Security-Aware Routing and Localization for a Directional Mission Critical Network

Unoma N. Okorafor, *Member, IEEE,* and Deepa Kundur, *Senior Member, IEEE*

***Abstract*—There has been recent interest in the development of untethered sensor nodes that communicate directionally via free space optical communications for mission critical settings in which high-speed link guarantees in hostile environments are needed. Directional wireless optical sensor networks have the potential to provide gigabits per second speeds for relatively low power consumption enabling bursty traffic and longer network lifetimes. In randomly deployed sensor settings, the crucial steps of ad hoc route setup and node localization are not only non-trivial, but also vulnerable to security attacks. In response to these challenges, this paper proposes a lightweight security-aware integrated routing and localization approach that exploits the benefits of link directionality inherent to wireless optical sensor networks. The circuit-based algorithm that makes use of directional routing loops, called SIRLoS, leverages the resources of the base station and a hierarchical network structure to identify topological information and detect security violations in neighborhood discovery and routing mechanisms. We study the performance of the SIRLoS algorithm demonstrating that reduced localization error, routing overhead, and likelihood of attack in various contexts are possible within lightweight computational constraints.**

***Index Terms*—Directional optical mission critical network, secure routing and localization, free space optical sensor network, circuit-based routing.**

I. Introduction

THE LAST few decades has seen a substantial transformation of wireless networking technologies leading to the recent interest in the integration of computation, communications and sensing mechanisms for low cost untethered device development. There is currently also an active interest in enabling a tighter coupling of this sensor networking technology to the physical world through actuation. This would lead to numerous new applications including smart vehicles, autonomous disaster exploration, and the surveillance and control of critical infrastructure. In such life-critical contexts designing for safety often translates to ensuring communication system security and device "awareness". For example, in disaster exploration, autonomous agents must have the ability to acquire and transmit sensed multimedia data such as temperature and video signals as well as identify their location in order to provide essential information to first responders.

Research in mission critical networks (MCNs) addresses such challenges through the development of mechanisms that promote specialized networks that are adaptable, ultra-dependable and secure in the face of adverse conditions. In some contexts, these networks are comprised of small-sized wireless battery-operated nodes that are randomly and rapidly deployed. Such characteristics are essential for system operation, but their untethered nature and resource limitations pose power and bandwdith challenges. In addition, without adequate security design, these ad hoc networks are vulnerable to attacks including passive eavesdropping, denial-of-service (DoS) and data and node corruption [1] easily leading to catastrophe in safety-critical situations.

A. Directional Optical Mission Critical Networks

There has recently been a push toward the development of directional communication paradigms for ad hoc networking [2], [3]. In contrast to traditional omnidirectional radio frequency (RF) communications, directional RF antennas and broad beam or scanning free space optical (FSO) laser technologies provide higher bandwidths, longer communication ranges and smaller transmission footprints to aid security. Nodes employing free space optics, in comparison to RF, have the advantage of smaller size (for greater agility), power conservation (orders of magnitude better) and gigabits per second speeds suitable for broadband multimedia transmission. These capabilities are imperative to provide multimodal surveillance guarantees and to handle bursty traffic for effective decision-making in mission critical settings. By focusing light in one direction, reduced multi-path interference and greater spatial reuse over conventional RF communication is possible. However, it is necessary to account for atmospheric effects and line-of-sight necessities of the laser beam at both the data link and networking levels [4], [5], [6]. Table I summarizes some differences between conventional omnidirectional RF and FSO sensor node technologies [7], [4], [8], [9], [5], [10]. As witnessed by the popularity of the Smart Dust mote [4], [10], the use of wireless optical communications requires welcome paradigm shifts in network design for safety-critical applications. We refer to such communication systems as directional optical mission critical networks (DOMCNs).

Surveillance of critical infrastructure, for example, is a safety-critical application that relies heavily on the ability of arbitrarily positioned nodes to securely gain knowledge of their location and to establish secure ad hoc routing mechanisms to identify, track and communicate vital data such as the presence of danger. Given the possibly harsh communication environment as well as the heterogeneity of nodes with varying degrees of size and communication capability, it is often imperative that sensor nodes have multiple modes of data

Manuscript received 9 April 2009; revised 25 October 2009. A preliminary version of this paper appears in the Proc. of the 2nd IEEE Workshop on Mission-Critical Networking. This research was partially supported by NSF under grants ECCS-0735114 and EEC-0649142.

U.N. Okorafor is with Texas Instruments, Inc. in Dallas, TX; D. Kundur is with the Department of Electrical and Computer Engineering, Texas A&M University, College Station.

Digital Object Identifier 10.1109/JSAC.2010.100605.

TABLE I
COMPARISON OF OMNIDIRECTIONAL RF AND FSO NODES.

	Omni RF Nodes	**FSO Nodes**
Transmit energy	$O(100)$ nJ/bit	$O(10)$ pJ/bit
Receive energy	$30-50$ nJ/bit	Negligible
Frequency spectrum	Licensed/costly	Unregulated/free
Bandwidth	up to 1 Mb/s	$0.045-1.25$ Gb/s
Commun. channel	Broadcast	Line-of-sight
Commun. range	>100 km	<6 km
Interference	Electromag or RF jamming	Phys. obstruction weather, solar

transmission. For this reason hybrid RF/FSO technologies have been of interest [11]. In some contexts, omnidirectional communication is employed for communicating control signals while directional transmission is employed for bursty high bandwidth acquired data [2].

It has been demonstrated how a significant majority of links in DOMCNs based on ad hoc networking models such as [4], [10], [12] are directional by nature (i.e., communications over a link is unidirectional, not bidirectional) and thus cannot be ignored. This makes neighborhood discovery, routing and localization mechanisms developed for traditional omnidirectional RF networks [13] (primarily based on reverse path routing approaches) inapplicable. Furthermore, the resource constraints of the nodes impedes the use of global positioning systems and costly security primitives based on asymmetric cryptography. It is therefore imperative that the feasibility of an integrated and low-cost routing and localization scheme for DOMCNs be studied.

B. Related Work

Recently, a number of routing protocols have been proposed for lightweight ad hoc networks [14]. These approaches attempt to minimize energy usage for routing while maximizing network lifetime. Protocols such as TinyOS, MCFA, SPINS, GEAR, SAR, Rumor Routing and Directed Diffusion, intended for multihop ad hoc networking, use various optimization considerations including data aggregations, data dissemination latency and energy dissipation. These traditional ad hoc routing approaches apply to bidirectional-link networks and are fundamentally based on a *reverse-path* routing paradigm that is incompatible with the (non-reversible) directional links present in DOMCNs.

A simple and efficient solution for dealing with networks with some unidirectional links is called *tunneling* [15], in which bidirectionality is emulated for a unidirectional link by using a multihop reverse backchannel consisting of bidirectional links to establish the tunnel. However, because of its high overhead [15], [16], [17], [18], [19], [20] tunneling is inappropriate for DOMCNs in which a significant proportion of links are unidirectional. As discussed in [15], designing a routing paradigm from scratch for DOMCNs, in contrast to modifying existing routing protocols, is the most desirable alternative.

For unidirectional link optical wireless networks, two main routing paradigms exist: broadcast-gather [10], [21] and circuit-based [22], [23], [24], [25], [26]; the latter is the focus of this paper. The broadcast-gather approach has been shown to be inefficient in contrast to circuit paradigms [22], [23] because uplink and downlink communications are accounted for separately, and it does not account for security. The circuit-based routing paradigm enables bidirectional communications amongst nodes with unidirectional links by using distinct paths to and from sender and receiver nodes. This results in bidirectional communications occurring along a circuit (a closed multihop loop originating and terminating at the same node). However, prior circuit-based research has not addressed the localization issue. To the best of the authors' knowledge, this is the first secure integrated routing and localization scheme for directional optical link networks.

C. Contributions and Organization of this Paper

This paper presents SIRLoS, a novel lightweight secure integrated routing and localization scheme for DOMCNs. In order to conserve power, size and cost, SIRLoS does not make use of expensive range estimation methods, time synchronization or localization hardware. Instead the SIRLoS approach exploits a hierarchical cluster-based organization of the network to offer: (1) a circuit-based neighborhood discovery and routing approach; (2) a practical location estimation algorithm that exploits topology control mechanisms; and (3) lightweight security services based on symmetric cryptography and that leverage the base station. 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 the security benefits of link directionality in SIRLoS and provide performance evaluations as well as attack and security analysis to demonstrate its potential in MCN applications.

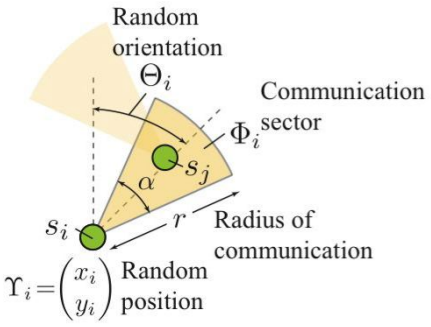
Section II introduces the DOMCN architecture, threat model and security assumptions. Section III details the SIRLoS approach highlighting the lightweight design characteristics. Security and performance analysis are presented in Section IV followed by final remarks in Section V.

II. NETWORK MODELS AND ASSUMPTIONS

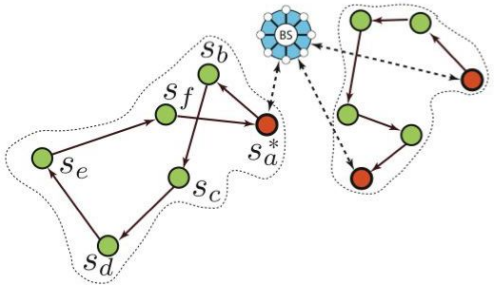
A. The Directional Mission Critical Network

It is assumed that n DOMCN nodes are randomly and densely deployed with uniform distribution in a planar two-dimensional region $\mathcal{A}$. The set of n nodes are denoted $\mathcal{S}_n = \{s_i : i = 1, 2, \cdots n\}$ with each node s_i having an equal and independent likelihood of falling at any coordinate location $\Upsilon_i = \binom{x_i}{y_i} \in \mathcal{A}$ and facing a random orientation $\Theta_i \sim \text{Uniform}[0, 2\pi)$ with respect to a common reference axis (e.g., pointing north) as shown in Figure 1(a). We denote $I(s_i) = (\Upsilon_i, \Theta_i)$ as s_i's information vector.

Each node is equipped with a directional broad beamed FSO transmitter of communication range r (in units of km) and a beamwidth of α (in units of radians unless otherwise stated) whose center points in the direction of the node's orientation θ_i. As depicted in Figure 1(a), by scanning a laser beam, s_i transmits data within a contiguous, randomly oriented communication sector $-\frac{\alpha}{2}+\Theta_i \leq \Phi_i \leq +\frac{\alpha}{2}+\Theta_i$ of radius r, and angle $\alpha \in [0, 2\pi)$, such that Φ_i is uniquely defined by the three-tuple $(I(s_i), r, \alpha)$. Following convention [10], a node's receiver is omnidirectional, so that s_i may directly transmit



(a) A DOMCN node.



(b) BS-circuit Paradigm.

Fig. 1. The Directional Mission Critical Network. (a) Directionality of data transmission at the physical layer results in unidirectional links; here $s_i \rightarrow s_j$, but $s_j \not\rightarrow s_i$; (b) At the network-level a circuit-based routing paradigm is employed. CHs are denoted with bolded outlines.

to s_j (denoted $s_i \rightarrow s_j$) if and only if $\Upsilon_j \in \Phi_i$. However, s_j can only transmit to s_i via a directed multihop reverse route (denoted $s_i \rightsquigarrow s_j$), with other nodes acting as routers (unless of course $\Upsilon_i \in \Phi_j$, resulting in the bidirectional link $s_i \rightleftarrows s_j$). Naturally, in discovering a multihop reverse path, the notion of a *circuit* [27] (a closed multihop loop originating and terminating at the same node) results, and serves as the fundamental mechanism for bidirectional communications in DOMCNs [28].

This idealized model provides a opportune way to link device level parameters to large-scale network behavior. It also models the well known class of Smart Dust FSO sensor networks [4] providing a theoretical platform to design networking algorithms. Moreover, the parameter α conveniently controls the proportion of unidirectional to bidirectional network links, where as $\alpha \rightarrow 2\pi$ the network approaches a random geometric graph (RGG) model commonly employed to analyze omnidirectional RF networks; this provides a framework for comparing the ad hoc networking properties when omnidirectional and directional physical layer transmissions are employed to better assess applicability to various mission critical settings.

In an ad hoc network, the *base station* (denoted BS) gathers critical information from the sensors and transmits queries or control information to the sensor nodes. For scalability and improved connectivity [12] a hierarchical network structure is created that involves communication of the sensor nodes to the base station via cluster heads (CHs) that have bidirectional links to the base station. In hybrid sensor networks, CH communications can be achieved via omnidirectional RF transmissions. In all-optical wireless networks, hardware such as passive corner cube retroreflectors (CCRs) can establish bidirectional links with the base station without significantly depleting energy [4]. Typically, CHs are gateway nodes that send/receive data directly to/from the BS on behalf of other nodes in their associated *clusters*. We denote the set of CH nodes by $\mathcal{CH}$, and mark a node $s_k \in \mathcal{CH}$ with a superscript asterisk to give s_k^*.

The fundamental type of circuit used for communications in the DOMCN is known as a *BS-circuit* illustrated in Figure 1(b), which is a circuit that necessarily includes the BS; all non-base station nodes in the BS-circuit are said to be in the same cluster. An *uplink* path to the BS and *downlink* path from the BS for every node in a BS-circuit (or cluster) exists. For example, in Figure 1(b), nodes s_a^*, s_b, s_c, s_d, s_e and s_f are in the same cluster, and s_d has uplink path $s_d \rightarrow s_e \rightarrow s_f \rightarrow s_a^* \rightarrow BS$ and downlink path $BS \rightarrow s_a^* \rightarrow s_b \rightarrow s_c \rightarrow s_d$. Because CHs directly communicate to the BS, each BS-circuit has one or two CHs (an entry and exist CH that may or may not be distinct) as shown in Figure 1(b).

The random directed n-node *graph* $G_n(\mathcal{S}_n, \mathcal{E})$ representing the DOMCN consists of a vertex node set $\mathcal{S}_n$ and an edge set $\mathcal{E}$. The edges are represented via an $n \times n$ adjacency matrix where $\mathcal{E}(i,j)_{1 \leq i,j \leq n} = 1$ if $\Upsilon_j \in \Phi_i$ or 0 otherwise indicating that the edge $s_i \rightarrow s_j$, does or does not exist, respectively. We define $\mathcal{E}(i,i) = 0$ to prevent self loops. The graph $G_n(\mathcal{S}_n, \mathcal{E})$, defined by parameters (n, r, α), is called a random sector graph (RSG) [10] and converges to the traditional RGG model of ad hoc networks for $\alpha = 2\pi$. A significant distinction with the RSG model is that two distinct sets of neighbors must be defined for each node s_i: the set $\mathcal{S}_i =: \{s_k\}, \forall k : \mathcal{E}(i,k) = 1$ consisting of s_i's *successors*, and the set $\mathcal{P}_i =: \{s_h\}, \forall h : \mathcal{E}(h,i) = 1$ consisting of s_i's *predecessors*. In omnidirectional networks, popularly modeled as RGGs, such distinction between successors and predecessors does not exist because links are bidirectional. To aid in scalability and connectivity, by definition, a virtual bidirectional grid connects all CHs via the BS so that $\mathcal{E}(i,j) = \mathcal{E}(j,i) = 1, \quad \forall s_i, s_j \in \mathcal{CH}$ and $i \neq j$, additionally.

B. Threat Model

In safety-critical settings, guaranteeing a high degree of undisrupted information flow, upon which vital decisions are made, is essential. SIRLoS is a network-level protocol, so the threat model considered in this paper is focused on routing-message and routing-operation attacks during neighborhood discovery and route setup . Given the high degree of collaboration during networking, deliberate efforts to breach routing security may cause catastrophic DoS [1]. Within this class of routing attacks, we consider the common two categories of *oustider attacks*, in which the opponent possesses no special access to the network resources and cryptographic keying information, and *insider attacks*, in which a motivated opponent

compromises (via physical or remote exploitation) a subset of authentic nodes, gaining access to secret cryptographic materials and hence already having entry into exclusive network resources.

The most common outsider attacks on routing data include passive eavesdropping, where an attacker attempts to glean information on traffic flows in order to conduct traffic analysis for devastating future attacks, and active injection and replaying of false routing packets in order to disrupt information flow. As we will demonstrate, practical lightweight cryptographic approaches may be used in order to combat these problems.

For insider attacks modeled in this paper, the opponent is limited by the hardware restrictions of the corrupted node; hence, an attacker has the same capabilities as any other node, albeit the resources may be harnessed to maximize damage. Because there is a large variability the execution of an insider attack, measuring the degree of associated network debilitation is not a tractable approach to characterizing the robustness or security of DOMCNs. Given that such an attack is unwanted in general, we assert that a better approach is to measure the difficulty for an opponent to successfully achieve a given form of insider attack and to go undetected.

C. Assumptions

As is convention, the base station is assumed to be 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 or may be placed on a stationary medical aid vehicle. Each node s_i is uniquely identified by its name and is aware of a preset positive integer δ representing the maximum hop count and its orientation Θ_i (by employing an inexpensive compass); the values of r and α are selected to satisfy connectivity constraints [12].

Each 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 all entities, which are each 64-bit random values; symmetric key security primitives using K_i, PW_i, and K_N are employed. 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 MAC of message M with key K [29]. Where appropriate, the lightweight RC5 scheme and the HMAC-MD5 algorithm (with a 128-bit authenticator value) are utilized [30], and the XOR function $\oplus$ is employed to avoid byte expansion.

It is assumed that $s_i \in \mathcal{CH}$ with probability $0 < p_{CH} < 1$ to model arbitrary scattering of CHs in the network. Nodes are not tamper resistant and may be subverted by an attacker with probability $0 < p_a < 1$.

III. SIRLoS: Secure Integrated Routing and Localization Scheme

A. Off-line Key Setup

The first stage of SIRLoS is off-line key generation performed by the BS and setup performed prior to network deployment. As common, a μ-TESLA [30] inspired approach is leveraged for BS broadcast authentication; however, we do not require time synchronization given our BS-circuit paradigm. Given the resource constraints of each node, asymmetric approaches are considered to be too costly necessitating simple symmetric methods of BS data authentication. Here, the BS pre-computes and stores a length-$(E+1)$ one-way key chain $\{K_e\}$ for $e = 0, 1, \ldots, E$, by successively applying a known one-way hash function $\mathcal{F}$ to a randomly generated initial key K_E, so that $K_{e-1} = \mathcal{F}(K_e)$ where $e = 1, 2, \ldots, E$ indexes a particular broadcast communications *era*, and E eras are 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 ones. However, it is trivial to verify that a key K_e (once revealed) was derived from the committment by simply repeatedly 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 $K_1, K_2, \ldots, K_E$, yielding an efficient, simple and lightweight mechanism for each node to authenticate BS messages.

B. Secure Neighborhood Discovery

After DOMCN deployment, ad hoc route establishment requires that topology discovery be initiated. Each CH $s_a^* \in \mathcal{CH}$ indicates its readiness to begin neighborhood discovery by sending a `READY` signal to the BS who responds to s_a^* by generating a unique nonce η_t^a at the current time t, and initiating a simple challenge-and-respond protocol (CRP) to authenticate s_a^* employing K_a and PW_a. The CRP signal also allows the BS to employ a simple range and angular estimation mechanism to determine Υ_a [4]. If s_a^* passes the challenge, the BS sends it a *circuit discovery beacon* (CDB) containing the CH's position Υ_a, marked with η_t^a and encrypted with K_N for onward flooding. The exchange is:

$$
\begin{aligned}
&BS \rightarrow s_a^* : \mathbb{E}_{K_a}[\eta_t^a] \\
&s_a^* \rightarrow BS : \mathbb{E}_{K_a}[PW_a \oplus \eta_t^a] \\
&BS \rightarrow s_a^* : \mathbb{E}_{K_N}[\underbrace{HT = 0 \mid e = 1 \mid K_1 \mid \eta_t^a \mid \Upsilon_a}_{\text{CDB initiated at } BS}]
\end{aligned}
$$

where HT counts the number of hops traveled by the CDB and is thus incremented at every intermediate node. The CDB consists of a 140-bit header with 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. The payload is variable into which each node s_i encountering the CDB appends 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 MAC signature computed as $MAC_{K_i}\{I(s_i)|PW_i\}$. The CDB provides information for nodes to securely update their routing tables and estimate their locations.

Each node s_i (including CHs) 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 corresponding downlink and an associated *cost value*, computed based on HT. Upon receipt of a CDB from node s_h, s_i decrypts the packet using key K_N and performs the following security checks: (1) validation of the source of the

packet by checking that $\mathcal{F}^{e-1}(K_e) = K_0$; (2) verification that $I(s_i)$ is not in the CDB's current payload, to avoid routing loops. If $s_i \notin \mathcal{CH}$, it estimates its location Υ_i^{est} based on the location of its predecessors, included in the payload of CDBs it receives, by employing the location estimation algorithm described in the following section. If $s_i \in \mathcal{CH}$, it simply obtains its coordinates from the CDB received from the BS as previously noted above. To detect wormhole-type attacks, a range-and-orientation constraint (ROC) test that we detail in the next section is performed.

Before forwarding the CDB, s_i also verifies that $HT \leq \delta$ (i.e., the CDB has not expired), increments HT by one, updates the current nonce η^*_{t+HT} in the packet as $\eta^*_{t+HT+1} = \eta^*_{t+HT} \oplus PW_i$, appends its data $[I(s_i) \mid MAC_{K_i}\{I(s_i)|PW_i\}]$ to the CDB's payload, re-encrypts the new CDB with K_N, and then re-broadcasts the updated CDB to its successors. The route discovery task of a CDB with $1 < HT \leq \delta$ is terminated when it encounters a CH, who closes the BS-circuit by returning the packet to the BS.

A CDB is discarded if $HT > \delta$ or if it fails any of the security checks including the ROC test. As a final step, within τ seconds after sending out the CDB, s_i broadcasts a low-bit hello packet ($\texttt{HELLO}_i$) within a communication sector $-\frac{\alpha}{2} + \Theta_i \leq \varphi_i^1 \leq +\frac{\alpha}{2} + \Theta_i$ of radius $r' < r$, to improve the granularity of the location estimation as discussed in the next section.

Assuming all security checks pass at every phase and $\delta > 3$, the above exchange will continue as follows for the first three nodes, s_a^*, s_b and s_c, in the BS-circuit of Figure 1(b):

$$
\begin{aligned}
s_a^* \rightarrow s_b \;&: \mathbb{E}_{K_N}[HT = 1 \mid e = 1 \mid K_1 \mid \eta_t^a \oplus PW_a \parallel I(s_a) \\
&\quad \mid MAC_{K_a}\{I(s_a)|PW_a\}] \\
s_b \rightarrow s_c \;&: \mathbb{E}_{K_N}[HT = 2 \mid e = 1 \mid K_1 \mid \eta_t^a \oplus PW_a \oplus PW_b \\
&\quad \parallel I(s_a) \mid MAC_{K_a}\{I(s_a)|PW_a\} \\
&\quad \parallel I(s_b) \mid MAC_{K_b}\{I(s_b)|PW_b\}] \\
s_c \rightarrow s_d \;&: \mathbb{E}_{K_N}[HT = 3 \mid e = 1 \mid K_1 \mid \eta_t^a \oplus PW_a \oplus PW_b \\
&\quad \oplus PW_c \parallel I(s_a) \mid MAC_{K_a}\{I(s_a)|PW_a\} \\
&\quad \parallel I(s_b) \mid MAC_{K_b}\{I(s_b)|PW_b\} \parallel I(s_c) \\
&\quad MAC_{K_c}\{I(s_c)|PW_c\}]
\end{aligned}
$$

The protocol differs from standard flooding based neighborhood discovery approaches for omnidirectional ad hoc networks in the following ways. First, routing is circuit-based due to the directionality of links making it necessary for the beacons to be both initiated and terminated at a single network entity, in this case the BS. Second, it is necessary that location and orientation information be provided in the CDB in order for the BS to create a network graph to assess optimal routing and to identify attacks such as wormholes, node identity replication and Sybil [1], [31]. A successor node can also identify a potential wormhole attack as we describe in the next section.

Furthermore, to keep the protocol overhead lightweight, to avoid byte expansion in the header the $\oplus$ operation is employed for cheap source authentication. A compromise is that, upon receiving a CDB and testing the nonce field of the header (given by $\eta_t^a \oplus PW_a \oplus PW_b \oplus PW_c \oplus PW_d \oplus PW_e \oplus PW_f \oplus PW_a$ for the circuit in Figure 1(b)), a failed test leaves it ambiguous, which of the nodes may not legitimately be part of the network.

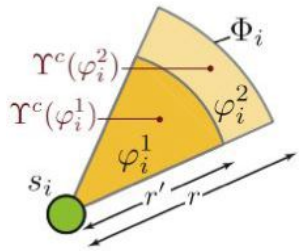


Fig. 2. The centroids of φ_x^1 and φ_x^2.

C. Location Estimation and ROC Test

The reception of the CDB provides a node s_j with knowledge that it lies within a sector of a predecessor. If s_j has s_g, s_h and s_i as predecessors, then s_j may easily deduce that it lies somewhere in the region $\Phi_g \cap \Phi_h \cap \Phi_i$. Assuming random deployment, the optimal estimate for Υ_j in the least square sense is the centroid of $\Phi_g \cap \Phi_h \cap \Phi_i$, which for arbitrary-shaped regions is likely to be complex to compute at each sensor.

To provide finer granularity yet be lightweight, the following procedure is employed that leverages the compact transmission footprint of directional communications. After τ seconds of receiving a CDB from s_i, s_i transmits a $\texttt{HELLO}_i$ signal using a transmission range r'; then, s_j determines that its location Υ_j lies either within the sector $\varphi_i^1 \in \Phi_i$ if it received $\texttt{HELLO}_i$, or otherwise within the semi-annular segment $\varphi_i^2 \in \Phi_i$ as depicted in Figure 2, and then assigns its location Υ_j^{est} as the centroid of the corresponding region. The radius is assigned to be $r' = \frac{r}{\sqrt{2}}$ to make $A(\varphi_1) = A(\varphi_2)$, implying it is equally likely that s_j falls within either part. Specifically, the centroid computations are given by the following easy-to-derive formulas.

Case 1: s_j concludes that $\Upsilon_j \in \varphi_i^1$ and determines Υ_j^{est} as the centroid $\Upsilon^c(\varphi_i^1)$ of φ_i^2:

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

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

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

If s_j has heard thus far $m > 1$ distinct predecessors, it refines its location estimate as the running average of the centroids of the m pie-shaped sectors within which it falls, given by

$$\Upsilon_j^{est} = \frac{1}{m} \sum_{q=1}^{m} \Upsilon^c(\varphi_i^q), \tag{3}$$

where Υ_j^{est} can be computed as the previous estimate scaled by $\frac{m-1}{m}$ plus $\Upsilon^c(\varphi_i^m)$. It should be noted that Υ_j^{est} is not the centroid of the overlapping region of the m sectors, but is a practical estimate that does not require complex search and grid score table schemes to obtain the boundary of the overlap region as employed in [32]. Our scheme differs from the triangulation method of [10] (in which each node waits to receive beacons from three known-location predecessors to

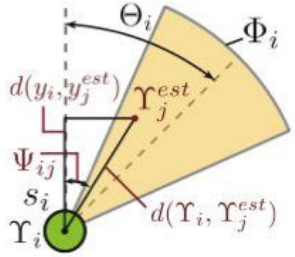


Fig. 3. The ROC test to determine if $\Upsilon_j^{est} \in \Phi_i$.

determine its location), and nodes do not need to perform range estimation or angle-of-arrival measurements, keeping both computational and communication overhead lower.

Once a location estimate is computed, the node s_j performs the ROC test as illustrated in Figure 3 to verify that $d(\Upsilon_i, \Upsilon_j^{est}) \leq r$ and $|\Theta_j - \Psi_{ij}| \leq \frac{\alpha}{2}$ where $d(a,b)$ is the Euclidean distance between points a and b, and $\Psi_{ij} = \arccos \frac{d(y_i, y_j^{est})}{d(\Upsilon_i, \Upsilon_j^{est})}$ (where $\Upsilon_j^{est} = \binom{x_j^{est}}{y_j^{est}}$ and $\Upsilon_j = \binom{x_i}{y_i}$) ensures that $\Upsilon_j^{est} \in \Phi_i$. The ROC test provides a geometric constraint on the network graph which is exploited as a security check to protect against routing attacks such as wormholes. It is possible that a node involved in a wormhole will fabricate its location to avoid deception, however, this will also cause unwanted effects for the corrupt node. First, because of the unidirectional nature of the links, this fabricated location must first be processed by the BS; if multiple incorrect locations are given to various wormhole neighbors, the node's actions will first be identified by the BS as a potential node replication attack. If only a single incorrect location is sent, then the BS may properly process it and send the data to the node's predecessors during a node routing table update phase; however, this runs the problem of not having any predecessors point their lasers in the correct direction and hence the corrupt node will cut itself off from the network.

D. Base Station Network Topology Reconstruction

The BS reconstructs $G_n(\mathcal{S}_n, \mathcal{E}^{'})$ from the BS-circuit and individual node information available in returned CDBs. First, it validates each CDB received; specifically, the BS verifies (1) that HT equals the number of appended sections in the payload; (2) the claimed identity and per hop entry of each node s_i in the CDB by ensuring that its computed $MAC_{K_i}\{I(s_i)\ |PW_i\}$ is equivalent to the signature entry of the node; (3) the final cumulative path nonce η_{t+h}^{*} included in the CDB for each h-hop path (for the circuit in Figure 1(b), it verifies that η_{t+7}^{*} matches $\eta_t^a \oplus PW_a \oplus PW_b \oplus PW_c \oplus PW_d \oplus PW_e \oplus PW_f \oplus PW_a$). If any of the security checks fail or the BS observes a discrepancy in the entries of any CDB, that CDB is discarded, and intrusion detection is initiated for the suspected route(s).

Using the validated CDBs, the BS constructs an adjacency matrix $\mathcal{E}^{'}$ by assuming that a subsequent node in a CDB's payload entry is a successor of the previous node; i.e., if s_j's entry follows that of s_i, the BS assumes $s_i \rightarrow s_j$ and hence $\mathcal{E}_{ij}^{'} = 1$. Once the associated graph is completed, the estimated locations for each node Υ_i^{est} are computed via Equation 3 using all of the predecessor data and the locations of the CHs, and a large-scale ROC test on each link of $\mathcal{E}^{'}$ is performed to determine any wormhole, node identity replication and Sybil attacks. Upon suspicion, further intrusion detection is initiated. At conclusion, links and nodes with unresolved security issues are removed from $\mathcal{E}^{'}$ leaving a graph of validated nodes.

E. Predecessor and Successor Routing Table Update

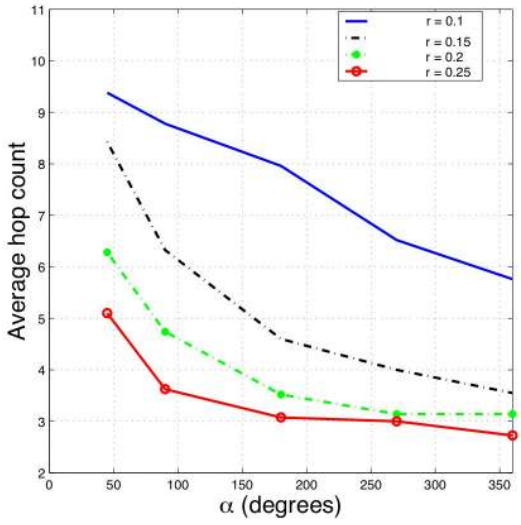
The distinction between predecessor and successor neighbors necessitates two routing tables for a node s_i. We call these predecessor and successor routing tables denoted PRT(s_i) and SRT(s_i), respectively. Collectively, they are given by $RT(s_i) = [PRT(s_i)|SRT(s_i)]$. From $\mathcal{E}^{'}$, the BS constructs PRT(s_i) and SRT(s_i) for each s_i; specifically, the PRT(s_i) (or SRT(s_i)) consists of each distinct downlink (or uplink) path for s_i and its associated cost (in terms of hop count). Route optimizations are then conducted in order to minimize hop count. 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. 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.

F. Dynamic Route Setup

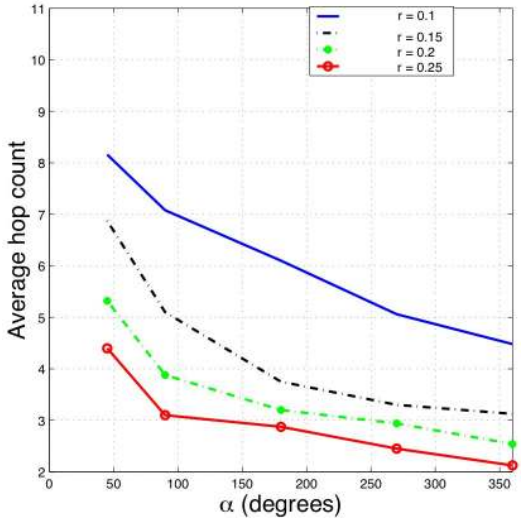
Due to link breakage, addition of new nodes, or mobility, it may be necessary to establish routes dynamically. Dynamic route establishment entails a node s_i seeking a secure and efficient route to any node s_j as needed, by leveraging the BS. Here, s_i sends an encrypted route request RREQ(s_j) for 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 to establish a secure communication for a session. In the case of new nodes that may have entered the network, more optimal routes to and from other nodes including the BS may now be possible. For a new node to enter the network it initiates a CDB as detailed in Section III-B; thus the BS has the most updated topology. When a RREQ is sent to the BS from a node s_i requesting a more optimal route to s_j, an updated minimum cost path can be sent to both s_i and s_j. More details of dynamic route setup can be found in [33].

IV. Performance, Security and Attack Analysis

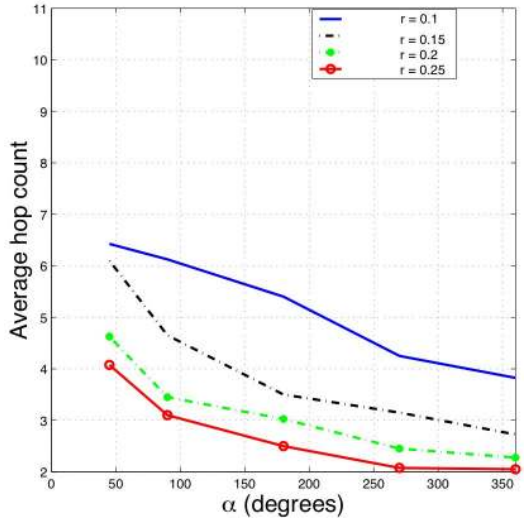
We select foundational metrics to assess SIRLoS for accuracy, overhead, and security. Average hop count and localization error are core measures in a directional paradigm; the average hop count provides an indication of the effort required for neighborhood discovery and routing operations that scale with circuit length. In addition to providing critical surveillance data and identifying wormhole type attacks, location information is important for laser pointing and the



(a) $p_{CH} = 0.1$



(b) $p_{CH} = 0.2$



(c) $p_{CH} = 0.3$

Fig. 4. Average hop count versus beam width α as a function of communication range r for different degrees of hierarchy. Solid, dash-dot, dash-dot line with closed circles, and solid line with open circles represent the $r = 0.1$, $r = 0.15$, $r = 0.2$ and $r = 0.25$ cases, respectively.

associated error will impact physical layer system properties related to transmission gain. Novel security analysis is based on the structure of SIRLoS and focuses on the advantages that circuit-based communications provides when the uplink and downlink paths are distinct. Other aspects of network security that are common to general ad hoc networks are not studied here.

We employ MATLAB for empirical studies with α, p_{CH} and r preset, and (unless otherwise stated) $n = 300$ nodes randomly (with uniform distribution) positioned and oriented in a planar square region of unit area 1 km^2. As predecessor relationships are derived by reversing successor links, it suffices to populate $\mathcal{E}$ by determining successor relationships only. Each simulation scenario is repeated 1000 times, with results averaged to yield statistical confidence within $\pm 1\%$ for parameter ranges for n, r and α that guarantee network connectivity asymptotically almost surely [12].

The reader should note that although the presented simulations correspond to $n = 300$, empirical analysis by the authors for n on the order of thousands demonstrates that the approach scales well. Specifically, as n increases the CH density increases providing shorter uplink and downlink paths to the BS as well as lower localization error. As analyzed in [12], K-connectivity properties are improved providing more network robustness.

A. Average Hop Count

We first observe average hop count $\overline{HT}$ (computed by averaging the HT values of legitimate CDBs received by the BS) versus α with r set to 0.1, 0.15, 0.2, and 0.25 and a corresponding fraction of CH nodes p_{CH} of $0.1, 0.2$ and 0.3. Results are provided in Figure 4; as expected $\overline{HT} \geq 2$. If α is fixed, hop count can be reduced to practical levels with an appropriate selection of range r and hierarchy (via selection of p_{CH}). It appears that r and α have the most significant effects on $\overline{HT}$ demonstrating that once connectivity is achieved, overhead can be reduced with effective selection of (r, α) related to communication device characteristics. Furthermore, given that $\overline{HT}$ is effectively the mean circuit length, and on average a node will take half the hops to reach the BS and vice versa, for all settings that we have tested, the multihop nature of the DOMCN does not create significant networking overhead.

B. 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:

$$LE = \frac{\sum_{i=1}^{n} \sqrt{(x_i - x_i^c)^2 + (y_i - y_i^c)^2}}{n}$$

as the mean squared error between the correct and estimated position vectors (initialized to zero) of $\mathcal{S}_n$. Figure 5 presents the results showing plots of LE versus r for SIRLoS denoted "S" which performs better, compared with the centroid only [32] method (positions are estimated as the average centroid of the sectors of predecessors) denoted "C", as r increases and α decreases. Observe that as $r \rightarrow 0$, LE $\rightarrow (1 - p_{CH})$ (in this case 0.9), since 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 [27], (LE transitions rapidly from a maximum to minimum value) which gets more dramatic as $\alpha \to 2\pi$. 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 5(b) illustrates plots of LE decreasing with increasing p_{CH} and α. Since CHs obtain accurate information of their location directly from the BS, as their proportion within the network increases, the data from which a node can estimate its location becomes more precise yielding a lower LE.

C. Security Analysis

It is straightforward to verify that the integrated security of SIRLoS ensures against outsider attacks such as unauthorized participation in route establishment, spoofed routing signaling, and alteration of routing messages via the lightweight cryptographic mechanisms embedded in the protocol. This section focuses on insider attacks and the fundamental security advantage that a directional paradigm for MCNs provides. We show how the BS verification and uplink-downlink path diversity in SIRLoS provides greater opportunities for network monitoring, increasing the difficulty for a malicious node to control both the forward and reverse flow of the beacon (i.e., with high probability the CDB reaches the BS before returning to a node). This yields security benefits for DOMCNs and provides alerts of intrusion. In the next section, we also analyze attacks aimed at path diversity. It should be noted that uplink and downlink path diversity is also possible in bidirectional paradigms; however, for the most part using distinct communication paths is considered to be inefficient (given that such networks do not possess the advantages that directional networks have at the physical layer) and at least for control signaling (e.g., the sending of ACKs) and protocols, the each link is used bidirectionally if possible.

1) Per Hop Authentication and Alteration of Routing Beacons: Per hop authentication requires the BS to verify the correct participation of each node claimed in the CDB's payload. Employing the cumulative updating of a unique nonce originally generated by the BS, with each node's passwords, a malicious insider node χ_A cannot arbitrarily alter routing information in a CDB without being detected. This distinguishing lightweight node-dependence feature strengthens the cryptographic property of SIRLoS, similar to the dependence structures used in common encryption algorithms. Consider the two possible cases in which χ_A hopes to disrupt routing by forging a non-existent route: (1) χ_A deletes the entry of one or more of its ancestors (i.e., nodes in its downlink path) from the CDB, and alters the HT value accordingly; (2) χ_A inserts false node information in the CDB. In both cases however, without prior knowledge of the original nonce or the impersonated nodes' password and individual key, it is impossible to modify the accumulated nonce value in order to either extract entries to annihilate nodes, or input false entries into the CDB. Furthermore, tampering with the CDB in this way results in the non-verifiability of the final nonce received at the BS, and subsequent discarding of the packet. We have however identified two possible problem cases.

a) Problem Case I: In the two attacks enumerated above, χ_A may succeed in fooling its descendants (i.e., nodes in its uplink path) into making erroneous entries into their PRTs since the CDB is not verified until it is returned to the BS, prior to which nodes already update their PRTs. However, this falsehood is detected when the BS sends routing tables to each node, who then compares the PRT received from the BS with the one it recorded during neighborhood discovery. As previously stated, inconsistent entries are deleted and reported.

b) Problem Case II: A vulnerability exists when a bidirectional link $s_a \leftrightarrows s_b$ occurs involving a node s_a corrupted by χ_A. Say s_a receives the CDB first at hop count h, then χ_A is able to decipher s_b's password by storing the cumulative nonce η^*_{t+h-1} from the CDB when first received and then XORing it with the cumulative η^*_{t+h+1} (related to the same CDB progression) received from s_b due to the bidirectional link. Thus, χ_A deduces that $PW_b = \eta^*_{t+h-1} \oplus \eta^*_{t+h+1}$.

To analyze this vulnerability, we consider the probability of its likelihood (derived in Appendix A) given by

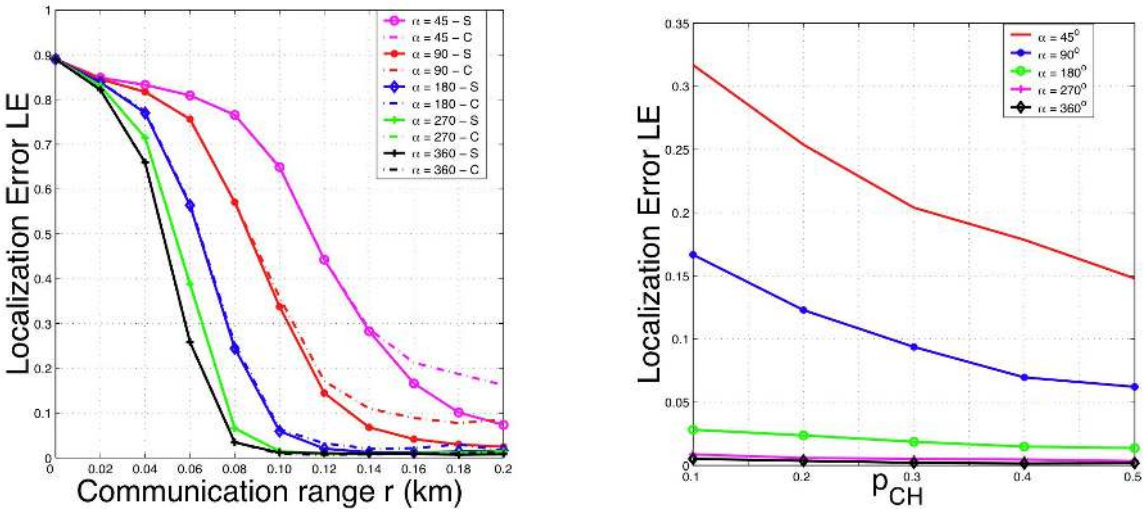
$$p_{\chi_A}(> 0 \leftrightarrows) = p_a \left(1 - e^{\frac{-n\alpha^2 r^2}{4\pi}}\right), \tag{4}$$

for large n. Observe that for $\alpha \to 0$, $p_{\chi_A}(> 0 \leftrightarrows) \to 0$, however as $\alpha \to 2\pi$, $p_{\chi_A}(> 0 \leftrightarrows) \to p_a(1 - e^{-nr^2})$, which represents the RGG model [27], for which directionality cannot no longer be exploited. For larger values of α interestingly, 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 $s_a \leftrightarrows s_b$ could represent an unwanted routing loop.

Figure 6 presents the results for *normalized* $p_{\chi_A}(> 0 \leftrightarrows)$ to demonstrate the advantages of directed communications; a measure normalized with respect to p_a is presented to highlight the dependence on the network graph associated with (n, r, α) instead of on the probability of node corruption p_a. The advantages of directional communications in reducing the risk of this vulnerability for $\alpha \approx \frac{2\pi}{9} = 40^o$ as has been proposed [4] over omnidirectional communications for $\alpha = 2\pi = 360^o$ is clear especially for node density ranges of approximately $n = 300$.

More general forms of vulnerability, in which a corrupt node hears progressing CDPs two hop counts apart, can be considered. For example, in a three node insider link scenario, if $s_b \to s_c$, $s_b \to s_a$ and $s_c \to s_a$ all exist, then a potentially corrupt s_a can deduce PW_b in a similar manner to above. The corresponding analysis is found in [33], but we do not present it here as similar insights are deduced regarding the advantage of directional communications.

2) Broadcast Authentication and Alien Node Participation: Broadcast authentication ensures that only the BS is able to initiate routing. The CRP and encryption with K_N for confidentiality, both serve to prevent outsiders from sniffing the K_e and subsequently initiating, spoofing or fabricating CDBs. While $\{K_e\}$ provides initial broadcast authentication (since no other entity can reveal a correct K_e to CHs), we observe that, a key, once revealed in the CDB appears exposed



(a) LE versus r with $p_{CH} = 0.1$.

(b) LE versus p_{CH}, $r = 0.1$ km.

Fig. 5. Localization error as a function of r, α, and p_{CH}. (a) LE versus r; the annotated solid lines represent SIRLoS results while the dash-dot lines represent results from the centroid only method [32] for $\alpha = \frac{\pi}{4}, \frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2\pi$ for plots with the highest values (residing toward the top right extreme) approaching the lowest values (residing toward the bottom left extreme), respectively; (b) LE versus p_{CH}; solid line, solid in with closed circle, solid line with open circle, solid line with + and solid line with diamond represent results for $\alpha = \frac{\pi}{4}, \frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2\pi$, respectively.

to insider attackers. However, this information does not benefit the opponent as nodes do not route data back in the reverse direction from which they first received a CDB, but forward it along a directed path until it inadvertently reaches a CH. Hence, the unique nonce marking all CDBs are eventually validated by the BS identifying wrongful initiations.

D. Attack Analysis

The previous section illustrated the security advantages of path diversity in circuit-based routing. In this section, we focus on attacks that exploit the possibility of certain types of loop configurations to modify routing information sent to the BS during neighborhood discovery.

1) BS-Circuit Collusion Attack: We introduce a novel attack for DOMCNs 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_b, thereby breaking the security advantage of the represented BS-circuit. The motivation for this wormhole-type insider attack, as depicted in Figure 7(a), is to disrupt routing by deciphering PW_b, as similarly described in Section IV-C (Problem Case II), and then successfully dropping s_b's entry from any CDB, as illustrated in Figure 7(b); here, χ_{A1} receives a CDB at hop count $h-2$ and transmits η^*_{t+h-2} to χ_{A2}, who two hop counts later receives the same CDB at hop count h and computes $PW_b = \eta^*_{t+h-2} \oplus \eta^*_{t+h}$. Using PW_b, χ_{A2} can then modify its CDB to eliminate the presence of s_b as shown. For tractability, we only consider here the case with two colluding invaders χ_{A1} and χ_{A2} attempting a 2-hop attack targeting s_a and s_c, both 1-hop from/to node s_b, respectively. We state the collusion attacker's problem by asking: Given that χ_{A1} has successfully invaded s_b's predecessor s_a, what is χ_{A2}'s probability p_{ca} of invading a second node s_c that is one of s_b'successors?

We define the search region Ω_a where χ_{A2} attempts an invasion to be the region delineated by the locus of points at a fixed distance r from Φ_a, illustrated as the shaded regions in Figures 8(a) and (b) for $\alpha < \pi$ and $\alpha \geq \pi$ respectively. The probability p_{ca} of χ_{A2} invading node $s_c \in \Phi_b$ given $s_b \in \Phi_a$ (derived in Appendix B) is given by:

$$p_{ca} = p_a \left(1 - e^{-\frac{n\alpha r^2 A(\Phi_b)}{2A(\Omega_a)}}\right), \tag{5}$$

for $n \to \infty$ where $A(\cdot)$ is the area of the argument two-dimensional region, $A(\Phi_b) = \frac{\alpha r^2}{2}$ and

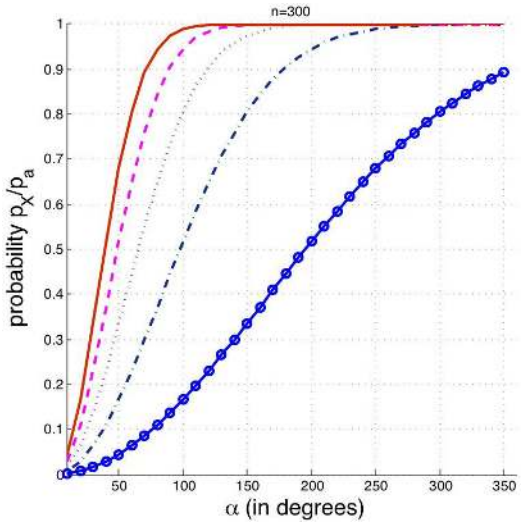
$$A(\Omega_a) = \begin{cases} r^2\left[2 + \frac{3\alpha}{2} + \pi\right] & \alpha < \pi \\ r^2\left[2(1+\alpha) + \frac{\pi}{2} - \sin(\frac{\alpha-\pi}{2})\right] & \pi \leq \alpha \leq 2\pi \end{cases} \tag{6}$$

where the corresponding regions Ω_a are shown in Figure 8.

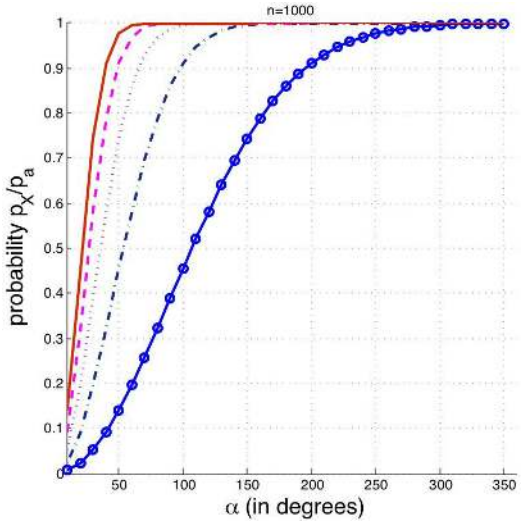
Figure 9 illustrates *normalized* p_{ca}/p_a versus α for $r = 0.05, 0.1, 0.15, 0.2$ and 0.25 and $n = 300, 1000$ and 5000. The results verify the advantage of directional communications in DOMCNs. Clearly for practical values of $n = 300$, and typical laser beamwidths of $\alpha \approx \frac{2\pi}{9}$, there is a significant security gain. As n and r are decreased, there is also less risk of the BS collusion attack since the attacker has fewer degrees of freedom to exploit to apply the attack.

2) Other Attacks on Routing: Other types of routing attacks well known in the literature can be considered for DOMCNs, but they fundamentally are not applicable due to the lack of bidirectional links. The interested reader is referred to [23], [25] for further details.

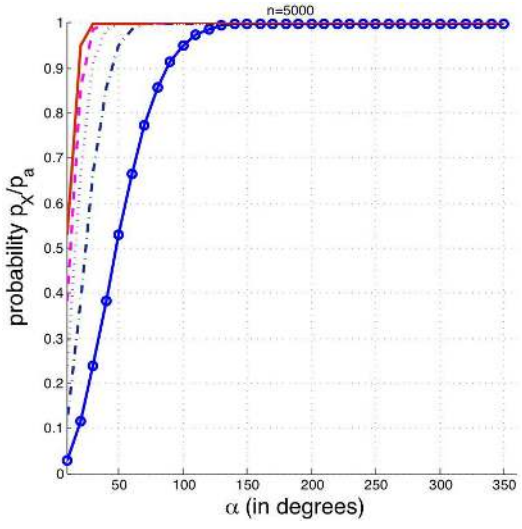
A particularly devastating outsider attack that does apply to DOMCNs is the *wormhole*, which has been widely studied for omnidirectional ad hoc networks [1], [34], [32]. Aimed at disrupting routing, a low metric route is established between two network locations through which the attacker tunnels packets recorded at one end of the wormhole to the other



(a) $n = 300$.

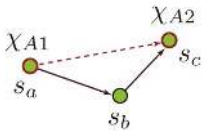


(b) $n = 1000$.

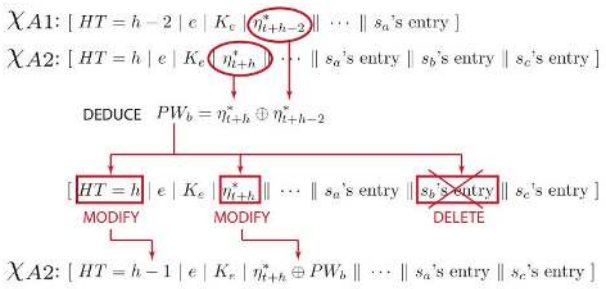


(c) $n = 5000$.

Fig. 6. Normalized bidirectional vulnerability (i.e., $p_{\chi_A}(> 0 \leftrightarrows)/p_a$) versus α for varying communication range r and node density n. Solid line, dashed line, dotted line, dash-dot line and solid line with open circle represent results for $r = 0.05, 0.1, 0.15, 0.2$ and 0.25, respectively.

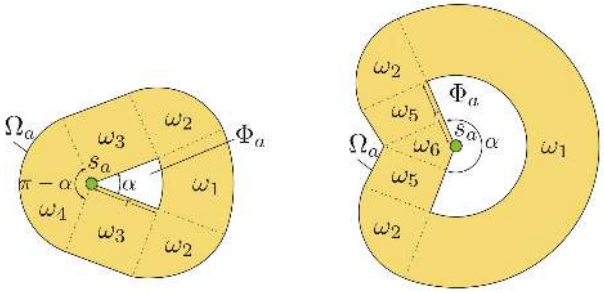


(a)



(b)

Fig. 7. BS-circuit collusion attack. (a) Colluders χ_{A1} and χ_{A2} have corrupted nodes s_a and s_c conveniently separated by legitimate node s_b; (b) Password information about s_b can be obtained to effectively remove knowledge of s_b from the CDB.



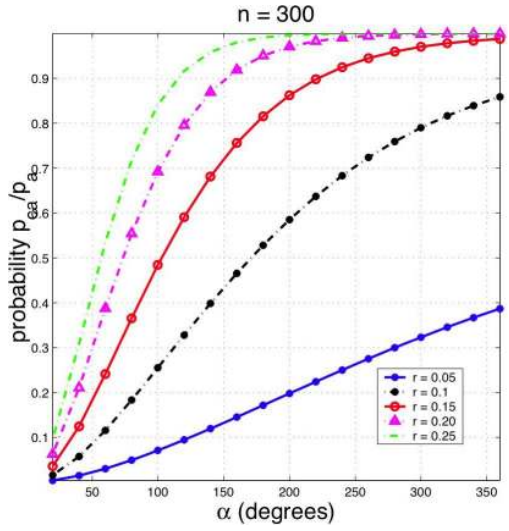
(a) $\alpha < \pi$ (b) $\alpha \geq \pi$

Fig. 8. Depicting the region of possibility where s_b's successor falls.

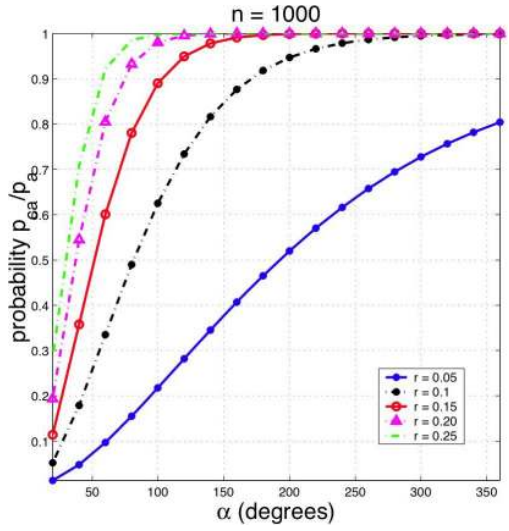
where he replays them in a timely manner. Two common models, long range and short range wormholes [35], are typically considered. We assert that for both models applied to the DOMCN, an ROC test can be employed to address these issues, so we do not consider them further.

V. Conclusion

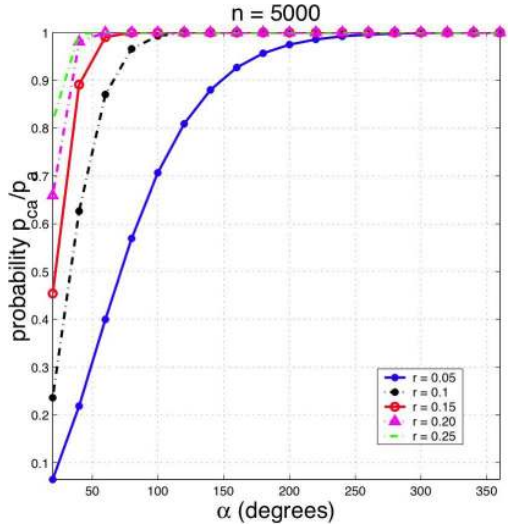
This paper introduced SIRLoS, a lightweight algorithm for integrated secure network discovery and localization for DOMCNs. To the best of the authors' knowledge, the research presented is the first contribution focused on directional optical link networks for MCN settings. For this reason, we have focused on evaluating foundation performance metrics for directional routing paradigms that would have near-monotonic relations to communications overhead and localization accuracy. These more general performance insights lead to an understanding of fundamental system compromises useful to



(a) $n = 300$.



(b) $n = 1000$.



(c) $n = 5000$.

Fig. 9. Normalized vulnerability to BS collusion attack versus α for varying communication range r and node density n. Solid line close circle, dash-dot line closed circle, solid line open circle, dash-dot line triangle and dash-dot line represent results for $r = 0.05, 0.1, 0.15, 0.2$ and 0.25, respectively.

those who intend to build upon or implement more specific networking protocols for DOMCNs.

Through analysis of SIRLoS we demonstrate, in part, the feasibility of directional communication paradigms at the networking level. In addition, to improved bandwidth, range, interference, power efficiency and security at the physical layer, we demonstrate the feasibility for practical network-level routing and the security advantages against network-level routing attacks through analysis of average hop count, localization error and the risk of insider attack. Additional performance and security analysis by the authors can be found in [22], [25], [36], [33], [12].

ACKNOWLEDGMENT

The authors thank members of Dr. Kundur's research group at Texas A&M University for lively discussions and insightful ideas. The authors also acknowledge several hours of use on The Texas A&M Supercomputing Facility (*http://sc.tamu.edu/*).

APPENDIX A
BIDIRECTIONAL VULNERABILITY ANALYSIS

The likelihood of a bidirectional vulnerability $p_{\chi_A}(> 0 \leftrightarrows)$ in a given node s_a is equal to p_a (the likelihood that χ_A compromises s_a) times the probability of s_a having one or more bidirectional links; the latter is given by one minus the likelihood it has no bidirectional links. We let Z_a be a random variable (r.v.) counting the number of s_a's successors. Therefore,

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

for $n \to \infty$, where it is employed from spatial point processes [37] that Z_a, follows a Poisson distribution of parameter $n\frac{\alpha r^2}{2}$, with $\frac{\alpha r^2}{2}$ as Φ_a's area.

APPENDIX B
COLLUSION ATTACK ANALYSIS

We let Z_b be a random variable (r.v.) counting the number of s_b's successors. The probability of χ_{A2} invading node $s_c \in \Phi_b$

given $s_b \in \Phi_a$ is:

$$\begin{aligned} p_{ca} &= p_a \sum_{z=0}^{n-1} (1 - \Pr[s_c \notin \Phi_b | s_c \in \Omega_a | Z_b = z]) \Pr[Z_b = z] \\ &= p_a \sum_{z=0}^{n-1} \left(1 - (1 - \frac{A(\Phi_b)}{A(\Omega_a)})^z\right) \frac{e^{\frac{-n\alpha r^2}{2}} \left(\frac{n\alpha r^2}{2}\right)^z}{z!} \\ &= p_a \left(1 - e^{-\frac{n\alpha r^2 A(\Phi_b)}{2A(\Omega_a)}}\right) \quad \text{for} \quad n \to \infty, \end{aligned}$$

where $A(\cdot)$ is the area of the argument two-dimensional region, Ω_a is shown in Figure 8 and the simplifying steps are analogous to those in Appendix A. $A(\Omega_a)$, given by Equation 6, is computed as the sum $\sum_i A(\omega_i)$ of the areas of the six regular-shaped partitions of the composite shape Ω_a as depicted in Figure 8, with $A(\omega_1) = \frac{\alpha r^2}{2}$, $A(\omega_2) = \frac{\pi r^2}{4}$, $A(\omega_3) = r^2$, $A(\omega_4) = \frac{(\pi-\alpha)r^2}{2}$, $A(\omega_5) = 2r^2[1 - \sin\frac{(\alpha-\pi)}{2}]$, and $A(\omega_6) = r^2[\sin\frac{(\alpha-\pi)}{2}]$.

REFERENCES

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

[2] R. Roy, X. Yang, R. Ramanathan, and N. H. Vaidya, "On designing MAC protocols for wireless networks using directional antennas," *IEEE Trans. Mobile Comput.*, vol. 5, no. 5, pp. 477–491, May 2006.

[3] Y. Li and H. Man, "Video transport over multi-hop directional wireless networks," *Wireless Communications and Mobile Computing*, vol. 7, pp. 217–233, 2007.

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

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

[6] P. Clark and A. Sengers, "Wirless optical networking challenges and solutions," in *Proc. IEEE Military Communications Conference*, 2004, pp. 416–422.

[7] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *Communications of the ACM*, vol. 43, no. 5, pp. 51–58, May 2000.

[8] J. M. Rabaey, M. J. Ammer, J. L. da Silva, D. Patel, and S. Roundy, "Picoradio supports ad hoc ultra-low power wireless networking," *Computer*, vol. 338, no. 7, pp. 42–48, July 2000.

[9] A. Chandrakasan, R. Min, M. Bhardwaj, S.-H. Cho, and A. Wang, "Power aware wireless microsensor systems," in *Proc. European Solid-State Circuits Conference*, Florence, Italy, September 2002.

[10] J. Díaz, J. Petit, and M. Serna, "A random graph model for optical networks of sensors," *IEEE Trans. Mobile Comput.*, vol. 2, no. 3, pp. 186–196, July-September 2003.

[11] S. D. Milner and C. C. Davis, "Hybrid free space optical/rf networks for tactical operations," in *Proc. IEEE Military Communication Conference*, Monterey, California, October-November 2004.

[12] U. N. Okorafor and D. Kundur, "On the relevance of node isolation to the K-connectivity of wireless optical sensor networks," *IEEE Trans. Mobile Comput.*, pp. accepted Feb. 10, 2009 as regular paper, 2009.

[13] P. Papadimitratos and Z. J. Haas, "Secure routing in mobile ad hoc networks," in *Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference*, San Antonio, Texas, January 2002.

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

[15] W. Dabbous, E. Duros, and T. Ernst, "Dynamic routing in networks with unidirectional links," in *Proc. Second International Workshop on Satellite-based Information Services*, Budapset, Hungary, October 1997, pp. 35–47.

[16] S. Nesargi and R. Prakash, "A tunneling approach to routing with unidirectional links in mobile ad-hoc networks," in *Proc. IEEE International Conference on Computer Communications and Networks*, Las Vegas, October 2000, pp. 522–527.

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

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

[19] V. Ramasubramanian and D. Mosse, "Statistical analysis of connectivity in unidirectional ad hoc networks," in *Proc. International Conference on Parallel Processing Workshops*, August 2002, pp. 109–115.

[20] A. Saha and D. B. Johnson, "Routing improvements using directional antennas in mobile ad hoc networks," in *Proc. IEEE Global Telecommunications Conference*, Dallas, Texas, November-December 2004, pp. 2902–2908.

[21] J. Díaz, J. Petit, and M. Serna, "Random scaled sector graphs," Department de Llenguatges i Sistemes Informàtics, Universitat Politècnica de Catalunya, Jordi Girona Salgado 1–3, Barcelona, Tech. Rep. LSI-02-47-R, 2002.

[22] U. N. Okorafor and D. Kundur, "Efficient routing protocols for a free space optical sensor network," in *Proc. IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, Washington, DC, November 2005, pp. 251–258.

[23] ——, "OPSENET: A security enabled routing scheme for a system of optical sensor networks," in *Proc. International Conference on Broadband Communications, Networks, and Systems (BROADNETS)*, San Jose, California, October 2006, pp. 1–10.

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

[25] D. Kundur, W. Luh, U. N. Okorafor, and T. Zourntos, "Security and privacy for distributed multimedia sensor networks," *Proc. IEEE*, vol. 96, no. 1, pp. 112–130, January 2008.

[26] U. N. Okorafor and D. Kundur, "On node isolation in directional sensor networks," in *Proc. ACM Conference on Embedded Networked Sensor Systems (SenSys)*, Syndney, Australia, November 2007, pp. 433–434.

[27] M. D. Penrose, Ed., *Random Geometric Graphs*. Oxford University Press, 2003.

[28] T. Ernst and W. Dabbous, "A circuit-based approach for routing in unidirectional links networks," Institut National de Recherche en Informatique et en Automatique, Tech. Rep. INRIA Research Report-3292, November 1997.

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

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

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

[32] L. Lazos and R. Poovendran, "SeRLoc: Secure range-independent localization for wireless sensor networks," *ACM Trans. Sensor Networks*, vol. 1, no. 1, pp. 73–100, August 2005.

[33] U. N. Okorafor, "Secure integrated routing and localization in wireless optical sensor networks," Ph.D. dissertation, Texas A&M University, College Station, Texas, August 2008.

[34] Y. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 370–380, February 2006.

[35] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Networks*, vol. 13, no. 1, pp. 27–59, January 2007.

[36] U. N. Okorafor and D. Kundur, *Security Aware Routing in Hierarchical Optical Sensor Networks*. Nova Science Publishers, 2008, ch. 5. [Online]. Available: https://www.novapublishers.com/catalog/product_info.php?products_id=6983

[37] N. Cressie, *Statistics for Spatial Data*. John Wiley & Sons, 1991.

Unoma N. Okorafor received the M.Sc. degree in electrical and computer engineering department from Rice University, Houston, TX, in 2001, and completed her Ph.D. degree in the Electrical and Computer Engineering Department, Texas A&M University, College Station in August 2008. Her research interests include secure network connectivity for wireless networks. In the past, she has interned at Intel, HP and IBM. She currently works with the Education Technology Division at Texas Instruments, Dallas Texas.

Dr. Okorafor is a member of IEEE, ACM, SWE, NSBE and SPIE. She has been the recipient of the Rice and TAMU university fellowships, Sloan Foundation Fellowship for minority Ph.D. students, the AAUW Engineering Dissertation Fellowship and the NSF Graduate Fellowship for promoting STEM education in middle schools. In 2008 and 2009, Dr. Okorafor served as a visiting faculty at the African University of Science and Technology, Nelson Mandela Institution in Abuja Nigeria. She teaches short courses in Software Engineering and Programming, and has published one book chapter and numerous international journals and conferences articles.

Dr. Okorafor is very passionate about promoting science, technology, engineering and math education for middle school and high school students, with a special focus on female and minority students. She is the founder of a non profit organization named WAAW Foundation (Working to Advance African Women), and has attended numerous women in science conferences.

Deepa Kundur received the B.A.Sc., M.A.Sc., and Ph.D. degrees all in electrical and computer engineering in 1993, 1995, and 1999, respectively, from the University of Toronto, Canada. From September 1999 to December 2002 she was an Assistant Professor and held the title of Bell Canada Junior Chair-holder of Multimedia in the Department of Electrical and Computer Engineering at the University of Toronto. In January 2003, she joined the Department of Electrical and Computer Engineering at Texas A&M University, where she is currently an Associate Professor.

Dr. Kundur is the author of over 100 technical publications in the field of information security, multimedia and signal processing and communication systems. Her current research interests include cybersecurity of the electric smart grid, security and privacy of social and sensor networks, multimedia security, and computer forensics. She is an appointed member of the NERC Smart Grid Task Force, an elected member of the IEEE Information Forensics and Security Technical Committee, vice-chair of the Security Interest Group of the IEEE Multimedia Communications Technical Committee and on the editorial boards of the IEEE Transactions on Multimedia, and EURASIP Journal on Information Security.