC of its appended identity using its individual key shared with the base station. Furthermore, XORing its password (known only to itself and the base station) with the cumulative nonce propagating along the BS-circuit adds another degree of source authentication.

b. Type II: Blackhole Attacks

A blackhole entails a malicious node illegally attracting traffic to a nonexistent route so that packets attempting to traverse such hops are not received by any node and are therefore dropped. We discuss three mechanisms a malicious node may employ to launch a blackhole attack.

- HELLO Flood Attacks: In this attack, malicious nodes broadcast high-powered long range HELLO packets to deceptively announce themselves as neighbors to a much larger coverage area than can be attained using the required maximum communication range of a standard network node. Assuming the opponents to be neighbors, legitimate nodes will attempt to route data to the base station. In reverse path routing, this involves legitimate nodes routing data to the base station via the out-of-range opponents leading to "in air" packet dropping. In SIRLoS, application of this attack will not have a relevant effect since routing is conducted through successor nodes that provide an uplink path to the base station. The opponent will be considered

a predecessor neighbor who is part of the downlink path not used by the legitimate node for routing.

- Identity Replication Attacks: Identity replication, in which the same identity is used many times in multiple locations, can be performed and defended against by the SIRLoS protocol. By centrally registering each nodes identity and location, the base station easily detects that the same identity exists in multiple locations. Another feasible approach is for the base station to centrally count the number of connections of each node using the networks adjacency matrix, and revoke those with more connections than an allowable maximum.

- Location Misrepresentation Attacks: Another possible attack by a malicious node involves misrepresenting its location information to fool the routing and localization protocol by causing its neighbors to route data away from legitimately receiving nodes thereby wasting resources. Such an attack in the WOSN scenario is easily identifiable by the base station, as the network topology is available to validate a nodes location. Moreover, such an attack has negative implications that are emergent from the structure of SIRLoS. In particular, since the uplink and downlink paths of a node are distinct, the malicious node cannot be selective and stealthy in which neighbors it misrepresents its position to. Such an attack effectively cuts the malicious node off from participating in network protocols since its predecessors will assume the incorrect orientation of its laser towards the node, obtained from its SRT. SIRLoS' route maintenance mechanism detects this link as broken and reroutes data via other links.

c. Type III: Other Denial of Service Attacks

- Neglect and greed: In this attack, the malicious node neglects to route some or all messages passed to it. The subverted or malicious node can still participate in lower level protocols such as route maintenance but drops messages on a random or arbitrary

basis or may give undue priority to its own messages. Packet acknowledgments are normally employed to ensure data are appropriately received in unreliable networks. Such paradigms are also useful for identifying this attack in WOSNs. However, if a node is stealthy, it may pass so-called acknowledgments to a node whose signals it has not passed, appeasing it. For unidirectional networks, the success of such an attack is limited because the malicious node cannot exist in both the uplink and downlink paths of a legitimate node; this additional level of diversity in multi-hop routing makes it possible for a malicious node to either control data flow but not acknowledgments, or vice versa, alerting intrusion detection mechanisms.

- Homing attack: Based on traffic analysis, an attacker sniffs packet headers in order to decipher where they come from and where they are going. For the WOSN scenario, such an attack may aim to determine the global network topology by observing routed packets and use such information to launch more harmful attacks. Given the passive nature of eavesdropping, such an attack is not easily detectable. However, in comparison to omnidirectional RF networks where communication is broadcast-based, FSO beams are physically more inaccessible, requiring that an attacker distribute itself and providing a higher level of effort, possibly deterring such opponent activity.

- Misdirection attacks: These are similar to (victim-directed) sinkholes in which the attacker forwards messages along a wrong path with the intention of flooding its victims link. One way to achieve this is for the attacker to forge replies to route-discovery requests, including the victims ID in the spoofed routes. SIRLoS guards against this attack and other route spoofing attacks by requiring that all nodes append their ID along with their MACs (encrypted with their individual keys, using the nonce as freshness). The above analysis gives a flavor of the advantages and novelty that directional communications provides for routing security. The higher overhead

required for directional routing is, in part, offset by its capability to naturally protect against traditional types of routing attacks based on reverse path routing as well as traditional eavesdropping due to the directed nature of the communication beam. In addition, the circuit-based routing anchored at the trusted base station provides additional security. The base station acts as the watchdog for the network, as it possesses the global picture of the network topology, and our proposed solutions leverage redundancy, in part, to mitigate catastrophic network failures, and directionality for security gains.

4. Summary of Insights

In summarizing the insights gained from our overall connectivity and secure neighborhood discovery analysis for directional WOSNs, we observe the following:

1. A linear change in r produces a much more significant direct impact on the connectivity of the network, and an inverse impact on the security of the network (with regards to its vulnerability to the impact of insider attacks), than a corresponding change in either α or n, making r is a high sensitivity parameter.

2. We provide an analytical expression which characterizes the relationship between α and security in WOSNs, and therefore demonstrates the direct benefits of directionality for security in WOSNs.

3. We show through performance evaluation, security and attack analysis and synthesis, the fundamental trade off between security and connectivity in WOSNs. In particular, even though directionality of links yields a sparser network which negatively impacts on connectivity when compared to omnidirectional networks, link directionality proves beneficial to security for neighborhood discovery and routing in WOSNs.

CHAPTER V

CONCLUSION

In this dissertation, we have investigated the feasibility of directional wireless optical sensor networks (WOSNs) for security sensitive broadband applications. In this regard, we consider the following novel contributions.

First, we addressed the requirements on the physical layer network properties of node density, transmission radius and beam width for the free space optics (FSO) signal. We employed a probabilistic approach to analytically determine the relationship between the network properties and the node isolation property for WOSNs and determine its relationship to the probability of network connectivity. We also considered this problem within a fading channel framework with attenuation due to adverse weather and turbulence. This analysis is vital to network engineers striving to determine practical network parameter values in order to achieve a highly connected network with a given confidence level. Our results are also of significance in the light of recent research that has shown that the probability that there is no isolated node provides a tight lower bound to the probability that the network is connected. We showed how this result applies to the WOSNs as $\alpha \rightarrow 2\pi$. Finally, for this aspect, we provided analytical insights on the impact of hierarchy and clustering on connectivity in WOSNs.

Secondly, we have introduced SIRLoS, a lightweight algorithm for integrated secure network discovery and localization for WOSNs, anchored at the base station. SIRLoS exploits link directionality, circuit based routing, and the resources of a trusted base station to construct a global topology visualization of the WOSN at the base station, which acts as a watch dog and authenticator for the network. Our algorithm entails various phases such as the initial hot potato routing, compounded

flooding, base station processing, node routing table updates, dynamic route set up and route maintenance mechanisms. Additionally, we have provided detailed performance evaluations, security analysis, and attack analysis and synthesis to illustrate the various novel features of SIRLoS, including the tangible benefits of directionality to the security of the neighborhood discovery scheme. Through simulation results and analysis, we show that SIRLoS yields enhanced performance, compared to previously proposed route establishment protocols for WOSNs.

A. Future Work

In this section, we identify some ideas that are topics of our ongoing or future research efforts for WOSNs, including:

- Investigating the impact of more than two colluding attackers in the BS-circuit collusion attack. Developing additional novel attacks on the WOSN that target the directional framework. Considering the impact of nodes sending false information to fool the PRT of its successors.

- A more thorough performance evaluation of SIRLoS such as an investigation on the effects that quantization will have on the performance metrics such as localization error, and how propagated localization error will affect the accuracy of wormhole attack detection. Also, a quantitative assessment of routing attacks to measure the robustness and degradation of SIRLoS for this emerging WOSN paradigm.

REFERENCES

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

[2] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for smart dust," in *Proceedings on ACM/IEEE International Conference on Mobile Computing and Networking*, Seattle, WA, August 1999, pp. 271-278.

[3] B. Warneke, M. Last, B. Liewbowitz, and K. Pister, "Smart Dust: Communication with a cubic-millimeter computer," *IEEE Computer,* vol 34, no. 1, 2001, pp. 44–51.

[4] D. Kedar and S. Arnon, "Optical wireless communication in distributed sensor networks," *SPIE Newsroom,* vol. 10, no. 2, 2006, pp. 79–81.

[5] J. Akella, C. Liu, D. Partyka, M. Yuksel, S. Kalyanaraman, and P. Dutta, "Building blocks for mobile free-space-optical networks," in *Proceedings of IFIP/IEEE International Conference on Wireless and Optical Communications Networks (WOCN)*, Dubai, United Arab Emirates, March 2005, pp. 164–168.

[6] C. Davis, I. Smolyaninov and S. Milner, "Flexible optical wireless links and networks," *IEEE Communications Magazine*, vol. 41, no. 3 March 2003, pp. 51–57.

[7] S. Teramoto and T. Ohtsuki, "Optical wireless sensor network system using

corner cube retroreflectors," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, no. 1, 2005, pp. 39–44.

[8] J. Llorca, A. Desai, U. Vishkin, C. Davis, and S. Milner, "Reconfigurable optical wireless sensor networks," in *Proceedings of SPIE Optics in Atmospheric Propagation and Adaptive Systems VI Conference*, J. D. Gonglewski and K. Stein, Eds., Barcelona, Spain, vol. 5237, February 2004, pp. 136-146.

[9] J. Diaz, J. Petit, and M. Serna, "A random graph model for optical networks of sensors," *IEEE Transactions on Mobile Computing*, vol. 2, no. 3, July–September 2003, pp. 186-196.

[10] J. Hill, R. Szewczyk, A. Woo, S. Holler, D. Culler and K. Pister, "System architecture directions for networked sensors," in *Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems*, 2000, pp. 93–104.

[11] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proceedings of IEEE International Workshop on Sensor Network Protocols and Applications*, May 2003, pp 113–127.

[12] S. Yi and P. Naldurg and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001)*, Long Beach, CA, Oct 2001, pp. 299–302.

[13] I. F. Akyildiz, T. Melodia and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Computer Networks Journal*, vol. 52, no. 4, 2007, pp. 921–960.

[14] H. Willebrand and B. Ghuman, "*Free Space Optics: Enabling Optical Connectivity in Todays Networks*," Indianapolis, IN: Sams Publishing, 2002.

[15] U. Ndili Okorafor and D. Kundur, "A secure integrated routing and localization scheme for broadband mission critical networks," in *Proceedings of IEEE Workshop on Mission-Critical Networking, INFOCOM*, Phoenix, Az, April 2008, to appear.

[16] H. Izadpanah, T. ElBatt, V. Kukshya, F. Dolezal and B. Ryu, "High-availability free space optical and RF hybrid wireless networks," *IEEE Wireless Communications*, vol. 10, no. 2, 2003, pp. 45–53.

[17] J. Derenick, C. Thorne, J. Spletzer, "Hybrid Free-space Optics/radio Frequency (FSO/RF) Networks for Mobile Robot Teams," *Multi-Robot Systems: From Swarms to Intelligent Automata*, Alan C. Schultz and Lynne E. Parker (eds.), New York, NY: Springer, 2005.

[18] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, Dec 2004, pp. 6–28.

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

[20] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," *Stochastic Analysis, Control, Optimization and Applications*, Volume in honor of W.H. Fleming, W.M. McEneaney, G. Yin and Q. Zhang (Eds.), Boston, MA, 1998, pp. 547–566.

[21] E. Kranakis, D. Krizanc, and E. Williams, "Directional versus omnidirectional

antennas for energy consumption and k-connectivity of networks of sensors," in *Proceedings of OPODIS*, Teruo Higashino (ed.) vol. 3544, 2004, pp. 357–368.

[22] A. Kashyap and M. Shayman, "Routing and traffic engineering in hybrid RF/FSO networks," in *Proceedings of IEEE International Conference on Communications*, vol. 24, no. 4, 2005, pp. 351-365.

[23] U. Ndili Okorafor and D. Kundur, "On the connectivity of hierarchical directional optical sensor networks, " in *Proceedings of IEEE Wireless Communications and Networking Conference WCNC - Networking*, Hong Kong, March 2007, pp. 3524–3528.

[24] P. Hall, "*Introduction to the Theory of Coverage Processes*," New York, NY: John Wiley & Sons, 1988.

[25] N. Cressie, "*Statistics for Spatial Data*," New York, NY: John Wiley & Sons, 1991.

[26] S. Trisno, "Design and analysis of advanced free space optical communication systems," PhD. dissertation, University of Maryland, College Park, Department of Electrical and Computer Engineering. June 2006.

[27] T. Ernst and W. Dabbous, "A circuit-based approach for routing in unidirectional links networks," *INRIA Research Report*, no. 3292, November 1997.

[28] A. Harris, M.K. Al Akkoumi, F.N. Beainy, R.C. Huck, P.K. Verma and H.H. Refai, "Hybrid networks - free space optics to balloon mounted wireless LAN for remote emergency operations," in *Proceedings on the Wireless and Optical Communications Conference*, Montreal, Canada, May 2007, pp. 867–891.

[29] P. Erdos and A. Renyi, "On the evolution of random graphs," *Publication of Math. Institute of Hungary Academy Science*, vol. 5, 1961, pp. 17–61.

[30] H. Chan and A. Perrig, "Security and privacy in sensor networks," *IEEE Computer Magazine*, vol. 36, no. 10, October 2003, pp. 103-105.

[31] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in *Proceedings of ACM International Conference on Mobile Computing and Networking*, Rome, Italy, July 2001, pp. 189–199.

[32] P. Santi, D. Blough and F. Vainstein, "A probabilistic analysis for the range assignment problem in ad hoc networks," in *Proceedings on ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Rome, Italy, 2001, pp. 212–220.

[33] P. Santi, and D. Blough, "The critical transmitting range for connectivity in sparse wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2. no 1. January-March 2003, pp. 25 –39.

[34] A. Clementi and P. Penna and R. Silvestri, "Hardness results for the power range assignment problem in packet radio networks," in *Proceedings of the 2nd International Workshop on Approximation Algorithms for Combinatorial Optimization Problems*, Berkeley, CA, vol. 1671, 1999, pp. 197–208.

[35] S. Shakkottai, R. Srikant and N. Shroff, "Unreliable sensor grids: Coverage, connectivity and diameter," in *Proceedings of IEEE INFOCOM*, San Francisco, CA, vol. 2, 2003, pp. 1073–1083.

[36] B. Liu and D. Towsley, "A study of the coverage of large-scale sensor networks,"

in *Proceedings of the 1st IEEE International Conference on Mobile Ad-Hoc and Sensor Systems*, Fort Lauderdale, FL, October 2004, pp. 475–483.

[37] H. Zhang and J. C. Hou, "Maintaining sensing coverage and connectivity in large sensor networks," *Wireless Ad Hoc and Sensor Networks: An International Journal*, vol. 1, no. 1–2, January 2005, pp. 89–123.

[38] P. Piret, "On the connectivity of radio networks," *IEEE Transactions on Information Theory*, vol. 37, no. 5, September 1991, pp. 1490–1492.

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

[40] M. Zavlanos and G. Pappas, "Potential fields for maintaining connectivity of mobile networks," *IEEE Transactions on Robotics*, vol. 23, no. 4, August 2007, pp. 812–816.

[41] S. Song, D. L. Goeckel and D. Towsley, "An improved lower bound to the number of neighbors required for the asymptotic connectivity of ad hoc networks," *IEEE Transactions on Information Theory*, vol. 52, no. 6, June 2005, pp. 2756–2761.

[42] 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 & computing*, Lausanne, Switzerland, 2002, pp. 80–91.

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

[44] E. Gilbert, "Random plane networks," *Journal of the Society of Industrial and Applied Mathematics*, vol. 4, no. 9, 1961, pp. 533–543.

[45] R. Meester and R. Roy, "Continuum percolation," Cambridge, UK: Cambridge University Press, 1996.

[46] B. Bollobas, "Modern Graph Theory," Cambridge, UK: *Springer*, 2002.

[47] L. Kleinrock and J. Silvester "Optimum transmission radii for packet radio networks or why six is a magic number," in *Proceedings of IEEE National Telecommunications Conference*, Birmingham, AL, vol. 1, December, 1978, pp. 431–435.

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

[49] L. Lazos and R. Poovendran, "Stochastic coverage in heterogeneous sensor networks," *ACM Transactions on Sensor Networks*, vol. 2, no. 3, August 2006, pp. 325–358.

[50] K. Kar and S. Banerjee, "Node placement for connected coverage in sensor networks," in *Proceedings of the Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, Sophia*, Antipolis, France, 2003, pp. 352–361.

[51] E. Kranakis, D. Krizanc and J. Urrutia, "Coverage and connectivity in networks

with directional sensors," in *Proceedings of Euro-Par Conference*, Pisa, Italy, vol. 3149, 2004, pp.917–924.

[52] H. Ma and Y. Liu, "On coverage problems of directional sensor networks," in *Proceedings of the 1st International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, Wuhan, China, vol. 3794, 2005, pp. 721–731.

[53] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," in *Proceedings of Hawaiian International Conference on Systems Science*, Big Island, Hawaii, vol. 2, January 2000, pp.10-19.

[54] F. Ye, A. Chen, S. Lu, and L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks, in *Proceedings on the 10th International Conference on Computer Communications and Networks*, Scottsdale, AZ, October 2001, pp. 304–309.

[55] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, Boston, MA, August 2000, pp. 2–16.

[56] J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, and D. Ganesan, "Building efficient wireless sensor networks with low-level naming," in *Proceedings of the 18th ACM symposium on Operating systems principles*, Banff, Canada, October 2001, pp. 146–159.

[57] D. Ganesan and R. Govindan, S. Shenker and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *Mobile Computer Communications Review*, vol. 5, no. 4, 2001, pp. 11–25.

[58] R. C. Shah and J. M. Rabaey, "Energy aware routing for low energy ad hoc sensor networks," in *Proceedings of IEEE Wireless Communications and Networking Conference*, Orlando, FL, vol. 1, March 2002, pp. 17–21.

[59] C. Shurgers and M. Srivastava, "Energy efficient routing in wireless sensor networks," in *Proceedings of IEEE Military Communication Conference*, Washington D.C., vol. 1, October 2001, pp. 357–361.

[60] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in *Proceedings of IEEE Aerospace Conference*, Santa Clara CA, vol. 3, 2002, pp. 1125–1130.

[61] S. Lindsey, C. S. Raghavendra and K. Sivalingam, "Data gathering in sensor networks using the energy-delay metric," in *Proceedings on the Workshop on Issues in Wireless Networks and Mobile Computing*, Valencia, Spain, April 2001, pp. 188–192.

[62] A. Manjeshwar and D. P. Agarwal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks," in *Proceedings of the 1st International workshop on Parallel and Distributed Computing: Issues in Wireless Networks and Mobile Computing*, San Fransisco CA, April 2001, pp. 2009–2015.

[63] A. Manjeshwar and D. P. Agarwal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in *Proceedings of the International Parallel and Distributed Computing Conference*, Fort Lauderdale, FL, June 2002, pp. 195-202.

[64] L. Subramanian and R. H. Katz, "An architecture for building self configurable systems," in *Proceedings of the IEEE/ACM Workshop on Mobile Ad Hoc Networks and Computing*, Boston, MA, August 2000, pp. 63–73.

[65] Q. Fang, F. Zhao and L. Guibas, "Lightweight sensing and communication protocols for target enumeration and aggregation," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Annapolis MD, June 2003, pp. 165-76.

[66] J. N. Al-Karaki, R. Ul-Mustafa and A. E. Kamal, "Data aggregation in wireless sensor networks exact and approximate algorithms," in *Proceedings on IEEE Workshop on High Performance Switching and Routing*, Phoenix AZ, April 2004, pp. 241–245.

[67] Q. Li, J. Aslam and D. Rus, "Hierarchical power-aware routing in sensor networks," in *Proceedings of the DIMACS Workshop on Pervasive Networking*, Piscataway NJ, May 2001, pp. 420–423.

[68] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless sensor networks," in *Proceedings of ACM International Conference on Mobile Computing and Networking*, Boston MA, August 2000, pp. 243–254.

[69] Y. Yu, D. Estrin, and R. Govindan, "Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks," *UCLA Computer Science Department Technical Report,* UCLA-CSD TR-010023, May 2001.

[70] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad-hoc routing," in *Proceedings of ACM International Conference on Mobile Computing and Networking*, Rome Italy, August 2001, pp. 70–84.

[71] F. Kuhn, R. Wattenhofer, and A. Zollinger, "Worst-case optimal and average-case efficient geometric ad-hoc routing," in *Proceedings of the 4th ACM Inter-*

national Conference on Mobile Computing and Networks, San Diego CA, vol. 37, September 2003, pp. 267-78.

[72] I. Stojmenovic and X. Lin, "GEDIR: Loop-free location based routing in wireless networks," in *Proceedings of the International Conference on Parallel and Distributed Computer and Systems*, Boston MA, November 1999, pp. 1025–1028.

[73] L. Doherty, L.E. Ghaoui, S.J. Pister, "Convex position estimation in wireless sensor networks," in *Proceedings of the IEEE 20th Annual Joint Conference of the IEEE Computer and Communications Societies*, Anchorage AL, vol. 3, April 2001, pp. 1655–1663.

[74] T. He, C. Huang, B. M. Blum, "Range-free localization schemes for large-scale sensor networks," in *Proceedings of the IEEE 9th Annual International Conference on Mobile Computing and Networking*, San Diego CA, September 2003, pp. 81–95.

[75] N. Bulusu, J. Heidemann, D. Estrin, "GPS-less low cost outdoor localization for very small devices," *IEEE Personal Communication Magazine*, vol. 7, no. 5, 2000, pp. 28–34.

[76] D. Niculescu and B. Nath, "DV-based positioning in ad hoc networks," *Telecommunication Systems Magazine*, vol. 22, no. 4, 2003, pp. 267–280.

[77] L. Lazos, and R. Poovendran, "SeRLoc: Robust localization for wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 1, no. 1, August 2005, pp. 73–100.

[78] Y. Wu, L. Zhang, Y. Wu, and Z. Niu, "Interest dissemination with directional

antennas for wireless sensor networks with mobile sinks, " in *Proceedings of the 4th international conference on Embedded networked sensor systems (Sensys '06)*, Boulder CO, October-November 2006 pp. 99–111.

[79] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, Norwell, MA: Kluwer Academic Publishers, vol. 353, 1996.

[80] L. Bao and J. J. Garcia-Luna-Aceves, "Link-state routing in networks with unidirectional links," in *Proceedings of International Conference on Computer Communications and Networks*, Boston MA, October 1999, pp. 358-363.

[81] H Huang, G.H. Chen, F.C.M. Lau, and L. Xie, "A distance-vector routing protocol for networks with unidirectional links," *Computer Communications*, vol. 23, no. 4, 2000, pp. 473–478.

[82] S. Nesargi and R. Prakash"A tunneling approach to routing with unidirectional links in mobile ad-hoc networks," in *Proceedings of the 9th International Conference on Computer Communications and Networks*, Las Vegas NV, October 2000, pp. 522–527.

[83] W. Dabbous, E. Duros, and T. Ernst, "Dynamic routing in networks with unidirectional links," in *Proceedings of the 2nd Workshop on Satellite-Based Information Systems*, Budapest Hungary, October 1997, pp. 3547.

[84] M. Marina and S. Das, "Routing performance in the presence of unidirectional links in multihop wireless networks," in *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Lausanne Switzerland, June 2002, pp. 12-23.

[85] R. Prakash, "A routing algorithm for wireless ad hoc networks with unidirectional links," *Wireless Networks*, vol. 7, no. 6, 2001, pp. 617-625.

[86] V. Ramasubramanian, R. Chandra, and D. Mosse, "Providing a bidirectional abstraction for unidirectional ad hoc networks," in *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies*, New York NY, June 2002, pp. 1258-1267.

[87] W. Lou and J. Wu, "A multi-path routing protocol for unidirectional networks," in *Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications*, Las Vegas NV, June 2001, pp. 2021-2027.

[88] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in *Proceedings of SCS Conference on Communication Networks and Distributed Systems Modeling and Simulation*, San Antonio TX, January 2002, pp. 86–93.

[89] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis and defenses," in *Proceedings of the Symposium on Information Processing in Sensor Networks*, Berkeley CA, April 2004, pp 259–268.

[90] Y. Hu, A. Perrig and D.B. Johnson, "Wormhole Attacks in Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, February 2006, pp. 370–380.

[91] L. Lazos and R. Poovendran, SeRLoc: secure range-independent localization for wireless sensor networks, in *Proceedings of the ACM Workshop on Wireless Security*, Philadelphia PA, October 2004, pp. 21–30.

[92] A. Arora, P. Dutta, S. Bapat,V. Kulathumani, H. Zhang, V. Naik, H. Mittal, M. Cao, Y. Choi, T. Herman, S. Kulkarni, U. Arumugam, M. Nesterenko,

A. Vora and M. Miyashita, "A line in the sand: A wireless sensor network for target detection, classification, and tracking," *ACM Computer Networks: Special Issue on Military Communications Systems and Technologies*, vol. 46, no. 5, 2004, pp. 605–634.

[93] A. Leon-Garcia, "Probability and Random Processes for Electrical Engineering," Boston, MA: Addison-Wesley, 1993.

[94] A. V. Aho, J. E. Hopcroft and J. D. Ullman, "The design and analysis of computer algorithms," Boston, MA: Addison-Wesley, 1974.

[95] T. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, "Introduction to algorithms, 2nd edition," Cambridge, MA: The MIT press, 2001.

[96] "Texas A & M University Super Computing Facility," http://sc.tamu.edu/.

[97] S. Bandyopadhyay and E. J. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," in *Proceedings of the IEEE 22nd Annual Joint Conference of the IEEE Computer and Communications Societies*, San Francisco CA, vol. 3, March-April 2003, pp. 1713–1723.

[98] A. Amis and R. Prakash, "Load-balancing clusters in wireless ad hoc networks," in *Proceedings of 3rd IEEE Symposium on Application-Specific Systems and Software Engineering Technology*, Richardson, TX, April 2000, pp. 25-32.

[99] B. Das and V. Bharghavan, "Routing in ad-hoc networks using minimum connected dominating sets," in *Proceedings of IEEE International Conference on Communications*, Montreal Canada, vol. 1, June 1997, pp. 376–380.

[100] A. Farid, and S. Hranilovic, "Outage capacity optimization for free-space optical

links with pointing errors," *IEEE Journal of Lightwave Technology*, vol. 25, no. 7, July 2007, pp. 1702–1710.

[101] X. Zhu and J. M. Kahn, "Free-Space Optical Communication through Atmospheric Turbulence Channels," *IEEE Transactions on Communications*, vol. 50, no. 8, August 2002, pp. 1293–1300.

[102] M. Uysal, S. M. Navidpour, and J. Li, "Error rate performance of coded free-space optical links over strong turbulence channels," *IEEE Communications Letters*, vol. 8, no. 10, October 2004, pp. 635–637.

APPENDIX A

NOTATION

Notation	Meaning
s_i	the sensor node's identity
$\mathcal{S}_n$	the set of all n nodes
$\mathcal{E}$	the adjacency matrix/edge set of the WOSN
$G(\mathcal{S}_n, \mathcal{E})$	the directed random graph model of the WOSN
θ_i	the orientation of node s_i
Υ_i	the point position of node s_i
Φ_i	the sector centered at Υ_i, of radius r, angle α, and orientation θ_i.
δ_i^+	in degree of node s_i
δ_i^-	out degree of node s_i
$s_i \rightarrow s_j$	direct one hop path from s_i to s_j
$s_i \rightsquigarrow s_j$	a path originating at s_i and ending at s_j
$\mathcal{S}_i$	set consisting of s_i's successors
$\mathcal{P}_i$	set consisting of s_i's predecessors
$\Pr[N]$	the probability that event N occurs
p_f^i	$\Pr[\delta_i^+ > 0]$
p_b^i	$\Pr[\delta_i^- > 0]$

Notation	Meaning
$p^i_{b\|f}$	$\Pr[\delta_i^- > 0 \| \delta_i^+ > 0]$
p^i_d	$\Pr[s_i$ is not isolated$]$
p_d	$\Pr[$there is no isolated node in $G(\mathcal{S}_n, \mathcal{E})]$
p_c	$\Pr[G(\mathcal{S}_n, \mathcal{E})$ is connected$]$
BS	the base station
CH	a cluster head
s_i^*	a node s_i that is a cluster head
P_{CH}	the probability that a node is a cluster head
$\mathcal{CH}$	the set of cluster head nodes
$UL(s_i)$	an uplink path $s_i \rightarrow BS$
$DL(s_i)$	a downlink path $BS \rightarrow s_i$

APPENDIX B

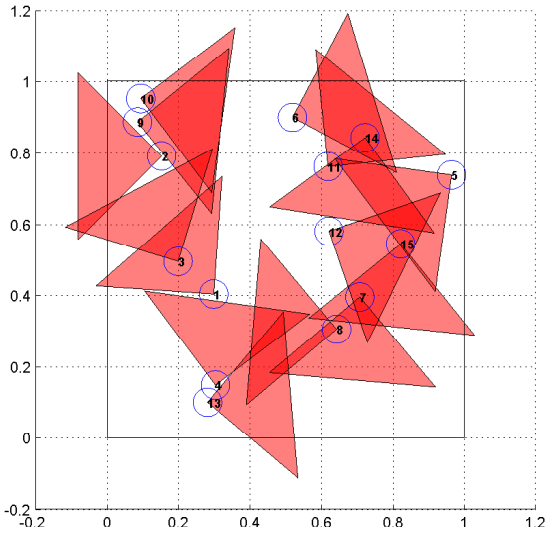
COMPUTING TOROIDAL DISTANCES

The Toroidal distance metric is employed to eliminate border effects [42]. If $d\left(\binom{x_i}{y_i}, \binom{x_j}{y_j}\right)$ denotes the usual Euclidean distance between two point $\binom{x_i}{y_i}$ and $\binom{x_j}{y_j}$ on a bounded area $[0, x_{max}][0, y_{max}]$. Then the Toroidal distance $d_T(s_1, s_2)$ between nodes s_1 and s_2 is:

$$\min\left[d\left(\binom{x_i}{y_i}, \binom{x_j}{y_j}\right), d\left(\binom{x_i + x_{max}}{y_i}, \binom{x_j}{y_j}\right), d\left(\binom{x_i - x_{max}}{y_i}, \binom{x_j}{y_j}\right),\right.$$
$$d\left(\binom{x_i}{y_i + y_{max}}, \binom{x_j}{y_j}\right), d\left(\binom{x_i}{y_i - y_{max}}, \binom{x_j}{y_j}\right), d\left(\binom{x_i + x_{max}}{y_i + y_{max}}, \binom{x_j}{y_j}\right),$$
$$\left.d\left(\binom{x_i + x_{max}}{y_i - y_{max}}, \binom{x_j}{y_j}\right), d\left(\binom{x_i - x_{max}}{y_i + y_{max}}, \binom{x_j}{y_j}\right), d\left(\binom{x_i - x_{max}}{y_i - y_{max}}, \binom{x_j}{y_j}\right)\right]$$

Note that $d_T(s_i, s_j) \leq d(s_i, s_j)$, and $s_i \rightarrow s_j$ if $d_T(s_i, s_j) \leq r$ and $|\Theta_i - \Psi_{ij}^T| \leq \frac{\alpha}{2}$.

The sample 15-node graph of figure B.1(a) and its corresponding adjacency matrix depicted in Figure B.1(b) is obtained by employing the Toroidal distance metric. The ones in the matrix marked with an asterisk indicate links occurring due to the Toroidal measure (i.e., they would be a zero if a Euclidean distance metric is employed). It suffices to populate the adjacency matrix by simply inserting one's for each node's successors as a node is a predecessor to all nodes that are its successors.



(a) A DSN node graph with 15 nodes, $r = 0.334, \alpha = 90^o$

$$\begin{pmatrix}
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1* & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1* & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

(b) Adjacency matrix of the DSN

Fig. B.1. Sample simulation scenario of node graph using Toroidal distance measure to compute the adjacency matrix. The 1s with asterisks indicates the positions affected by the Toroidal distance metric which would otherwise be a zero.

APPENDIX C

KOSARAJU'S ALGORITHM TO FIND SCC OF $G_N(\mathcal{S}_N, \mathcal{E})$

Function *Kosaraju* $[G_n(\mathcal{S}_n, \mathcal{E}), BS]$

1. *Perform DFS of* $G_n(\mathcal{S}_n, \mathcal{E})$ *and number the vertices in order of completion of the recursive call*

2. *Construct a new directed graph* $G'_n(\mathcal{S}_n, \mathcal{E})$ *by reversing the direction of every arc in* $G_n(\mathcal{S}_n, \mathcal{E})$

3. *Perform a DFS on* $G'_n(\mathcal{S}_n, \mathcal{E})$ *starting the search from the highest numbered vertex according to the numbering assigned in step 1.*

4. *If the DFS does not reach all vertices start the next DFS from the highest numbered remaining vertices.*

5. *Each tree in the resulting spanning forest is a strong component of* $G_n(\mathcal{S}_n, \mathcal{E})$*, and the largest tree is the SCC of* $G_n(\mathcal{S}_n, \mathcal{E})$

VITA

Unoma Ndili Okorafor received the Ph.D. degree in the Electrical and Computer Engineering Department, Texas A&M University, College Station, Texas in August 2008. She obtained her M.Sc. degree in Electrical and Computer Engineering Department from Rice University, Houston, Texas in 2001, and the B.Sc. degree in Electrical Engineering from the University of Lagos, Nigeria in 1998. Her research interests include secure routing and connectivity analysis for directional and broadband wireless sensor networks. Ms. Okorafor is a Student Member of IEEE, ACM, SWE, NSEB and SPIE, and she has been the recipient of the Sloan Foundation Fellowship for minority Ph.D. students and the AAUW Engineering Dissertation Fellowship.

Unoma Ndili Okorafor may be contacted at following address:
214-B Zachry Engineering Center, Mail Stop 61,
Texas A&M University, College Station, Texas 77843-3405.
Email: unondili@ece.tamu.edu.

The typist for this thesis was Unoma Ndili Okorafor.